Наръчник за длъжностните лица по защита на данните

Насоки за длъжностните лица по защита на данните в публичния сектор относно това как да осигурят спазване на Регламент (ЕС) 2016/679

(Общия регламент относно защитата на данните)

Финансиран по проект „T4DATA” от Европейския съюз по програма „Права, равенство, гражданство“

(Споразумение за безвъзмездна финансова помощ: 769100 — T4DATA — REC-DATA-2016/REC-DATA-2016-01)

Съставители:

Дау Корф

Почетен професор по международно право, Университет Метрополитан, Лондон
Лектор, Оксфорд Мартин Скуул, Университет Оксфорд

&

Мари Жорж

Независим международен експерт по защита на данните
(CNIL, ЕС, Съвета на Европа и т.н.)

Членове на Fundamental Rights Experts Europe (FREE) Group

Отразяващ съществения принос на италианския орган за защита на данните и партньорите по проекта

(Приет от Европейската комисия, юли 2019 г.)

Дау Корф и Мари Жорж

Наръчник на длъжностните лица по защита на данните

За Наръчника:

Този Наръчник е изготвен като част от обучителните материали за „T4DATA" – проект за обучение на обучители, финансиран от ЕС, който има за цел да обучи служители в органи по защита на данните (ОЗД) на държавите-членки на ЕС, за да осигурят обучение на длъжностни лица по защита на данните (ДЛЗД) в публичния сектор, за задълженията им по Регламент (ЕС) 2016/679 (Общия регламент относно защитата на данните, ОРЗД). Проектът се изпълнява в партньорство с италианския орган за защита на данните, *Garante per la protezione dei dati personali*, и се координира от *Fondazione Basso*, с помощта на двама експерти от Групата *Fundamental Rights Experts Europe* (FREE), г-жа Мари Жорж и проф. Дау Корф.

Голям принос за създаването на този наръчник носи Италианският надзорен орган, както и другите надзорни органи (партньори по проекта), които изпратиха много полезни практически примери и копия от своите собствени указания относно ОРЗД.

В случай на цитиране на предходния опит на ключовите експерти, името му/ѝ е в бележка под линия, позоваваща се на публично достъпни източници. Предвид институционалната обвързаност и достъпа до поверителни документи на национални и международни органи в областта на защита на данните при Мари Жорж това рядко е възможно.

За информация относно програмата, партньорите и експертите, вж.:

http://www.fondazionebasso.it/2015/wp-content/uploads/2018/04/T4Data_Brochure.pdf

Макар и създаден по проект T4DATA, се надяваме, че Наръчникът ще бъде полезен и за всеки друг, който проявява интерес от прилагането на Регламент 2016/679, и – по-специално – други длъжностни лица по защита на данните (в публичния или частния сектор). Предложеният текст се предоставя публично с лиценз „Creative Commons" (CC).

.

Бележка: Тъй като Наръчникът има за цел да подпомогне обучението на длъжностни лица по защита на данните (ДЛЗД) в областта на задълженията им по ОРЗД, той се фокусира върху законодателството на ЕС в областта на защитата на данните, върху законодателството в областта на защитата на данните във връзка с въпросите, които преди се отнасяха към „Първия стълб". или относно въпроса за вътрешния пазар. Раздели 1.3.4 - 1.3.6 и 1.4.3 - 1.4.5 все още накратко въвеждат правилата и инструментите за защита на данните, които са се прилагали или се прилагат по други въпроси, обхванати от правото на ЕС, т.е. въпроси, които попадат в сферата на преди наричаната „Правосъдие и вътрешни работи" (ПВР) или „Трети стълб" - сега се нарича област на „Свобода, сигурност и правосъдие" (ССП); въпроси, свързани с така наречената Обща външна политика и политика на сигурност (ОВППС) - предишният „Втори стълб"; и дейностите на самите институции на ЕС; раздел 1.4.6 разглежда обмена на данни между различните режими на ЕС. Също така не се обхваща защитата на данните извън ЕС / ЕИП, въпреки че смятаме, че ДЛЗД би трябвало да придобият поне някои познания за основното влияние, което правилата на ЕС са оказали и продължават да оказват върху защитата на данните в световен мащаб.

Надяваме се да сме в състояние да добавим тези въпроси в последващо, второ издание на този наръчник, в което след това би трябвало да можем и да актуализираме информацията по въпроси, които са все още неуточнени в момента на написване на това първо издание, като – по-специално – развития във връзка с Регламента в областта на правото на неприкосновеност на електронните комуникации, който към момента на съставянето все още са в процес на приемане.

Наръчника:

е достъпен и на италйански, хърватски, български, полски, испански (тоест езиците на всички партньори по проекта

ОПРОВЕРЖЕНИЕ:

Информацията и възгледите, изложени в този наръчник, са на авторите и не отразяват непременно официалното становище на Европейския съюз. Нито институциите и органите на Европейския съюз, нито което и да е лице, действащо от тяхно име, не могат да бъдат отговорни за използването на съдържащата се в наръчника информация.

Допълнителни преводи (по-специално превод на френски) се разглеждат (в зависимост от финансирането).

Предисловие

Това издание на „Наръчника“, изготвен като част от проект „T4Data – Обучение за данните“, финансиран от Европейския Съюз (ЕС). Вярваме, че той ще се окаже повече от „просто поредното“ ръководство за Общия регламент относно защитата на личните данни (ОРЗД).

Това е полезно помагало, чието осъществяване стана възможно, най-напред, благодарение на упоритя труд и отдаденост на двамата експерти, избрани за тази цел, г-жа Мари Жорж (Marie Georges) и професор Дау Корф (Douwe Korff), които имат дългогодишни познания в областта на правата на човека, както и концептуални и практически въпроси в областта на информационните и комуникационни технологии (ИКТ) и защитата на данните – и второ, благодарение на съдействието на служителите и членовете на петте участващи надзорни органи, които са споделили своите ежедневни практика и опит, за да осигурят значим принос към насоките, които се съдържат в Наръчника.

Преди всичко в този наръчник се разглежда действащо законодателство. Основната му цел е да се преведат новите, безспорно, по-взискателни дейности за отчетност, заложени в новата правна рамка на ЕС, които са насочени към гарантиране на ефективността на защитата на данните в един свят, в който обработката на данни засяга всички измерения на живота - чрез практични, стабилни, документирани насоки и съвети, които ще бъдат адаптирани и разширени допълнително благодарение на националните дейности за обучение и разпространение. Те ще продължат през цялата 2019 г. върху основите на Наръчника. Целта на тези насоки е да достигнат до длъжностните лица за защита на данните (ДЛЗД), и по-специално тези, работещи в публичния сектор, които ще могат да го използват като своеобразен трамплин за укрепване и повишаване на собствената си компетентност в областта на защитата на данните в полза на всички заинтересовани страни - администраторите, субектите на данни и широката общественост.

Ето защо, нашите пет надзорни органи решиха да обединят силите си в изпълнението на проекта T4Data. Особено доволни сме да представим този проект, преведен на английски език, както и на съответните ни национални езици. Надяваме се, че Наръчникът ще бъде достъпен и на френски език в близко бъдеще - знаейки, че това ще подсили връзката на веригата от инструменти за сътрудничество, които развиваме всеки ден на европейско ниво и в световен мащаб.

- Венцислав Караджов, Председател на Комисия за защита на личните данни на Република България

/п/

- Анто Райковача, Директор на Агенция за защита на личните данни на Република Хърватия

/п/

- Антонело Соро, Президент на надзорния орган на Италианската република

/п/

- Едита Биелак – Йомаа, Президент на Службата за защита на личните данни в Република Полша

/п/

- Мар Еспания Марти, Директор на Агенцията за защита на данните на Кралство Испания

/п/

СЪДЪРЖАНИЕ

Задача 10: Съветване и извършване на мониторинг на спазването на политиките за защита на данните, на договори между съвместни администратори, между администратори и между администратор и обработващ лични данни, на Обвързващи корпоративни правила и клаузи за предаване на данни

Задача 11: Участие в кодекси за поведение и системи за сертифициране

Сътрудничество и консултиране с органа по защита на данните:

Задача 12: Сътрудничество с органа по защита на данните

Разглеждане на молби на субекти на данни :

Задача 13: Разглеждане на заявки и жалби на субекти на данни

Информация и повишаване на осведомеността

Задача 14: Вътрешни и външни задачи за информиране и повишаване на осведомеността

Задача 15: Планиране и преглед на дейностите на ДЛЗД

- o – O – o -

Насоки за длъжностните лица по защита на данните в публичния сектор относно това как да осигурят спазване на Регламент (ЕС) 2016/679 (Общия регламент относно защитата на данните)

Въведение

На 25 май 2018 г. започна прилагането на Общия регламент относно защитата на данните на ЕС (**ОРЗД** или „**Регламента**")[1], заместващи Директивата за защита на данните от 1995 г. („Директивата от 1995 г.").[2] Приет в отговор на все по-мащабното обработване на лични данни след въвеждането на Директивата от 1995 г. и на разработването на все по-натрапчиви технологии, Регламентът надгражда Директивата и практиката на Съда на Европейския съюз (CJEU) по нея. Изпълнявайки тази функция, той развива в детайли заложеното от Директивата и същевременно значително засилва основния режим за защита на данните на ЕС. Той въвежда много изменения с цел постигане на по-добра хармонизация, по-големи права на субектите на данни, по-тясно трансгранично сътрудничество между органите по защита на данните (ОЗД),и т.н.

Сред най-важните изменения са въвеждането на нов принцип на „отчетност", и на задължително определяне на длъжностни лица за защита на данните (**ДЛЗД**). Те са свързани помежду си: длъжностните лица по защита на данните ще бъдат хората, които, на практика, ще трябва да осигурят спазване на принципа на отчетност от и в рамките на организациите, към които принадлежат. Този Наръчник има за цел да подпомогне длъжностните лица по защита на данните в публичния сектор в това начинание.

Наръчникът се състои от три части:

- **Част едно** въвежда понятията на „поверителност", „неприкосновеност" и „защита на данните" и първите закони, принципи и международни инструменти (по-специално конвенцията на Съвета на Европа за защита на данните от 1981 г.) в областта на защитата на данни, преди да разгледа директивите за защита на данните от „Първия стълб" на ЕС от 90-те години на 20 век и началото на първото десетилетие на 21 век и да представи наскоро приетите и предстоящи инструменти в областта на защитата на данните за бъдещето (ОРЗД, предложеният Регламент в областта на правото на неприкосновеност на електронните комуникации, и „Осъвременената" Конвенция на Съвета на Европа).[3] Първата част не разглежда все още инструментите в сферата на „Третия

[1] Пълно наименование: Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните), О.В. L 119 от 4.5.2016 г., стр.1 и сл., може да бъде намерен на: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

[2] Пълно наименование: Директива 95/46/ЕО на Европейския парламент и на Съвета от 24 октомври 1995 година за защита на физическите лица при обработването на лични данни и за свободното движение на тези данни, ОВ L 281 от 23.11.1995 г., стр.31 и сл., може да бъде намерена на: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=en

[3] Относно ограниченията свързани с обсъдените въпроси, вж. Бележката в кутията „*Относно този наръчник*" на стр.1.

стълб" на ЕС от 90-те години на 20 век и правилата за защита на данните за собствените институции на ЕС и техните правоприемници.

- **Част две** предоставя обзор на всички ключови елементи от Общия регламент относно защитата на данните, преди да се фокусира върху новия основен принцип на „отчетност" и концепцията и правилата в ОРЗД във връзка с Длъжностното лице по защита на данните.
- **Част три** предоставя практическо ръководство за това как длъжностните лица по защита на данните в публичния сектор могат и следва да изпълняват своите задачи, с примери от реалния живот, във връзка с трите области на фокус: образование, финанси и здравеопазване.

Освен подробните позовавания и връзки към материали в бележки под линия, отделна част две към наръчника съдържа допълнителни материали, които се предоставят на участниците в обученията по „T4DATA".

Уебсайт:

Възможно най-голям брой от горепосочените материали и връзки ще бъдат предоставени и на публично достъпния уебсайт, който придружава този Наръчник (който също е безплатно предоставен с лиценз „Creative Commons"):

http://www.fondazionebasso.it/2015/t4data-training-data-protection-органи-and-data-protection-officers/

ПЪРВА ЧАСТ

Произходът и значението на защитата на данните

Тази част е посветена на обяснение на това какво е „защита на данните“, как тя се е развила в Европа и как новите и „модернизирани” европейски инструменти в областта на защитата на данните се стремят да отговорят на най-новото технологично развитие.

- Раздел 1.1 разглежда различаващите се (ако се припокриват) концепции на поверителност, неприкосновеност, личен живот, защита на данните, както и разработеният в Европа подход за защита на данните, включително изискванията за правата на човека и върховенството на закона, които – в Европа – са в основата на защитата на данните.
- Раздел 1.2 обхваща произхода на защитата на данните в Европа, появата на основните принципи и права на защита на данните, и тяхното развитие в европейските и глобалните необвързващи нормативни актове – и в един обвързващ, Конвенцията на Съвета на Европа за защита на данните от 1981 г. (включително нейния Допълнителен протокол от 2001).
  - Раздел 1.3 разглежда начина, по който правилата и принципите за защита на данните бяха доразвити в Директивите на ЕС за защита на данните от 1990 г. и началото на 21 век (за да се даде възможност за развитието на „Вътрешния пазар” на ЕС, който изискваше както свободния поток на данни, така и защита на основното право на защита на данните), с акцент върху Директивата за защита на данните от 1995 г (с които Допълнителният протокол от 2001 г. към Конвенцията от 1981 г. се стреми да приведе тази конвенция в съответствие): (подраздели 1.3.1 и 1.3.2); и обсъжда специалните правила за телекомуникационния сектор (подраздел 1.3.3).Бележка: Надяваме се да представим останалите инструменти на ЕС в областта на защитата на данните, приети в този период, за т.нар. „Трети стълб” (обхващащи правоприлагане и съдебна взаимопомощ), както и за собствените институции на ЕС, и да предоставим обзор на правилата за защита на данните/ неприкосновеността на информацията в останалата част от света, част две на наръчника.
- Раздел 1.4 представя най-новите нормативни актове, приети, за да посрещнат бъдещото: Общ регламент относно защитата на данните на ЕС от 2016 г. (ОРЗД, в сила от 25 май 2018 г.); (подраздел 1.4.1) и предложената замяна на директивата на ЕО от 2002 г. относно правото на неприкосновеност на личния живот и електронните комуникации с Регламент в областта на правото на неприкосновеност на електронните комуникации; (подраздел 1.4.2)..
  - Следващите подраздели в този раздел накратко отбелязват основния нов инструмент за защита на данните в така наречената пространство на правосъдие, свобода и сигурност (ПССП), ДИРЕКТИВА (ЕС) 2016/680 (ПВР) за защита на данните за правоприлагане от 2016 г. (подраздел 1.4.3); ситуацията във връзка с ОВППС (подраздел 1.4.4); и актуализацията на инструмента за защита на данните за институциите на ЕС, Регламент 2018/1725 (подраздел 1.4.5). В подраздел 1.4.6 са разгледани потоците от данни между различните режими на защита на данните в ЕС.
  - „Модернизирана“ Конвенция на Съвета на Европа, отворена за подписване през октомври 2018 г., се обсъжда в последния подраздел (подраздел 1.4.7).

-

Бележка: Още веднъж се надяваме да представим инструментите на ЕС за защита на данните за посочени по-горе области (правоприлагане и съдебна взаимопомощ, ОВППС, и собствените институции на ЕС), приети, за да заменят тези от 90-те години на 20 век и началото на първото десетилетие на 21 век, и най-новите глобални правила, по подробно в едно второ издание.

ОРЗД – който е в ядрото на този наръчник – е доразвит в Част Две.

1.1 Поверителност, неприкосновеност/личен живот и защита на данните: различни но допълващи се институти в епохата на дигитализация

1.1.1 Поверителност и неприкосновеност на личен живот

Винаги е имало области, в които личната информация е третирана като обект на специални правила за **поверителност**. Класически примери са Хипократовата клетва за **лекарите**[4] **от 4ти век пр. Хр.** и „**тайната на изповедта**" в Римокатолическата църква.[5]От 19 век насам, **банкерите, адвокатите**, други **свещенослужители**, **пощенски и телекомуникационни служители** и много други е трябвало да третират информацията, която получават от лицата в своето служебно качество като поверителна, адвокатска тайна,[6] или дори свещена.

Тези задължения за поверителност принципно се разглеждат, като служещи, както на отделното лице, така и на обществото: субектът може да има доверие на лицето, на което разкрива информация третирана като поверителна и това доверие на свой ред служи за общественото благо, тъй като липсата му може да възпре хората да търсят помощ или да разкриват информация на органите на властта, което подкопава общественото здраве и други социални блага, например, при опит за борба с разпространението на предавани по полов път заболявания, политически или религиозни въпроси.

Както обяснява Фритц Хондиус, заместник-директор по правата на човека в Съвета на

---

[4] Хипократовата клетва се приписва на Хипократ (около 460-370 г. пр.н.е.) в античността, макар че според нова информация тя може да е била написана след смъртта му. Най-старата съществуваща версия датира от около 275 г. сл. н.е. и следната: ἃ δ᾽ ἂν ἐνθεραπείῃ ἴδω ἢ ἀκούσω, ἢ καὶ ἄνευ θεραπείης κατὰ βίον ἀνθρώπων, ἃ μὴ χρή ποτε ἐκλαλεῖσθαι ἔξω, σιγήσομαι, ἄρρητα ἡγεύμενος εἶναι τὰ τοιαῦτα. "*Всичко, каквото видя или чуя при изпълнението на своята професия или извън нея и което не бива да се разправя, аз ще го пазя в тайна и ще го смятам за нещо свещено.*" (Превод от Джеймс Лойб, 1923 г.). Вж.: https://en.wikipedia.org/wiki/Hippocratic_Oath

[5] В Римокатолическата църква „тайната на изповедта" е ненакърнима. Вж.: https://www.catholiceducation.org/en/religion-and-philosophy/catholic-faith/the-seal-of-the-confessional.html

[6] Според Регулаторния орган на юристите (Solicitors Regulation Authority (SRA)), който урегулира адвокатите и адвокатските кантори в Англия и Уелс, (в английското право) има „разлика между поверителност и адвокатска тайна. Накратко, поверителната информация може да бъде оповестена, когато е подходящо това да бъде направено, но адвокатската тайна е абсолютна и, поради това, адвокатската тайна не може да бъде оповестявана. Поверителните съобщения между адвокати и клиенти за целите на получаването и даването на юридическа консултация са адвокатска тайна."
https://www.sra.org.uk/solicitors/code-of-conduct/guidance/guidance/Disclosure-of-client-поверителна-information.page
Във Франция, професионалната тайна (*secret professionnel*) на адвоката (*avocat*) е въпрос на *ordre public*, абсолюта, неограничена във времето и обхващаща всички видове правни въпроси и всяка форма на информация (писмена, електронна, аудио и т.н.). Вж.:
http://www.avocatparis.org/mon-metier-davocat/deontologie/secret-professionnel-et-поверителнаite

Европа и отговарящ за изготвянето на първия международно-обвързващ инструмент в областта на защитата на данните, Конвенцията на Съвета на Европа за защита на данните от 1981 г., обсъдена в точка 1.2.3, по-долу), въпреки наложеното им задължение за поверителност:[7]

> нямаше съответно право, предоставено на пациентите, клиентите или гражданите, да проверят точността и относимостта на данните, които ги засягат. И макар да съществуваха правни санкции за наказание на грубите злоупотреби с обработка на данни, нямаше закони, предвиждащи указания за това как надлежно да се създават и управляват досиета с лични данни.

Правото на „**неприкосновеност**" или „**зачитане на неприкосновеността на личния живот**" е включено в международните договори за правата на човека след втората световна война, Международния пакт за граждански и политически права на ООН (МПГПП, чл. 17) и Европейската конвенция за правата на човека (ЕКПЧ, член 8).[8] Защитава от ненужни намеси от страна на държавата в личния живот на лицето, като например прихващане на комуникации от държавни агенции[9] или инкриминиране на лични полови актове.[10] Правото, също така се е тълкувало, от Европейския съд по правата на човека, като изискване към държавата да защитава лицата, от публикуването на техни снимки направени от частни лица, без тяхно съгласие, [11] и срещу следене на лични съобщения и комуникациите им от техните работодатели без съответното правно основание.[12]

Също така, чл. 8 от ЕКПЧ в последно време все повече се тълкува и прилага така, че да защитава, както физическите лица по отношение на техните лични данни, така и във връзка със събирането, използването и запазването на тези данни за тях, по-специално от националните служби за сигурност,[13] през 70-те и 80-те години на 20 век, степента, в

---

7 Frits Hondius, *A decade of international data protection*, in: Netherlands International Law Review, Vol. XXX (1983), pp. 103 – 128 (Фриц Хондиус, *Десетилетие международна защита на данните*, в: Нидерландски международно-правен обзор, том XXX (1983), стр.103 – 128) (не може да бъде намерена онлайн).

8 Чл. 12 от Всеобщата декларация за правата на човека от 1948 г. Всеобщата декларация за правата на човека, която е инструментът „майка" и на МПГПП и на ЕКПЧ (но, която не е обвързващ договор), вече предвижда в Чл. 12, че: „Никой не трябва де бъде подлаган на произволна намеса в личния му живот, семейството, жилището и кореспонденцията…" МПГПП и ЕКПЧ са създадени успоредно през периода 1949-50 г. (но ЕКПЧ, която е открита за подписване в края на 1950 г. и влиза в сила през 1953 г., влиза в сила повече от двадесет години преди МПГПП, която е откриата за подписване през 1966 г. и влиза в сила едва през 1976 г.).

9 Напр., ЕСПЧ, *Klass v. Germany*, решение от [ДОБАВЕТЕ ДАТА].

10 Напр., ЕСПЧ, *Dudgeon v. the UK*, решение от [ДОБАВЕТЕ ДАТА].

11 Напр., ЕСПЧ, *von Hannover v. Germany*, решение от [ДОБАВЕТЕ ДАТА].

12 Напр., ЕСПЧ, *Halford v. the UK*, решение от 25 юни 1997 г.

13 Вж. Информационен лист – защита на личните данни на Съвета на Европа от 2018 г., който може да бъде намерен на:
https://www.echr.coe.int/Documents/FS_Data_ENG.pdf
Неизчерпателен списък с дела на Европейския съд по правата на човека във връзка със защитата на личните данни може да бъде намерен на:
https://www.coe.int/en/web/data-protection/echr-case-law
За по-общо обсъждане, вж. Lee A Bygrave, *Data Protection Pursuant to the Right to Privacy in Human Rights Treaties*, International Journal of Law and Information Technology, 1998, volume 6, (Лий А Байгрейв, *Защита на данните съгласно правото на личен живот в договорите за защита на правата на човека*, Международен журнал за право и информационни технологии) стр.247–284, което може да бъде намерено на:

която можеше да се разчита на правото на личен живот в отношенията между физическите лица и между физическите лица и частните юридически лица (т.нар. въпрос за „хоризонталния ефект на правата на човека" или *Drittwirkung*) беше много неясна[14] – и все още не е напълно уточнена от гледна точка на традиционното право в областта на правата на човека. Във всеки случай, физическите лица не могат да изведат от Европейската конвенция за правата на човека (или МПГПП), правото на иск срещу други физически лица – мярката с най-силно въздействие, която могат да предприемат е действие срещу съответната държава членка за това, че не ги защитава, съгласно съответното национално право, срещу действията на тези други лица.

В обобщение: Законите и правилата в областта на поверителността, професионалната защитена информация и тайна, и гаранциите за неприкосновеност на правата на човека, и личния живот не са и не защитават адекватно физическите лица срещу злоупотреба със събирането и използването на техните лични данни.

Следователно, е признато едно отделно и обособено право на „**защита на личните данни**" („защита на данните"), като то се обсъжда по-долу. Но, разбира се, това ново *sui generis* право трябва винаги да се разглежда,ч като тясно свързано с и допълващо традиционните права – както са заложени в Европейската конвенция за правата на човека и по-специално в МПГПП: защитата на данните се стреми да гарантира пълното и ефективно прилагане на традиционните права в (относително) новия цифров контекст.

1.1.2 „Защита на данните"

Първите компютри са създадени за военни цели през **втората световна война**. Британските разбивачи на кодове, под ръководството на великия Алън Тюринг,[15] създават примитивни версии за декриптиране на германските съобщения, кодирани с *Enigma* и *Lorenz*.[16] В САЩ, IBM, под ръководството на първия си главен изпълнителен директор, Томас Джей Уотсън, произвежда големи количества оборудване на обработване на данни за военните и започва да експериментира с аналогови компютри.[17] А немците ги използват за изчисляване на траекторията на ракетните снаряди *V2*[18].

---

https://www.uio.no/studier/emner/jus/jus/JUR5630/v11/undervisningsmateriale/Human_rights.pdf

[14] Вж. Хондиус, о.с. (бележка под линия 7, по-горе), стр.107, във връзка с Report by the Committee of Experts on Human Rights (Доклад на Експертния комитет по правата на човека), Съвет на Европа (DH/EXP(70)15).

[15] Вж.: http://www.maths.manchester.ac.uk/about-us/history/alan-turing/

[16] Вж.: Chris Smith, *Cracking the Enigma code: How Turing's Bombe turned the tide of WWII*, 2 November 2017 (Крис Смит, *Разбиването на кода Enigma: Как Бомбе на Тюринг обърна вълната на втората световна война*, 2 ноември 2017 г.), която може да бъде намерена на: http://home.bt.com/tech-gadgets/cracking-the-enigma-code-how-turings-bombe-turned-the-tide-of-wwii-11363990654704
Машината *Colossus*, използвана за декодиране на съобщенията *Lorenz*, принципно считана за „първият програмируем електронен, цифров копмютър на света". Вж.: https://en.wikipedia.org/wiki/Colossus_computer

[17] Вж.: https://en.wikipedia.org/wiki/Thomas_J._Watson

[18] Вж.: Helmut Hoelzer's Fully Electronic Analog Computer used in the German V2 (A4) rockets (Helmut Напълно електронният аналогов компютър на Хьолцер, използван в германските ракети V2 (A4)) (основно на немски език), която може да бъде намерена на: http://www.cdvandt.org/Hoelzer%20V4.pdf

Необходимостта от защита на човешките права и свободи в една демокрация във връзка с автоматизираната обработка на лични данни се появява едва по-късно, когато – през **60-те години на 20 век** – започват да се използват компютри за управленски цели в публичния и частния сектор. Поради високата цена на компютрите и голямото пространство, което им е необходимо към онзи момент, това се прави само в развити държави, и дори там – само за големи публични органи и дружества. Първите компютъризирани дейности са за изплащане на заплати и доставчици, за регистър на пациентите в болници, за публично преброяване и статистика - и за полицейски досиета..

В светлината на тези събития, в **края на 60-те години/началото на 70-те години на 20 век**, същите дебати започват да се провеждат във Федерална Република Германия (по-специално, в *Провинция* Хесен, относно полицейските досиета), Норвегия, Швеция и Франция , Обединеното кралство, САЩ и др. – както и в ОИСР и Съвета на Европа.[19] Първоначално тези дебати се водят между професионалисти, обвързани от етични задължения (в САЩ, по-специално между лекари и ИТ инженери, които първи създадоха насоки за „Практиките за обективно информиране")[20], и сред политици, които са по-загрижени за рисковете от злоупотреба, неправилно обработване и сигурност на лични данни, които се обработват автоматично.

След това, в **средата и края на 70-те години и началото на 80-те години на 20 век**, те се разпространиха сред по-широки кръгове от населението във Франция. Това бе в следствие на сигнали през 1974г. за нередности, на правителствени планове да се създаде национална база данни на всички френски граждани и жители с уникален идентификационен номер за всеки от тях; и на съществуването на спорни полицейски досиета[21]. В Германия имаше широка опозиция, в един напрегнат политически климат, срещу предложеното национално преброяване от 1983 г.[22] Тези обсъждания не бяха просто за риска от нарушение на неприкосновеността на личния живот, станало

---

[19] Съветът на Европа приема първите си решения по въпросите през 1973 г. и 1974 г.: Решения на Съвета на министрите (73) 22 и (74) 29 (за линкове, вж. бележки по линия 38 и 39, по-долу). Вж. Обяснителния меморандум към Конвенцията от 1981 г. на Съвета на Европа за защита на данните, пар. 6, който може да бъде намерен на:
https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800ca434
Принципите, изтъкнати в тези решения, са включени в Приложение 1 към наръчника.

[20] Вж.: Robert Gellman, Fair Information Practices: A basic history (Робърт Гелмън, Практики за обективно информиране: Основна история), available at:
https://bobgellman.com/rg-docs/rg-FIPshistory.pdf
В продължение на много години, от 70-те до 90-те години на 20 век, Гелман работи по американски законодателни въпроси във връзка с личния живот в Камарата на представителите.

[21] Вж. статията във вестник Le Monde от 21 март 1974 г., "*SAFARI ou la chasse aux Français*" („SAFARI, или ловът на французи"), която може да бъде намерена на:
http://rewriting.net/2008/02/11/safari-ou-la-chasse-aux-francais/
Името на базата данни SAFARI беше акроним на „*système automatisé pour les fichiers administratifs et le répertoire des individus*" (Автоматизирана система за административни досиета и събиране на преписки за физически лица). Разкритието беше отразено от всички вестници през следващите дни и правителството спря проекта няколко дни по-късно, назначавайки *ad hoc* комисия, която да проучи целия проблем и да предложи законни решения.

[22] Вж.: Marcel Berlinghoff, *Zensus und Boykott. Die Volkszählung vor 30 Jahren*, в: Zeitgeschichte-online, юни 2013 г., което може да бъде намерено на:
https://zeitgeschichte-online.de/kommentar/zensus-und-boykott-die-volkszaehlung-vor-30-jahren

възможно чрез използването на нови технологии, но и относно последиците от грешки в данните и относно евентуална авторитарна власт, създадена от централизиране на данните, събирани за различни цели и/или използването на уникални идентификатори за свързване на досиета. В Европа, те доведоха до търсене на специфична, основана на закона „защита на данните" или „информатика и свободи", подкрепена от нарастващото разпознаване на тази нужда от висши съдилища, както и от приемането на международни инструменти (както е разгледано в раздел 1.2, по-долу).

Терминът „защита на данните" (на немски език: Datenschutz) първоначално е включен в заглавието на първия закон по темата, Закона за защита на данните от 1970 г. (Datenschutzgesetz) на немската провинция Хесен, изготвен от „бащата на защитата на данните", проф. Спирос Симитис.[23] Както изтъква Буркерт, заглавието е всъщност „неправилно, тъй като [Законът] не защитава данните, а правата на лицата, чиито данни [се] обработват."[24]

Понятието остава и сега вече е известно по целия свят (французите сега също говорят за ***protection des données***), то е съкращение на „защитата на лицата по отношение на обработването на лични данни" (дългата фраза, използвана в заглавията и на Директивата на ЕО от 1995 г. за защита на данните и на Общия регламент относно защитата на данните на ЕС от 2016 г.).[25] Но дори тази по-пълна фраза не изяснява напълно значението на понятието в очите и съзнанието на европейците.

Защитата на данните има както индивидуални, така и социални аспекти.

Така, във Франция (където законът използва израза „информатика, файлове и свободи"/"*informatique, fichiers et libertés*") защитата на данните се разглежда като част от ролята на лицето и свързаните с нея социални и конституционни изисквания, според които:

> **Информатиката трябва да бъде в служба на всеки гражданин. … Тя не може да застрашава самоличността на човека, правата на човека, личния живот, индивидуалните или обществените свободи**[26]
>
> (Чл. 1 от *Закона за информатиката, досиетата и свободите* от 1978 г.)

Този френски закон е придобил конституционен статут и решенията на висшите съдилища на страната са основани на неприкосновеността или свободата, в зависимост от конкретните случаи.

В Германия защитата на данните се разглежда предимно като произтичаща от правото

---

[23] *Hessisches Datenschutzgesetz (HDSG) 1970*, в сила от 13 октомври 1970 г., *Gesetz- und Verordnungsblatt für das Land Hessen, Teil I*, 1970, № 41 (12 октомври 1970 г.), стр.625 и сл., оригиналният текст (на текст) може да бъде намерен на: http://starweb.hessen.de/cache/GVBL/1970/00041.pdf

[24] Herbert Burkert, Privacy-Data Protection: A German/European Perspective (Херберт Буркерт, Защита на личния живот и данните: немска/европейска перспектива) (без дата, приблизително 2000 г.), стр.46, може да бъде намерено на: http://www.coll.mpg.de/sites/www/files/text/burkert.pdf

[25] ОРЗД използва „natural persons" (физически лица) вместо „individuals" ((физически) лица).

[26] *„L'informatique doit être au service de chaque citoyen. ... Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques."* Пропуснатото изречение предвижда, че „[Защитата на данните] следва да се развива в рамките на международното сътрудничество".

на „зачитане на човешката личност" (*das allgemeine Persönlichkeitsrecht*), гарантирано от чл. 2, ал. 1 от Конституцията, във връзка с чл. 1, ал. 1. Конституционният съд излиза срешение в следствие на *преброяването* от 1983 г., за едно по-специфично право на „**информационно самоопределение**" (*informationelle Selbstbestimmung*).[27] Въпреки това *Bundesverfassungsgericht,* все още ясно и силно свързва това индивидуално право с по-широки, основни социални норми:[28]

> В един обществен и правен ред, в който гражданинът вече не може да знае кой какво, и кога знае за него, и в каква ситуация, е несъвместим с правото на информационно самоопределение. Човек, който се пита дали необичайното поведение се отбелязва всеки път и след това винаги се записва, използва или разпространява, ще се опитва да не привлича вниманието по този начин. Лице, което допуска, например, че участието в среща или гражданска инициатива е официално записано и може да създаде риск за него, може да реши да не упражнява съответните основни права ([както са гарантирани в] членове 8 и 9 от Конституцията). Това не само би ограничило възможностите за личностно развитие на лицето, но също така и общото благо, тъй като самоопределението е съществена предпоставка за свободно и демократично общество, което е базирано на капацитета и солидарността на неговите граждани.

Други европейски държави, макар да приемат необходимостта от защита на данните, и действително често да я включват в своите конституции, като *sui generis* право,[29] не са приели до една немската концепция за информационно самоопределение – често пъти точно защото чувстват, че тя поставя твърде голямо ударение върху аспектите на индивидуалната свобода и не достатъчно върху по-широките обществени такива.[30] Все пак, по същество, в Европа всички са съгласни, че, както Хондиус вече е посочил през 1983 г.:[31]

> Защитата на данните цели осигуряването на справедлив и разумен баланс между интересите на лицата и тези на общността [във връзка с обработването на лични данни].

Европейските държави изразяват позицията, че за да се постигне този баланс – е необходимо да се прилагат следните **регулаторни принципи**:

- Събирането и последващото използване и разкриване на лични данни следва да

---

[27] BVerfG, 15.12.1983, BVerfGE Bd. 65, S. 1 и сл. По въпроса за „информационното самоопределение", вж. § 151 и сл.

[28] *Вж.*, § 154 (наш превод).

[29] Сравни с австрийския Закон за защита на данните от 1978 г., който съдържа „конституционна" разпоредба първия си член, с която се обявява, че защитата на данните е конституционно-защитено право. Защитата на данните е изрично предвидена и в конституциите на държави, които са станали демократични по това време, като Испания (чл. 18-4), Португалия (чл. 35), Гърция (чл. 9А), Унгария (чл. 59), Литва (чл. 22), Словения (чл. 38), Словакия (чл.н 19), или които са изменили/допълнили своята конституция, така че да отрази модерното общество, като Холандия (чл. 10).

[30] Вж., напр., блога *Informationelle Selbstbestimmung - (noch) kein neues Grundrecht*, 26 октомври 2017 г., относно отказа на долната камара на Швейцарския федерален парламент (*Nationalrat*) да закрепи принципа на информационно самоопределение в швейцарската федерална конституция: https://www.humanrights.ch/de/menschenrechte-schweiz/inneres/person/datenschutz/informationelle-selbstbestimmung
В Нидерландия принципът също не е приет в закон или от съдилищата – макар че, в допълнение към това, най-висшият съд, *Hoge Raad*, е повлиян от съдебната практика на германския конституционен съд. Вж.: T. F. M. Hooghiemstra, Tekst en toelichting Wet bescherming persoonsgegevens (2001), раздел 4.3 (стр.18).

[31] Хондиус, о.с. (бележка под линия 7, по-горе), стр.108.

бъде предмет на **законова уредба** (т.е., на **обвързващи законови правила**, а не на доброволни кодекси или необвързващи насоки);[32]

- тези закони следва да бъдат **„омнибус" закони**, които по принцип се прилагат спрямо всички публични и частни юридически лица, които обработват лични данни (с изключения и изменения на тези правила и принципи, предвиждани в специални такива, както и когато това е необходимо, но винаги при зачитане на тяхната „основна същност");
- въпросният закон трябва да съдържа определени **основни съществени правила** (отразяващи **„основните" принципи на защита на данните**, разглеждани в следващото заглавие) и да представя на субектите на данни **важни индивидуални права**; и
- прилагането на тези закони следва да се следи от **специални надзорни органи** (обичайно наричани **органи по защита на данните** или **ОЗД**).

1.2 Първите закони, принципи и международни инструменти в областта на защитата на данните[33]

1.2.1 Първите закони в областта на защитата на данните

„Западна Европа е люлката на защитата на данните"[34]

Както беше посочено, първият закон за защита на данните в света е ***Datenschutzgesetz* на германската провинция Хесен, приет през септември 1970 г.**[35] Този закон въвежда и първия независим орган за защита на данните, само за публичния сектор и с ограничени правомощия за посредничество, а не заправоприлагане).

Законът за защита на данните на Хесен е последван в Европа, през това десетилетие, от приемането на национални (действащи в цялата държава) закони за защита на данните в **Швеция (1973 г.)**, първият **германски Федерален закон за защита на данните (края на 1977 г.)** (който обхваща обработването на лични данни от федералните агенции и от

---

[32] Сравни тълкуването на концепцията за „право" в Европейската конвенция за правата на човека (по-специално Членове 8 – 11) от Европейския съд по правата на човека.

[33] За исторически подробности, с особен акцент върху изготвянето успоредно с Насоките на ОИСР от 1980 г. и Конвенцията на защита на данните на Съвета на Европа от 1981 г., и върху вече появяващите се по това време разлики във възгледите между Европа и САЩ, вж.: Фриц Хондиус, о.с. (бележка под линия 7, по-горе), стр.103 – 128, и Обяснителния меморандум към Конвенцията на Съвета на Европа, о.с. (бележка под линия 19, по-горе), параграф 14. Един много полезен обзор на историческото развитие на личния живот е предоставен в Глава 4 от актуализианата Рамка на личния живот на ОИСР, озаглавена *The evolving privacy landscape: 30 years after the OECD Privacy Guidelines (Развиващият се пейзаж на личния живот: 30 години след Насоките на ОИСР)*, която е допълнително разгледана по-долу (вж. бележка под линия 40). Прекрасен личен разказ на историята на изготвянето на Насоките на ОИСР и политиката (Европа срещу САЩ) и ангажираните лица (включително Фриц Хондиус, Louis Joinet, Стефано Родота и Спирос Симитис), е предсатвен от Майкъл Кърби в, Privacy Today: Something Old, Something New, Something Borrowed, Something Blue (Личният живот днес: Нещо старо, нещо ново, нещо назаем, нещо тъжно), Journal of Law, Information and Science (Журнал за право, информация и наука), 2017 г. 25(1), което може да бъде намерено на:
http://www.austlii.edu.au/au/journals/JlLawInfoSci/2017/1.html

[34] Хонидус, о.с. (бележка под линия 7, по-горе), стр.104, във връзка с ранните закони, отбелязани в текста.

[35] Вж. бележка под линия 23, по-горе. За повече справочни материали по историята на защитата на данните в Германия, вж.: Херберт Буркерт, о.с. (бележка под линия 24, по-горе).

частния сектор), **френският *Закон за информатиката, файловете и свободите* от 6 януари 1978 г.**, закони в **Австрия**, **Дания**[36] и **Норвегия (всички също през 1978 г.)** и **Люксембург (1979 г.)**. Въпреки че някои от тях, като германския Федерален закон, съдържат отделни правила за (федералния) частен и публичен сектор, те са все пак „омнибус" закони, тъй като правилата за двата сектора са базирани на едни и същи основни принципи и права, често извеждани от конституцията.[37]

1.2.2 Основните принципи

Законите в Европа от 70-те години на 20 век се обединяват около, все по-общо приеман (широко формулиран) **набор от „основни" принципи и права**. Те са подобни на основните принципи на *Практики за обективно информиране*, изготвени по същото време в САЩ (макар че уредбата в тях не е толкова подробна и не се съдържа в обвързващ закон).[38]

Тези основни принципи на ранните закони в Европа са на свой ред отразени в **най-ранните (необвързващи) европейски инструменти** по въпроса, издадени от Съвета на Европа (и които, на свой ред, стават базата за по-късната, обвързваща Конвенция на Съвета на Европа за защита на данните):

- Резолюция (73) 22 на Съвета на Европа от 1973 г. относно защитата на неприкосновеността на личния живот на физическите лица по отношение на електронните бази от данни в частния сектор, приета от Комитета на министрите на 26 септември 1973 г.;[39]
- Резолюция (74) 29 на Съвета на Европа от 1974 г. относно защитата на неприкосновеността на личния живот на физическите лица по отношение на електронните бази от данни в публичния сектор, приета от Комитета на министрите на 20 септември 1974 г.[40]

„Основните" принципи са признати след това в **глобални международни, но все пак необвързващи интрументи**, т.е.:

- Основните насоки на ОИСР от 1980 г. за защитата на личния живот и трансграничните потоци лични данни;[41] и

---

[36] В Дания първоначално има два закона – един за частния сектор и един за публичния сектор, приети в един и същи ден (Закони №№ 293 и 294, и двата от 8 юни 1978 г.), но все още базирани на едни и същи широки принципи. За контекст, вж. *Въведението* в: Peter Blume, Personregistrering, Copenhagen, 1991. Те остават в сила, в различни изменения, до 2000 г., когато е прието ново законодателство, което да имплементира Директивата за защита на данните на ЕО от 1995 г.

[37] Отделните държавни закони за защита на данните (Landesdatenschutzgesetze) обхващат държавните публични сектори, но се основават на същите принципи, залегнали в Конституцията

[38] Вж. подраздел 1.3.4, по-долу.

[39] Може да се намери на: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016805028 30

[40] Може да се намери на: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804d1c 51

[41] ОИСР, Препоръка на Съвета относно Основните насоки на ОСИР за защитата на личния живот и трансграничните потоци лични данни, 23 септември 1980 г., може да се намери на: https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonal data.htm

- Основните насоки на ООН относно електронната обработка на личните данни от 1989 г., приети от Общото събрание на ООН (ОС на ООН).[42]

За пълния текст на основните принципи в горепосочените четири необвързващи международни инструменти от 70те и 80-те години на 20 век, както и за *Практики за обективно информиране в САЩ през 1973 г., ние се позоваваме на връзките в бележките под линия.*.

Тук ще бъде достатъчно да се отбележи, че всички те целят да разгледат присъщия на компютрите проблем: че по своя характер те улесняват употребата на данни, включително лични данни, без ограниченията за сигурност и обработване. С други думи, всички основни принципи се стремят да предотвратят злоупотреби с лични данни, които стават много лесни с новите технологии, освен ако не бъдат проверени. В този смисъл, те остават значими.

Както са представени накратко в Насоките на ОИСР.

Принципи на ОИСР от 1980 г.

Принцип на ограничаване на събирането

Следва да има граници на събирането на лични данни и всякакви такива данни трябва да бъдат получени по законен и ясен начин и, където е уместно, със знанието или съгласието на субекта на данни.

Принцип на качество на данните

Личните данни следва да бъдат относими към целите, за които ще бъдат събирани, и – доколкото е необходимо за тези цели – следва да бъдат точни, пълни и поддържани актуални.

Принцип на посочване на целите

Целите, за които се събират лични данни, следва да бъдат посочени не по-късно от момента на събиране на данните и последващото използване, ограничено до постигането на тези цели или такива други, които не са несъвместими с тези цели и които са посочени, във всеки случай на промяна на целта.

Принцип на ограничение на използването

Личните данни не следва да бъдат разкривани, предоставяни или използвани по друг начин за цели, различни от посочените в съответствие с [предходния принцип] освен:

а) със съгласието на субекта на данни; или

За предистория, вж. Кърби, о.с. (бележка под линия 33, по-горе).
Имайте предвид, че Насоките на ОИСР бяха редактирани през 2013 г. в контекста на създаването на по-широка *Рамка на личния живот* на ОИСР, която включва и нови правила за сътрудничество в областта на прилагането на законодателството в областта на неприкосновеността на личния живот, позоваващи се на препоръката от 2007 г. по въпроса, вж.:
https://www.oecd.org/sti/ieconomy/privacy.htm
Това обаче не засяга основните принципи от 80-те години на 20 век.

[42] Организация на обединените нации, Основни насоки относно електронната обработка на личните данни, UNGA Res. 44/132, 44 UN GAOR Supp. (№ 49) at 211, UN Doc. A/44/49 (1989), могат да бъдат намерени на:
https://www1.umn.edu/humanrts/instree/q2grcpd.htm
Имайте предвид, че това е първият инструмент, признаващ нуждата от независими органи по защита на данните.

b) по силата на закона.

Принцип на обезпечаването на сигурността

Личните данни следва да бъдат защитени с разумни мерки за сигурност срещу рискове, като загуба или неразрешен достъп, унищожаване, използване, изменение или разкриване на данни.

Принцип на отвореност

Следва да е налице обща политика на отвореност по отношение на разработки, практики и политики във връзка с лични данни. Следва да бъдат на разположение средства за установяване на съществуването и характера на личните данни, и основните цели, за които същите се използват, както и самоличността и обичайното местопребиваване на администратора на данни.

Принцип на участие на субекта на данни

Субекта на данни следва да има правото:

a) да получи от администратор на данни, или по друг начин, потвърждение дали администраторът на данни има данни във връзка с него;

b) да му бъдат изпратени данни, свързани с него, в рамките на разумен срок; срещу заплащане, ако има такова, което не е прекомерно; по разумен начин; и във форма, в която директно може да ги разбере;

c) да получи мотиви, ако бъде даден отказ на подадена молба по букви а) и б) и да може да оспори този отказ; и

d) да оспори данните, свързани с него, и, ако оспорването е успешно, данните да бъдат заличени, коригирани, попълнени или изменени.

Принцип на отчетност

Администраторът на данни следва да носи отговорност за спазването на мерките, привеждащи в изпълнение посочените по-горе принципи.

Важно е да се подчертае, че принципите (във всички инструменти) следва винаги да бъдат четени и прилагани заедно: само тогава те могат да предоставят сериозна защита срещу злоупотреби с лични данни, като грешки в дигитализирани или съхранявани данни, събиране на повече данни отколкото е необходимо или съхраняването им за по-дълъг период от необходимото, използването на данни за различни цели, кражбата или разкриването на данни на други за незаконни цели, загуби на данни, неправомерен достъп до данни и т.н. и т.н.

1.2.3 Конвенцията на Съвета на Европа от 1981 за защита на данните и нейния Допълнителен протокол

Първият обвързващ международен инструмент в областта на защитата на данните е Конвенцията на Съвета на Европа от 1981 г. за защита на лицата при автоматизираната обработка на лични данни, по-известна като Конвенцията за защита на данните или „Конвенция № 108" в съответствие с номера й в поредицата от европейски договори.[43] Като Конвенция на Съвета на Европа (а не „Европейска конвенция"), Конвенцията за защита на данните е открита за ратифициране и от държави, които не са членки на Съвета на Европа, по покана (чл. 23). Към днешна дата (август 2018 г.), Конвенцията е ратифицирана от всички 47 държави-членки на Съвета на Европа и от шест държави

[43] Пълно наименование: Съвет на Европа, Конвенция за защита на лицата при автоматизираната обработка на лични данни, открита за подписване в Страсбург на 28 януари 1981 г., CETS № 108, може да бъде намерена на: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37

извън Европа (Уругвай [2013 г.], Мавриций [2016 г.], Сенегал [2016 г.], Тунис [2017 г.], Кабо Верде и Мексико [2018 г.]).[44] Още две държави извън Европа бяха поканени да се присъединят към Конвенцията: Аржентина и Буркина Фасо.[45] През 2001 г., Конвенцията беше разширена с Допълнителен протокол.[46]

Конвенцията от 1981 г. и този Допълнителен протокол са описани накратко по-долу в минало време, тъй като съвсем скоро, през 2018 г., те бяха основно изменени („модернизирани") в още един протокол, както е обсъдено в раздел 1.3, по-долу. Трябва обаче да бъде подчертано, че редактираната („осъвременена")_Конвенция" ще се прилага само спрямо тези държави-членки, които са се присъедини към нея: за другите продължава да се прилага текстът от 1981 г. (четен заедно с Допълнителния протокол от 2001 г., както е приложим).

Като обвързващ международен инструмент, Конвенцията от 1981 г. (за разлика от по-ранните необвързващи инструменти) успешно включи по-точни правни **определения** на основните понятия в закона за защита на данните: „**лични данни**", „**администратор**" и „**обработване**" (въпреки че в по-късни обвързващи инструменти същите бяха разширявани и допълвани) (чл. 2).

Основните принципи за защита на данните, разгледани по-горе – **Принципът на ограничаване на събирането**, **Принципът на качество на данните**, **Принципът на посочване на целта** и **Принципът на ограничение на използването** – бяха зададени в чл. 5 от Конвенцията от 1981 г. (без да се използват тези понятия: Конвенцията изброява тези принципи заедно под заглавието „*Качество на данните* "). **Принцият за защита на данните** (наричан в Конвенцията *Принцип на обезпечаването на сигурността*) беше формулиран в чл. 7; а **Принципите на откритост и участие на лицата** бяха посочени в чл. 8 (под заглавието „*Допълнителни гаранции за субекта на данни*").[47]

Конвенцията добавя към тях специален член за обработването на „**специални категории данни**", т.е. „*личните данни, които разкриват расов произход, политически възгледи, религиозни или други убеждения, както и личните данни относно здравето или сексуалния живот*" и „*личните данни, свързани с осъдителни присъди*" (чл. 6). Предвижда се, че тези данни – общо наричани „**чувствителни данни**"

---

[44] Вж.: https://www.coe.int/en/web/conventions/search-on-treaties/-/conventions/treaty/108/signatures?p_auth=qsJbzlEi

[45] *Вж*.

[46] Пълно наименование: Съвет на Европа, Допълнителен протокол към Конвенцията за защита на лицата при автоматизираната обработка на лични данни по отношение на надзорните органи и трансграничните потоци от данни, открит за подписване в Страсбург на 8 ноември 2001 г., CETS № 181, може да бъде намерен на: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680080626
Допълнителният протокол е ратифициран от 36 от 47-те държави членки на Съвета на Европа и от шест държави, които не са членки (Кабо Верде, Мавриций, Мексико, Сенегал, Тунис и Уругвай). Буркина Фасо е поканена да се присъедини. Вж.: https://www.coe.int/en/web/conventions/search-on-treaties/-/conventions/treaty/181/signatures?p_auth=yDDCP83k

[47] Тъй като приложението на основните принципи представлява основната мярка за защита на лицата: правата на субектите на данни са в допълнение към тях, тъй като те позволяват повече контрол от страна на лицата, в отделни случаи.

– "*не могат да се обработват автоматизирано, освен ако вътрешното право гарантира подходяща защита*".

Бележка: Нуждата от специални правила за определени типове данни беше предмет на разгорещени дебати към онзи момент. Някои, включително Симитис, считаха, че всякакви данни могат да бъдат чувствителни в зависимост от контекста, докато някои от изброените данни биха могли да бъдат безвредни в други контексти. Други считаха, че трябва да бъдат регулирани само чувствителните данни, тъй като те са по същината си опасни и биха могли да доведат до дискриминация. Накрая надделя предложението, направено от Луис Джойнет, френският представител и председател на комитета на Съвета на Европа, отговарящ за изготвянето,[48] и всички лични данни бяха регулирани с по-високо ниво на защита за тези чувствителни данни.

В същото време, Конвенция позволи на държавите членки да приемат **изключения и ограничения** по отношение на повечето изисквания на Конвенцията (но не и по отношение на изискванията за сигурност на данните), за да защитят „***държавната сигурност, обществената безопасност, паричните интереси на държавата, борбата с престъпленията***", „***субекта на данни, или правата и свободите на другите***", при условие че отклонението беше „предвидено от ***правото*** на Страната" и „представлява ***необходима и пропорционална*** мярка в демократичното общество" за защита на тези интереси (чл. 9, пар. 2).[49]

Освен че дава правна база на основните принципи на защита на данните (с допълнението на специалните правила относно чувствителни данни) и правата на субектите на данни, Конвенцията от 1981 г. потвърди и две от другите горепосочени европейски **регулаторни изисквания**:

- Тя изискваше от държавите-членки да прилагат разпоредбите ѝ в **обвързващи законови норми**. Те могат да бъдат под формата на законови, подзаконови или административни разпоредби и могат да бъдат допълнени с необвързващи насоки или кодекси, но самите основни правила трябваше да бъдат под формата на „обвързващи мерки".[50]
- Тя изискваше от държавите-членки да прилагат широко своите закони , **спрямо (всички) „автоматизираните регистри с лични данни и автоматизираната**

---

[48] До оттеглянето си Луис Джойнет е висш френски съдия, който е бил член на *ad hoc* комисията по изготвянето на френския закон за защита на данните от 1978 г. преди да стане първият директор на френския орган за защита на данните (CNIL). Той става много изтъкнат френски представител в Комитета по правата на човека на ООН и в това си качество отговаря за изготвянето на Насоките на ООН (бележка под линия 41, по-горе). Вж.:
https://fr.wikipedia.org/wiki/Louis_Joinet
http://www.liberation.fr/societe/2013/12/18/louis-joinet-le-hessel-de-la-justice_967496

[49] В правото на ЕКПЧ, изискването за съразмерност се чете в изрично предвиденото изискване за необходимост (в демократичното общество), докато в правото на ЕС – по-специално в Хартата на основните права (ХОП) на ЕС – двете концепции се разглеждат като отделни (макар и все пак тясно свързани) принципи: сравни чл. 52 от ХОП.

[50] Обяснителен меморандум към Конвенцията на Съвета на Европа, о.с. (бележка под линия 19, по-горе), пар. 39.

> **обработка на лични данни в обществения и частния сектор”** (чл. 3, пар. 1). С други думи, тя изискваше приемането на **„омнибус” закони**.[51]

Въпреки това Конвенцията от 1981 г. все още не е изисквала от страните, участващи в нея, да създадат независим орган за защита на данните.. Също така тя все още не е разгледала въпрос, който скоро става известен в светлината на непрекъснато нарастващите трансгранични потоци от данни: **необходимостта да се ограничат тези трансгранични потоци**, за да се предотврати заобикалянето на съществените правила и отричане на решаващи права на субекта на данни, като се налагат правила, с които да се гарантира, че защитата би продължила да се предоставя и след като данните напуснат територията на държава с подходящи закони за защита на данните.

Вместо това, Конвенцията от 1981 г. просто предвижда, че страните по нея:

> не може единствено с цел защита на личния живот да забрани или да изисква специално разрешение за трансграничните потоци от лични данни, които преминават на територията на друга страна (чл. 12, пар. 2) –
>
> освен ако правните разпоредби на въпросната държава – страна по нея предоставят по-строга защита за съответната категория данни или предаването им се извършва на територията на другата страна по конвенцията с намерението за заобикаляне на законите на първата страна по конвенцията (чл. 12, пар. 3).

С други думи, Конвенцията от 1981 г. не урежда въпроса за лични данни, предавани към държави, които не са страна по Конвенцията.

Накрая може да бъде отбелязано, че Конвенцията се прилагаше само за „автоматизираните регистри с лични данни и автоматизираната обработка на лични данни” (чл. 3, пар.ф 1, вж. също чл. 1). С други думи, **досиета**, включително „структурирани досиета”, все още не бяха предмет на нейните разпоредби (макар че държавите – страни по конвенцията биха могли да изберат да разширят приложението на Конвенцията спрямо тези досиета (регистри): чл. 3, пар. 2, б. „c“)).

Два от недостатъците бяха коригирани в Допълнителния протокол по отношение на надзорните органи и трансграничните потоци от данни, приет през 2001 г. (вече споменат),[52] който, както показва заглавието, изисква създаването на **независими органи по защита на данните с правомощия за разследване и намеса, и за образуване на съдебни производства** (чл. 1) и налагането на **принципна забрана на предаването на лични данни в държава, която не осигурява „достатъчно ниво на защита ”** (чл. 2). Допълнителният протокол беше приет, за да приведе режима в Конвенцията в съответствие с режима по действащата към онзи момент Директива за защита на данните на ЕО от 1995 г., разгледана в 1.3, по-долу.

Съвсем скоро, през май 2018 г., Конвенцията от 1981 г. беше допълнително „**модернизирана**”, за да се приведе в съответствие с по-новото право на ЕС в областта на защитата на данните и общото (глобално) развитие на защитата на данните, както е допълнително разгледано в 1.4.3, по-долу.

---

[51] Това е при условията на уговорката, че всяка държава членка може да обяви, „че тя няма да прилага тази конвенция към дадени категории автоматизирани регистри с лични данни” (чл. 3, пар. 2, б. „a“).

[52] Вж. бележка под линия 45, по-горе.

В рамките на Съвета на Европа, въпросите на защитата на данните са допълнително разгледани от редица органи, в това число Парламентарната асамблея на Съвета на Европа (ПАСЕ), Консултативен комитет, известен като „T-PD", създаден с Конвенция № 108 – който носи основна отговорност за ежедневното наблюдение на свързаните със защитата на данните събития и за изработването на проект на секторни и други насоки и препоръки в тази област, и Комитета на министрите на Съвета на Европа (КнМ или КМ), който след това приема по-специално тези решения. Между тях, те са издали много становища, препоръки и изследвания в областта – винаги по отношение на Конвенцията.[53]

В допълнение към това, налице е взаимодействие между Конвенцията за защита на данните и Европейската конвенция за правата на човека, като Европейският съд по правата на човека все повече взема предвид Конвенцията за защита на данните и горепосочените видове документи в своето собствено тълкуване на член 8 от Конвенция за правата на човека (която гарантира правото на личен живот); докато ПАСЕ, Консултативният комитет и Комитетът на министрите, на свой ред, използват практиката на Съда в работата си в тази област.[54]

1.3 Закон за защита на данните на Европейската общност през 90-те години на двадесети век и началото на първото десетилетие на двадесет и първи век.

1.3.1 Защита на данните в Европейската общност.

Контекст

За известен период в Европейската общност (както се наричаше по това време ЕС)[55] се считаше, че Конвенцията за защита на данните на Съвета на Европа от 1981 г. предоставя достатъчна защита в тази област. Към края на това десетилетие обаче стана ясно, че Конвенцията не е довела до цялостна или напълно хармонизирана защита на личните данни в Общността: до септември 1990 г. Конвенцията беше ратифицирана само от седем държави членки на Европейската общност (една от които все още не беше приела

---

[53] Вж.:
http://website-pace.net/en_GB/web/apce/documents (документи на ПАСЕ) Имайте предвид, че те обхващат много повече въпроси, а не само защита на данните – но те могат да бъдат търсени с термина „защита на данните".
https://www.coe.int/t/dghl/standardsetting/dataprotection/Documents_TPD_en.asp (документи на T-PDч);
https://www.coe.int/t/dghl/standardsetting/dataprotection/legal_instruments_en.asp (документи на КнМ във връзка със защитата на данните).

[54] Вж. Информационен лист – защита на личните данни на ЕСПЧ (бележка под линия 13, по-горе) и *Приложение 1 – Юриспруденция* към работен документ на „Работната група по член 29" на ЕС, Работен документ 01/2016 относно обосноваването на намесата в основните права на личен живот и защита на данните чрез мерки за наблюдение при предаване на лични данни (Европейски съществени гаранции) (WP237), приет на 13 април 2016 г., който изброява 15 важни решения на ЕСПЧ, имащи отношение към защитата на данните (и пет такива на Съда на ЕС), намиращ се на:
http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp237_en.pdf

[55] По времето на въвеждането на пакета с предложения на Комисията, който се разглежда в тази част (септември 1990 г.), Комисията все още официално се наричаше "Комисия на Европейските общности" (мн.ч.). Терминът "Европейска общност" (ед. ч.) започна да се прилага едва през 1992 г. по силата на Маастрихтския договор, докато през 2009 г. не влезе в сила Лисабонският договор. За прегледност обаче в настоящия раздел като цяло ще използваме "Европейска общност", а в следващия раздел 1.4., както и във втора и трета част – "Европейски съюз".

съответното законодателство), а законите в тези държави членки се различаваха значително във важни аспекти.[56] По това време в Италия имаше закон за защита на данните само по отношение на работниците, Испания нямаше "омнибус" закон, макар защитата на данните да се посочваше в конституцията на страната като основно право, и т.н.

Тези различия бяха в противоречие с целта на Европейската общност в този момент, да хармонизира всички правила и закони с цел да улесни отварянето на вътрешния пазар и свободното движение на стоки, услуги, капитали и хора, което той предполагаше. По-конкретно, на състоялата се през 1989 г. международна конференция на органите по защита на данните в Берлин, Европейската комисия уведоми събралите се представители, че правилата за телекомуникационния сектор трябва да се хармонизират. Това показа, че се налага всички държави членки също да имат добре прилагано, строго законодателство за защита на данните.[57]

Ето защо, в отговор на този призив от страна на европейските органи по защита на данните, на следващата година, през септември 1990 г. – Европейската комисия предложи амбициозен, пакет от предложения, които целяха да се защитят личните данни чрез „Първия стълб" на ЕО[58]. Пакетът включваше предложения за две директиви,

---

[56] Комисия на Европейските общности, Съобщение за защитата на индивидите във връзка с обработването на лични данни в Общността и сигурността на информацията, COM(90) 314 final – SYN287 и 288, Брюксел, 13 септември 1990 г., *Въведение*. Пълният документ е наличен онлайн в превъзходния архив на Центъра по интелектуална собственост и информационно право при Кеймбриджкия университет, на:
https://resources.law.cam.ac.uk/cipil/travaux/data_protection/3%2013%20September%201990%20Communication.pdf.
Вж. по-специално параграфи 6 – 8.

[57] На конференцията в Берлин Спирос Симитис, комисар, отговарящ за защита на данните за германската провинция Хесен (и инициатор на първия закон за защита на данните в света в тази държава) публично призова Жак Фове, тогавашния председател на френския орган за защита на данните CNIL (а преди това директор на вестник "*Льо Монд*") да пише до своя дългогодишен приятел Жак Делор, по това време председател на тогавашната Европейската комисия, да инициира хармонизиране на законодателството за защита на данните в ЕО.

[58] Договорът за Европейския съюз, подписан в Маастрихт на 7 февруари 1992 г. („Маастрихтски договор"), предвиждаше тристълбова структура под един фронт. Първият стълб е съставен от първоначалната Европейска икономическа общност (ЕИО), Европейската общност за въглища и стомана (ECSC) и Европейската общност за атомна енергия (ЕАЕС) (въпреки че всеки от тях е запазила своята юридическа правосубектност) и впоследствие обхваща създадения единен пазар през 1993 г. Вторият и третият стълб обхващаха съответно Общата външна политика и политика на сигурност (ОВППС) и сътрудничеството в областта на правосъдието и вътрешните работи (ПВР). Стълбовете бяха официално премахнати от Договора от Лисабон, но все още се издават отделни инструменти за отделните области (вж. Обсъждането на обхвата на ОРЗД в част втора, раздел 2.3, по-долу). Вижте уебсайта на изследователския център CVCE на Люксембург, посветен на историческите събития в процеса на европейска интеграция (1945 - 2014 г.), по-специално страницата на „Първия стълб на Европейския съюз:

https://www.cvce.eu/en/education/unit-content/-/unit/02bb76df-d066-4c08-a58a-d4686a3e68ff/4ee15c10-5bdf-43b1-9b5f-2553d5a41274

Директивата за защита на данните от 1995 г. (както и другите директиви, обсъдени в настоящия раздел) беше (и бяша) издадена по времето, когато Първият стълб все още беше в сила, и бяха издадени само за този стълб. Мерките за защита на данните в другите два стълба са отбелязани накратко в подраздели 1.3.4 и 1.3.5 по-долу, а правилата за защита на данните за самите институции на ЕС са разгледани накратко в подраздел 1.3.6.

изготвени съгласно „Първия стълб“ а именно:[59]

- **обща директива на ЕО** *“относно защитата на лицата във връзка с обработването на лични данни”* – която, след продължителен законодателен процес, се превърна в главната директива на ЕО за защита на данните, Директива 95/46/ЕО, която се разглежда в 1.3.2 по-долу; и
- предложение за **Директива на ЕО** “*относно защитата на лични данни в контекста на публичните цифрови телекомуникационни мрежи, в частност цифровата мрежа за интегрирани услуги (ISDN) и публичните цифрови мобилни мрежи*” – впоследствие станала Директива за защита на данните в телекомуникационния сектор, Директива 97/66/ЕО, приета през декември 1997 г., впоследствие заменена от Директива 2002/58/ЕО, т.нар. “директива за правото на неприкосновеност на личния живот и електронни комуникации, която се разглежда в 1.3.3 по-долу;

Преди да разгледаме тези две директиви, важно е да отбележим естеството и присъщите ограничения на такъв тип инструменти.

Естество и ограничения на директивите на ЕО

При разглеждането на основните инструменти на ЕС за защита на данните и конкретно двете гореспоменати директиви за защита на данните, трябва да се имат предвид три неща. Първо, всички правни инструменти на ЕС (или, по-рано: на ЕО) по естеството си се

---

[59] Комисия на Европейските общности, Съобщение относно защитата на индивидите във връзка с обработването на лични данни в Общността и информационната сигурност (бележка под линия 55 по-горе). Пакетът съдържаше още четири предложения, а именно:

- проект за **резолюция** на представителите на държавите членки, която би разширила приложението на принципите на общата директива до архиви, съхранявани от публичните органи, към които главната Директива за защита на данните сама по себе си не важеше – което така и не беше прието по същество, но може да се разглежда като генезиса на правилата за защита на данните по отношение на правоприлагащите органи и при съдебни въпроси, в най-ново време достигайки кулминацията си в Директивата за защита на данните от страна на правоприлагащите органи (Директива (ЕС) 2016/680 (не се разглежда в настоящия наръчник: вж. бележка в карето “*За този наръчник*” на стр. 1 по-горе);
- проект за **декларация** на Комисията относно приложението на стандартите за защита на данните, зададени в главната Директива за защита на данните, към архиви, съхранявани от самите институции на Общността – което в крайна сметка доведе до Регламент (ЕО) 45/2001 (*пак там*);
- **препоръка за решение на Съвета** по отношение на присъединяването на Европейската общност към Конвенцията за защита на данните на Съвета на Европа – което до момента не се е случило, защото ЕС, който не е държава членка, няма как да се присъедини към Конвенцията – но това се коригира в “Осъвременената” конвенция за защита на данните на Съвета на Европа, разгледана по-долу в 1.4.3, и
- **предложение за решение на Съвета** за приемане на план за действие по отношение на информационната безопасност – което доведе до пространни действия в тази област от страна на ЕС, включително създаването на Агенцията на Европейския съюз за мрежова и информационна сигурност ENISA през 2004 г. и приемането на подробна стратегия за информационна и кибер сигурност, които не се разглеждат в този наръчник по-подробно, но информация за тях може да се намери тук:
  https://www.enisa.europa.eu/about-enisa
  https://ec.europa.eu/digital-single-market/en/cyber-security

За отделните предложения в Съобщението на Комисията (както и за други документи, свързани със законодателния процес), вж. връзките на тази страница:
https://www.cipil.law.cam.ac.uk/projectseuropean-travaux/data-protection-directive

ограничават до въпроси от обхвата на правото на ЕС (или, по-рано: на ЕО). Определени въпроси, по-специално дейностите на държавите членки, свързани с **национална сигурност**, се намират (почти) напълно извън обхвата на правото на ЕС (или по-рано: на ЕО)[60] и никой правен инструмент на ЕС (или на ЕО) (включително тези директиви – както и самият ОРЗД или каквито и да било бъдещи правила на ЕС за защита на данните под каквато и да било форма) не е приложим към такива дейности. Това е изрично потвърдено в директивите (и в ОРЗД): виж чл. 3(2) от Директивата за защита на данните от 1995 г. и чл. 1(3) от Директивата за правото на неприкосновеност на личния живот и електронни комуникации (и чл. 2(2)(а) в ОРЗД).[61]

Второ, директивите на ЕО, които се разглеждат по-долу, в качеството си на директиви на ЕО се ограничаваха до въпроси от така наречения **Първия стълб**[62] и поради естество си на директиви на ЕО не се прилагаха към дейности в рамките на Втория или Третия стълб, по отношение на които бяха изработени отделни инструменти за защита на данните, накратко споменати в раздели 1.3.4 и 1.3.5 по-долу, но които не са предмет на това първо издание на този наръчник. Достатъчно е да отбележим, че *всякакво предаване или предоставяне на лични данни* от страна на структури, подлежащи на директивите (както структури от частния сектор, така и публични органи, осъществяващи дейности, които са обект на правото на Първия стълб (на ЕО)) към каквито и да е правоприлагащи органи или агенции за национална сигурност беше (и, що се отнася до директивата за правото на неприкосновеност на личния живот и електронни комуникации, все още е) подчинено на тези инструменти (тъй като по смисъла на тези директиви такова разкриване представлява "обработване" от страна на тези структури), дори ако *придобиването (получаването) и по-нататъшното обработване* на разкритите данни е подчинено на други инструменти (вкл. до неотдавна, специално по отношение на правоприлагането, на Рамковото решение на Съвета 2008/977/ПВР и понастоящем на Директивата за защита на данните при правоприлагането от 2016 г.) или изобщо не е обект на правото на ЕС (или ЕО) (т.е., ако е извършено от агенции за национална сигурност).[63]

Трето, директивите по определение не се прилагат пряко в правните системи на държавите членки, те нямат "директен ефект". Държавите членки трябва да **"транспонират"** разпоредбите им в националното законодателство – като при това

---

[60] Казваме "(почти) напълно" поради две причини. Първо, става все по-трудно, особено във връзка с тероризма (само по себе си доста зле дефинирано понятие) да бъдат разграничени действия от страна на държавите във връзка с тяхната национална сигурност от действия, предприети по силата на наказателното право или правото, свързано с опазване на "международната сигурност", "обществената сигурност" или "обществения ред" – като всички тези въпроси в момента са, в по-голяма или в по-малка степен, поне частично обект на правото на ЕС. Второ, дори ако действията на агенциите на държавите членки, които отговарят за националната сигурност са извън обхвата на правото на ЕС, то тясно свързани дейности на агенциите за правоприлагане и частните структури (например събиране и разкриване на данни от банките по силата на законодателството срещу изпирането на пари или събирано и разкриване на записите на имената на пътниците от страна на авиолиниите пред агенциите на държавите членки) често са обект на правото на ЕС (по-конкретно, на правото на ЕС за защитата на данните). Вж. втора точка от текста.

[61] Относно ограниченията на обхвата на Общия регламент относно защитата на данните на ЕС, вж. втора част, раздел 2.3

[62] Вижте бележка под линия 67 по-долу.

[63] Относно подобни въпроси, повдигнати във връзка с Общия регламент относно защитата на данните на ЕС, вж. втора част, по-конкретно раздел 2.2, *Статут и подход на Общия регламент относно защитата на данните: хармонизиране с гъвкавост*.

държавите членки имаха (и все още имат) значителна **свобода на действие**. Определено такъв беше случаят с двете директиви, разгледани по-долу – и, както ще отбележим във втора част, това доведе до значителни различия между националните законодателства на държавите членки при имплементирането (“транспонирането”) на тези директиви; това всъщност беше една от главните причини да се избере формата на (директно приложим) регламент, който да наследи Директивата за защита на данните от 1995 г. – ОРЗД (макар, както ще видим в тази част, Регламентът също да позволява различия при приложението си в много отношения.[64]

1.3.2 Главна директива на ЕО за защита на данните от 1995 г.

Общи положения

Както отбелязахме по-горе, в началото на 90-те години на двадесети век Комисията на Европейските общности (както тогава беше известна)[65] беше изправена пред дилема. От една страна, защитата на данните все повече се разпознаваше като законово право за ЕС и бяха необходими ограничения при употребата и потоците на лични данни.[66] От друга страна, развитието на **вътрешен пазар** в рамките на т.нар. “Първи стълб” на Общността[67] изискваше свободното движение на данни, вкл. лични данни, във връзка с

---

[64] Вж. втора част, по-конкретно раздел 2.2, *Статут и подход на Общия регламент относно защитата на данните: хармонизиране с гъвкавост*.

[65] Вж. бележка под линия 54 по-горе.

[66] Защитата на данните е понастоящем изрично припозната, като право *sui generis* в чл. 8 от Хартата на основните права (ХОП) на ЕС, отделно от (макар, разбира се, да е много тясно свързана с) правото на личен и семеен живот и неприкосновеност на личния живот, защита по силата на чл. 7. ХОП е само обявена през 2000 г., но не влиза изцяло в правна сила до влизането в сила на Лисабонския договор на 1 декември 2009 г. Вж.:
https://en.wikipedia.org/wiki/Charter_of_Fundamental_Rights_of_the_European_Union
С други думи, Хартата все още нямаше пълна правна сила по времето на предлагане на директивите. Но дори преди написването на Хартата или влизането ѝ в правна сила основните права вече бяха придобили конституционен статут в Европейските общности, вж.: Франческа Ферaро и Хесус Кармона, Основни права в Европейския съюз – ролята на Хартата след Лисабонския договор (Fundamental Rights in the European Union – The role of the Charter after the Lisbon Treaty), Служба за научни изследвания на Европейския парламент, Брюксел, март 2015 г., раздел 2*: Основни права в ЕС преди Лисабонския договор*, налична на:
http://www.europarl.europa.eu/RegData/etudes/IDAN/2015/554168/EPRS_IDA(2015)554168_EN.pdf
Следователно съставителите на Директивата за защита на данните от 1995 г. правилно поставяли в основата на предложения инструмент като основно право защитата на личните данни.

[67] Договорът за Европейския съюз, подписан в Маастрихт на 7 февруари 1992 г. (“Маастрихтския договор”) предвиди структура с три стълба под обща “шапка”. Първият стълб се състоеше от първоначалната Европейска икономическа общност (ЕИО), Европейската общност за въглища и стомана (ЕОВС) и Европейската общност за атомна енергия (ЕОАЕ) (въпреки че всяка от тях запази собствена правосубектност). Вторият и Третият стълб обхващаха съответно Общата външна политика и политика за сигурност (ОВППС) и сътрудничество в областите на правосъдието и вътрешните работи (ПВР). Стълбовете бяха официално премахнати с Лисабонския договор, но все още се създават отделни инструменти за отделни области (сравни с обсъждането за обхвата на ОРЗД във втора част, раздел 2.3 по-долу). Вж. на уебсайта на изследователския Виртуален център за знания за Европа (CVCE) на Люксембургския университет Исторически събития при процеса на европейска интеграция (Historical events in the European integration process) (1945 – 2014), в частност страницата за “*Първия стълб на Европейския съюз*”:
https://www.cvce.eu/en/education/unit-content/-/unit/02bb76df-d066-4c08-a58a-d4686a3e68ff/4ee15c10-5bdf-43b1-9b5f-2553d5a41274
Директивата за защита на данните от 1995 г. (както и другите директиви, разгледани в настоящия раздел) беше (бяха) всичките издадени по времето, когато Първият стълб все още съществуваше и бяха издадени само по отношение на този стълб.

търговските транзакции. За да намери решение на тази ситуация, Комисията предложи да бъдат приети две директиви по отношение на Първия стълб. В този раздел ще разгледаме основната директива, Директива 95/46/ЕО.[68]

Цели на Директивата за защита на данните от 1995 г.:

С оглед на създалата се дилема Европейската общност включи в Директивата две свързани цели, а именно: да се осигури **високо ниво на защита на данните** в рамките на тогавашния "Първи стълб" на Общността ("високо ниво", тъй като цел на Директивата беше да защити правата на човека) като *conditio sine qua non* (абсолютно условие) за **свободното движение на лични данни** в рамките на главния елемент на този стълб, зараждащият се **вътрешен пазар** (виж чл. 1 на Директивата и съображение 10 и особено 11).

Ключови характеристики на Директивата за защита на данните от 1995 г.:

По-долу са изложени **ключовите характеристики** на Директивата за защита на данните от 1995 г. в сравнение с Конвенцията от 1981 г. (NB: Новите характеристики или характеристиките, съдържащи важни нови елементи, са маркирани *НОВО – макар да следва да се отбележи, че те често надграждат върху предложения, които вече са били направени или споменати в съображенията към Конвенцията). Описанието на тези ключови характеристики на Директивата от 1995 г. цели да даде общ поглед върху някои основни компоненти в подхода към защитата на данните в ЕС, потвърдени от ОРЗД от 2016 г. и съответно обяснени тук, докато ключовите нови характеристики, въведени с Регламента, са описани в част две. Най-важните нововъведения бяха изискването на независими органи за защита на данните и мерки за осигуряване на постоянна защита на данните, прехвърлени в трети страни (т.е. държави извън ЕС / ЕИП).

*НОВО Определения:

Директивата разшири обхвата на основните **определения** в Конвенцията от 1981 г., като прибавя нови. По-конкретно тя пояснява (в рамките на определението за "лични данни"), кога следва лицата да се считат за лица, които "***могат да бъдат идентифицирани***" (от "когото и да било") и кога ръчен набор от данни следва да се счита за достатъчно "***структуриран***", за да бъде обект на Директивата. В обхвата на Директивата са включени "[структурирани] ръчни досиета", с цел да се избегне заобикалянето на правилата ѝ чрез употребата на такива досиета.

Директивата дава ***донякъде модифицирано определение за "администратор"*** и добавя ***широкообхватно определение за "обработване на лични данни"***, както и определения за понятията "***обработващ***", "***трета страна***" и "***получател***". Добавя и определение за "***съгласие на субекта на данни***", в което фактически се задават условията, които трябва да бъдат изпълнени преди да може каквото и да било съгласие, за което се претендира, да се счита за валидно: за да бъде валидно, съгласието трябва

[68] Пълно заглавие: Директива 95/46/ЕО на Европейския парламент и на Съвета от 24 октомври 1995 г. за защита на физическите лица при обработването на лични данни и за свободното движение на тези данни, ОВ L281, 23.11.1995 г., стр. 31 – 50, налична на: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN

да бъде "***свободно дадено, конкретно и информирано***" и да бъде ***изразено*** по някакъв начин (чл. 2(з)).[69]

Докато Конвенцията от 1981 г. съдържаше четири определения, Директивата предоставя осем (или девет, ако броим отделно определението за "лице, което може да бъде идентифицирано", поставено в рамките на определението за "лични данни").

Принципи при защитата на данните:

Като цяло, Директивата повтаря принципите при **защитата на данните** на Конвенцията от 1981 г.**,** но с някои **разяснения**, включително че ***целта,*** с която личните данни ще се обработват, трябва да бъде не само "*конкретна*" и "*законна*" (което вече беше предвидено в чл. 5(б) на Конвенцията), но също "*изрична*" (чл. 6(1) (б)), а що се отнася до "*[по-]нататъшното обработване на данни за исторически, статистически или научни цели*" (виж чл. 6 (1)(в) и (д)).

*НОВО Правни основания за обработване

С цел постигането на по-добро хармонизиране на законодателствата на държавите членки, Директивата от 1995 г. включи в рамките на чл. 7 като важна нова характеристика **изчерпателен списък на "критерии, при които обработването на данните е законно"** – впоследствие наречени **"правни основания" за обработване на лични данни**. Директивата позволяваше да се обработват (нечувствителни) лични данни, само ако (в резюме):

(a) субектът на данни ***недвусмислено*** е дал **съгласието** си (което, разбира се, също трябваше да бъде "***свободно, конкретно и информирано***", както и ***изразено***: чл. 2(з) по-горе); или

(b) обработването е ***необходимо*** за изпълнението на **договор**, по който субектът на данни е страна, или с оглед предприемането на стъпки по искане на субекта на данни преди встъпване в договорни отношения (например, кредитна проверка); и

(c) обработването е ***необходимо*** за изпълнението на **законово задължение** на администратора; или

(d) обработването е ***необходимо*** за защитата на **жизненоважни интереси на субекта на данни;** или

(e) обработването е ***необходимо*** за изпълнението на **задача, която се осъществява в обществен интерес или при упражняване на официалните правомощия, които са предоставени на** администратора или на трета страна, на която се разкриват данните; или

(f) обработването е ***необходимо*** за целите на **законните интереси** на администратора или на третата страна или страни, на които се разкриват данните, с изключение на случаите, когато пред тези интереси имат преимущество интереси или основни права и свободи на субекта на данни, които изискват защита по силата на чл. 1(1). [т.нар. "законни интереси" или критерий "баланс"/правно основание].

В повечето случаи обработката на нечувствителни лични данни се разрешаваше на

[69] Ако цитираме пълния текст, съгласието трябвало да има формата на "свободно изразено, конкретно и информирано **указание за волята му, чрез което субектът на данни дава израз на своето съгласие** за обработка на личните данни, които се отнасят до него".

основание на закон, във връзка с договор или със съгласието на субекта на данни, или на основание на това, че служи за легитимен интерес на администратора в случаите, когато интересите или основни права и свободи на субекта на данни на субекта на данни нямат преимущество.

В Конвенцията за защита на данните от 1981 г. не се съдържаше подобен списък.

*НОВО Специални правила при обработването на чувствителни данни

В Директивата от 1995 г. като цяло се изброяват същите **основни** "**специални категории данни**" – обикновено наричани "**чувствителни данни**", както зададените в Конвенцията от 1981 г., с малки изменения, а именно:[70]

> лични данни, разкриващи расов или *етнически* произход, политически възгледи, религиозни или *философски* убеждения, *членство в професионални съюзи*, и … данни, свързани със здравето или сексуалния живот

Но не само определя, че такива данни "*не трябва да се обработват автоматично, освен ако националното законодателство не предоставя подходящи предпазни мерки*" (Конвенция на Съвета на Европа, чл. 6), в чл. 8(1) от Директивата се и формулира **принципна забрана** за обработването на такива чувствителни данни, към която се допускат ограничен брой **изключения**. Главните изключения всъщност представляват **особено рестриктивни правни основания** за обработване на чувствителни данни. Те са (отново в резюме):

- обработване на основание на съгласие, което е не само свободно, конкретно и информирано съгласие, но и ***изрично съгласие*** на субекта на данни, освен когато националното законодателство не забранява обработването на такива данни дори със съгласието на субекта на данни при определени обстоятелства (чл. 8(2)(а));
- обработване, ***необходимо*** за изпълнението на задълженията и правата на администратора в рамките на **трудовото законодателство** (при условие, че националното законодателство предвижда " адекватна защита ") (чл. 8(2)(б));
- обработване, ***необходимо*** за да се защитят **жизненоважните интереси** на субекта на данни или друго лице, когато субектът на данни е физически или юридически неспособен да даде своето съгласие (чл. 8(2)(в));
- обработване, „извършвано в хода на законно упражняваните дейности и при подходящи мерки за защита от фондация, сдружение или какъвто и да е друг **орган с нестопанска цел с политическа, философска, религиозна или профсъюзна цел** и при условие, че обработването касае единствено ***членовете*** на органа или ***лица, които редовно контактуват с него*** във връзка с неговите цели, и че данните ***не се разкриват на трета страна*** без съгласието на субектите на данни" (чл. 8, пар. 2, б. „г“));
- обработване на (чувствителни) лични данни „които **явно са направени обществено достояние от субекта на данни**" (чл. 8, пар. 2, б. „д“), първо изречение); и
- обработване на (чувствителни) лични данни, "необходимо с цел установяване, упражняване или защита на **правни претенции**" (чл. 8, пар. 2, б. „д“), второ

[70] В Конвенцията от 1981 г. нямаше референция към „етнически" данни, говореше се за „религиозни или други убеждения" (вместо за „религиозни или философски убеждения") и членството в професионални съюзи не беше включено.

изречение).

Трябва да се отбележи фактът, че списъкът не включва критерий за "**законния интерес**" или "**баланса**": обработването на чувствителни данни *би могло, вече съгласно* Директивата, по принцип да не бъде обработвано на основание на законните интереси на администратора или на трета страна, над които интереси нямаха преимущество интереси на субекта на данни, свързани с основните му права.

Директивата обаче също така определи, че принципната забрана за обработването на чувствителни данни (да се отбележи: чувствителни данни от какъвто и да било вид) не се прилага, "*когато обработването на данни* ***е необходимо*** *за целите на* ***превантивната медицина, поставяне на медицинска диагноза****, предоставяне на* ***грижи*** *или* ***лечение,*** *или за* ***управлението на здравни служби***", при условие, че то се извършва съгласно съответното задължение за тайна (чл. 8, пар. 3). Забележете, че това се отнася към всеки вид чувствителни данни – но и при това положение, естествено, такива данни може да се използват за такива цели само, когато това е уместно (например, информация за етническия произход може да има отношение към дадени заболявания като сърповидно-клетъчна анемия; религиозните убеждения на дадено лице пък могат да имат отношение към определени начини на лечение).

Освен това, макар горните правила да бяха строги сами по себе си, Директивата съдържаше една много по-общо формулирана разпоредба (чл. 8, пар. 4), позволяваща на държавите членки да предоставят **допълнителни изключения** – т.е., да позволяват обработване на (всякакъв вид) чувствителни данни извън основанията, изброени в чл. 8, пар. 2) – чрез закон или по решение на националния надзорен орган (органа за защита на данните, "***при съображения от съществен обществен интерес***", при условие, че това подлежи на "***подходящи предпазни мерки***" – определяни от държавата членка.

Директивата също така очерта малко по-рестриктивен подход към обработването на **лични данни, свързани с наказателни присъди** (чл. 8, пар. 5) и **на национални идентификационни номера или други "идентификатор[и] с общо приложение"** (чл. 8, пар. 7) – но подробностите при регламентирането на това обработване бяха оставени на държавите членки.

По подобен начин, макар да беше по-категорична от Конвенцията от 1981 г. относно необходимостта от **баланс между защитата на данните и свободата на изразяване и информация,** Директивата остави конкретиката при намирането на този баланс отново на държавите членки (чл. 9).

*НОВО Информиране на субектите на данни

Конвенцията за защита на данните от 1981 г. зададе изискване само за някаква обща прозрачност относно "съществуването на досие с лични данни, обработвано по автоматизиран начин, основните цели на това досие, както и самоличността и обичайното местожителство или основно място на дейност на администратора на досието" (чл. 8, б. „а")).

От друга страна в членове 10 и 11 от Директивата за защита на данните от 1995 г. се посочиха подробности относно **информацията, която трябва да се предоставя от всеки администратор на субекта на данни** *по инициатива на администратора* съответно при събиране на личните данни от администратора или от трета страна. Данните, които следваше да се предоставят и в двата случая включваха ***самоличността на***

администратора и ***целите на обработването***. ***Допълнителна информация*** (вкл. информация дали събирането на данните е задължително или не; информация относно всякакво разкриване на данните) трябваше да се предоставя дотолкова, доколкото това беше необходимо за гарантиране на добросъвестно обработване (виж чл. 10, б. „в“) и 11, пар. 1, б. „в“)).

*НОВО Права на субектите на данни

Конвенцията за защита на данните от 1981 г. изискваше субектите на данни да имат право да получават **достъп** до данните си при поискване, през разумни интервали от време; право на **коригиране или заличаване** на данни, които са неточни или са обработвани в нарушение на принципите за защита на данните; и право на **правна мярка за защита**, ако упражняването на тези права не е било спазено (чл. 8, б. „б“ – „г“).

Директивата потвърди първите две права, но добави и **важни допълнителни подробности**. Потвърдено беше, че **правото на достъп** включва правото данните да бъдат “съобщени” на субекта на данни (което вече фигурираше в Конвенцията), но се добави, че това трябва да бъде направено в “*разбираема форма*” и че “всяка налична информация за ***източника*** (на данните)” също трябва да се предоставя (чл. 12, б. „а“), второ тире). Към коригирането и заличаването беше добавена опция за “***блокиране***” (макар понятието да не беше дефинирано)[71] (чл. 12, б. „б“)); и се предвиди, че всякакви поправки, блокиране или изтриване трябва да се споделят с ***трети страни***, пред които данните са били разкрити (чл. 12, б. „в“).

Бяха въведени нови права: **общо право на възражение** срещу обработването съгласно „убедителни законови основания”, „поне” в случаите на обработване във връзка със задача от обществен интерес, при упражняване на официални правомощия, или на основание на критерия “законен интерес”/ “баланс” – като възражението трябваше да се уважи, ако е “обосновано” (чл. 14, б. „а“); по-конкретно и убедително **право на възражение срещу обработването за цели на директния маркетинг** (по онова време, предимно чрез директна поща – това беше преди зараждането на интернет и изпращането на нежелана електронна поща („спам”)) – което трябваше винаги да бъде уважено, без да е необходимо субектът на данни да предоставя обосновка (чл. 14, б. „б“); и **право да не бъде подлаган на изцяло автоматизирано решение на базата на профилиране**[72], което има правни или други съществени последствия (подлежи на важни, но строго определени ***изключения***) (чл. 15). В тази връзка е важно да се отбележи, че в чл. 12, б. „а“), трето тире се посочва, че субектите на данни придобиват и **ново** право да получат (в контекста на искане за достъп) **информация относно “логиката”**, свързана с каквото и да било автоматично обработване на данни, отнасящи се до тях, “поне” при такива изцяло автоматизирани решения на базата на профилиране.

Тези права в Директивата от 1995 г., които се пренасят и засилват допълнително в ОРЗД,

---

[71] Съответстващото понятие „**ограничаване на обработването**” е определено в ОРЗД като „*маркиране на съхранявани лични данни с цел ограничаване на обработването им в бъдеще*” (чл. 4(3) ОРЗД).

[72] Пълен текст: “*решение, което има правни последици за него [субекта на данни] или го засяга съществено, и което се основава единствено на автоматизираната обработка на данни, имаща за цел да се оценяват някои лични аспекти, свързани с него, като представянето му на работа, кредитоспособност, надеждност, поведение и т.н.*”. Разпоредбата е директно взета от френския закон за защита на данните от 1978 г., чл. 2 и 3.

придобиват все по-голямо значение във връзка с вземането на решения, основаващи се на „Изкуствен интелект“.

*НОВО Поверителност и сигурност на данните

Конвенцията от 1981 г. посочваше само, че трябва да се предприемат “подходящи мерки за сигурност”, за да се защитят личните данни от “случайно или непозволено унищожаване или случайна загуба, както и срещу непозволен достъп, промяна или разпространение” (чл. 7).

Директивата значително разшири темата, като наложи, преди всичко, **задължение за поверителност** от страна на всеки, ангажиран в обработването на лични данни (чл. 16) и предвиди, че администраторът трябва да въведе “*подходящи, технически и организационни мерки, за защита на личните данни срещу случайно или неправомерно унищожаване или случайна загуба, промяна, неразрешено разкриване или достъп, в частност, когато обработването включва предаване на данните по мрежа, както и срещу всякакви други незаконни форми на обработка*” (чл. 17, пар. 1), с допълнителни подробности). Последната разпоредба е взета от германския федерален закон за защита на данните от 1977 г.

Тя предвижда и важни нови изисквания за случаите, в които администраторът ангажира обработващ, който обработва данни от негово име (на администратора), включително изискване за “*достатъчни гаранции*” по отношение на сигурността и поверителността, както и изискване за подробен писмен договор между администратора и обработващия (чл. 17, пар. 2 – 4).

*НОВО Ограничения при трансграничното предаване на данни

Както беше отбелязано в 1.2.3 по-горе, Конвенцията от 1981 г., в първоначално приетия си вид, не изискваше страните по нея да приемат **забрана за изнасяне на лични данни от тяхната територия към държава, която не осигурява подобна защита**. Тя разглежда само потоци от данни между страните по Конвенцията. Затова въвеждането на такава забрана (подлежаща на ограничен брой изключения) – чийто произход идва от френския и датския законодателен опит – стана друга важна нова характеристика на Директивата от 1995 г.

По-конкретно тя предвижда, че личните данни, които са обект на Директивата принципно могат да се предават към трети държави, осигуряващи ниво на защита, което може да се счита за “**адекватно**” по смисъла на Директивата (чл. 25, пар. 1); и че Европейската комисия ще определя (чрез така наречената “решение за адекватност”) дали това е така по отношение на определена трета държава (чл. 25, пар. 2).[73] Комисията допълнително определи “адекватността” не само по отношение на трети държави като цяло, но и по отношение на **сектори** в определени държави (например, първоначално, режимът за органите от публичния сектор в Канада), както и специалните **системи**,

[73] Терминът “адекватна защита” беше избран, защото терминът “еквивалентна” беше запазен в правото на Европейската общност (след това – на Европейския съюз) за отношения между правила на държави членки, докато, на база на международното право, тя би била “еквивалентна по действие”. Но в решението си по делото *Максимилиан Шремс срещу комисаря по защита на данните,* решение на Съда на ЕС по дело C-362/14 от 6 декември 2015 г., Съдът се произнесе, че терминът “адекватна защита” трябва да се разбира като изискващ практически “еквивалентна по същество” защита в третата държава: вж. пар. 96 от решението – но това, разбира се, стана много години след приемането на Директивата от 1995 г. (както и на Допълнителния протокол от 2001 г. към Конвенцията от 1981 г., посочен по-нататък в текста).

установени в дадени страни (например режима "*Safe Harbor*", установен от САЩ, впоследствие заменен от "*Privacy Shield*").

Принципната забрана за пренасяне към страни (или сектори в страни) без адекватна защита подлежеше на ограничен брой **изключения**, посочени в чл. 26, пар. 1 на Директивата, повечето от които бяха сходни с правните основания за обработване като цяло, а именно (в обобщен вид):

(a) субектът на данни ***недвусмислено*** е дал **съгласието** си за пренасянето (което, разбира се, също трябва да е "***свободно, конкретно и информирано***" и ***изразено***: чл. 2, б. „з", посочен по-рано); или

(b) пренасянето е ***необходимо*** за изпълнението на **договор** между администратора и субекта на данни, или с оглед предприемането на стъпки по искане на субекта на данни преди встъпване в договорни отношения (например, кредитна проверка);

(c) пренасянето е ***необходимо*** за сключването на **договор** между администратора и трета страна, като договорът се сключва в интерес на субекта на данни (например, хотелска резервация);

(d) пренасянето е ***необходимо*** или ***изискуемо по закон*** поради основания от **важен обществен интерес**, или за установяването, упражняването или защитата на **правни претенции**;

(e) пренасянето е ***необходимо*** за защитата на **жизненоважни интереси на субекта на данни**; или

(f) пренасянето е направено от **обществено достъпен регистър** (при спазване на всички общо приложими условия по отношение на достъпа до регистъра)

Освен това, държавите членки можеха да **позволяват** пренасяния, ако администраторът представи "***достатъчни гаранции***" за защита на интересите, свързани със защитата на данните и правата да субектите на данни (чл. 26, пар. 2) – например, под формата на ***ad hoc клаузи за пренасяне на данни***; също така на Комисията беше **възложено да** одобрява някои определени "***стандартни договорни клаузи***" за пренасяне на данни, които биха осигурили такава защита (чл. 26, пар. 4).

Много органи по защита на данните, както и впоследствие Работната група по член 29, разгледаха и предпазните мерки, съдържащи се в т.нар. ***Обвързващи корпоративни правила*** (ОКП), т.е., правила, изработени от международни компании или групи от компании, които регламентират вътрешните употреби и потоци на лични данни в рамките на такива компании или групи.[74] Въпреки колебанието от страна на някои други

[74] Работната група по чл. 29 се занимаваше с ОКП в цяла поредица от работни документи и препоръки, между които:

- Работен документ: пренасяне на лични данни към трети държави: прилагане на член 26 (2) от Директивата на ЕС за защита на данните към Обвързващите корпоративни правила за международно пренасяне на данни, приет от Работната група по чл. 29 на 3 юни 2003 г. (WP74);
- Работен документ, създаващ примерно заявление с контролен списък за одобрение на Обвързващи корпоративни правила, приет от Работната група по чл. 29 на 3 юни 2003 г. (WP108);
- Препоръка 1/2007 относно стандартно заявление за одобрение на Обвързващи корпоративни правила за пренасянето на лични данни, приета от Работната група по чл. 29 на 10 януари 2007 г. (WP133);
- Работен документ, създаващ таблица с елементите и принципите, които трябва да се съдържат в Обвързващите корпоративни правила, приет от Работната група по чл. 29 на 24 юни 2008 г. (WP153);
- Работен документ, създаващ рамка за структурата на Обвързващи корпоративни правила, приет от Работната група по чл. 29 на 24 юни 2008 г. (WP154);

органи по защита на данните, идеята беше официално включена в ОРЗД (както е отбелязано във част две).

NB: Както е отбелязано в 1.2.3 по-горе, изискване за "адекватност" при пренасянето на данни се въведе по отношение на Конвенцията от 1981 г. чрез Допълнителния протокол от 2001 г. към нея с цел привеждането на режима на Конвенцията в това отношение в съответствие с режима съгласно Директивата на ЕО от 1995 г. (виж чл. 2(1) от Допълнителния протокол), макар, разбира се, това да се отнасяше само до онези държави, страни по първоначалната Конвенция, които се присъединиха и към Протокола.[75]

*НОВО Кодекси за поведение (и сертифициране)

Друга нова особеност, въведена с Директивата, е посочването на **кодексите за поведение** като средство, "*допринасящо за правилното прилагане на националните разпоредби, приети от държавите членки съгласно тази Директива, като се вземат предвид конкретните особености на различните сектори*" (чл. 27, пар. 1) – въпреки че Директивата се ограничи до "насърчаване" на такива кодекси ; до изискване към държавите членки да създадат разпоредби за оценяването на ***проекти за националните кодекси*** (чл. 27, пар. 2); и до създаване на разпоредби, за да може Работната група по член 29 (РГ29, разгледана по-долу в настоящата точка) да оценява по подобен начин ***проектите за кодекси на Общността*** (чл. 27, пар. 3).

На практика само няколко такива кодекса бяха одобрени или внесени за одобрение. Първият проект за Европейски кодекс за дейността при използването на лични данни при директния маркетинг на Европейската асоциация за директен маркетинг (FEDMA) беше внесен пред Работната група по член 29 през 1998 г., но окончателната версия беше одобрена едва през 2003 г.[76] Проект за Кодекс за поведение за доставчиците на облачни услуги, разработен от работна група от отрасъла, създадена през 2013 г. и всъщност съвместно председателствана от две Генерални дирекции на ЕС (DG Connect и DG Justice), беше внесен пред РГ29 през януари 2015 г., но не беше одобрен от нея в

- Работен документ с Често задавани въпроси (FAQs), свързани с Обвързващите корпоративни правила, приет от Работната група по чл. 29 на 24 юни 2008 г., последно преработен и приет на 8 април 2009 г. (WP155);
- Работен документ 02/2012, определящ таблица с елементите и принципите, което трябва да се намират в Обвързващите корпоративни правила за обработващия, приет на 6 юни 2012 г. (WP195).

Вж. също:

- Становище 02/2014 по справочен документ за Обвързващи корпоративни правила, внасяни пред националните органи по защита на данните в ЕС и Трансгранични правила за защита на неприкосновеността на личния живот, внасяни пред агентите по отчетността за трансграничните правила за неприкосновеност на личния живот (CBPR) в рамките на Азиатско-тихоокеанското икономическо сътрудничество (APEC), от 27 февруари 2014 г. (WP212).

[75] Вж. бележка под линия 45 по-горе. Следва да се отбележи, че не е ясно дали терминът "адекватни" в този член от Протокола може или следва да се разбира в съответствие с решението по делото *Шремс* (бележка под линия 70 горе) – и съответно дали Допълнителният протокол в действителност е постигнал тази цел.

[76] Текст на кодекса:
https://www.fedma.org/wp-content/uploads/2017/06/FEDMACodeEN.pdf
Становище 3/2003 на Работна група по член 29 за Европейския кодекс на поведение на FEDMA относно използването на лични данни при директния маркетинг, с което се одобрява кодекса (Работен документ 77, приет на 13 юни 2003 г.), е налично на:
http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp77_en.pdf

рамките на становището й по проекта, и остава "незавършен".[77]

Макар да не е изрично споменато в Директивата, Европейската комисия насърчи и създаването на схеми за сертифициране.[78] Тя предостави начално финансиране на група органи и експерти по защита на данните, ръководени от органа по защита на данните на Шлезвиг-Холщайн, с цел да се създаде **схема за сертифициране за целия Европейски съюз –(EuroPriSe)**, по която да се оценяват продукти и услуги, свързани с използването на лични данни и, ако бъдат оценени като съответстващи на Директивата (и, когато е уместно, на други инструменти на ЕС за защита на данните, например Директивата за правото на неприкосновеност на личния живот и електронни комуникации (Директива 2002/58/ЕО), разгледана в следващата точка), да получат сертификат, потвърждаващ това съответствие (тъй като в Директивата от 1995 г. няма официално основание за системата, това сертифициране да няма правна сила).[79]

*НОВО Правила за "приложимо законодателство"

Както става ясно от информацията в отделните точките по-горе, съгласно Директивата държавите членки имаха значителна свобода на действие при определянето на конкретните начини, по които биха желали да "транспонират" разпоредбите на Директивата; много от тези разпоредби оставяха на държавите членки да приемат правила, които те счетат за уместни в определени контексти. Това доведе до сериозна липса на хармонизация[80] – и стана една от основните причини за избирането на формата "регламент" като инструмент, който да наследи Директивата.[81]

Трудностите, причинени от тези различия до известна степен бяха облекчени от важна разпоредба в Директивата за защита на данните от 1995 г., отнасяща се до "приложимото законодателство". Тази разпоредба (чл. 4) на практика определи три различни правила за частния сектор:

(1) администраторите, установени само в една държава членка, трябва да спазват законодателството за защита на данните на тази държава членка при всякакво

---

77 Вж.:
https://ec.europa.eu/digital-single-market/en/news/data-protection-code-conduct-cloud-service-providers
(19 юли 2013 г. - общ контекст и документи, отнасящи се към контекста)
https://ec.europa.eu/digital-single-market/en/news/data-protection-code-conduct-cloud-service-providers
(12 октомври 2015 г. - най-нова налична информация на този уебсайт)
Становище 02/2015 на Работна група по чл. 29 по Кодекса на поведение на C-SIG при облачните изчисления (Работен документ 232, приет на 22 септември 2015 г.), наличен на:
http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2015/wp232_en.pdf
За повече подробности и гледни точки в светлината на ОРЗД, вж. писмо от РГ29 към доставчиците на услуги с облачна инфраструктура в Европа от 6 февруари 2018 г., налично на:
http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=615033

78 Когато интернет започна да фигурира по-широко в света в началото на 90-те години на двадесети век, френският орган за защита на данните изказа мнение пред другите органи за защита на данните в ЕС и пред Европейската комисия, че сертифициращите програми биха могли да са много ефикасно средство за уреждане на онлайн услугите, установени извън Европа, но по онова време не беше предприето нищо.

79 Вж.:
https://www.european-privacy-seal.eu/EPS-en/about-europrise

80 Вж. проучване на Дау Корф, възложено от ЕС: Доклад от проучване на Европейския съюз относно имплементирането на директивата за защита на данните [от 1995 г.] (Report on an EU study on the implementation of the [1995] data protection directive), 2002 г., налично на:
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1287667 –

81 Вж. втора част, раздел 2.1 и текста в първа подточка, "*Регламент …*" в раздел 2.2 по-долу.

обработване, контролирано от тях и "осъществявано в контекста на дейностите на мястото на установяване на [този] администратор" (чл. 4, пар. 1, б. "а"), първо изречение);

(2) администратори, които са установени в повече от една държава членка [да се разбира: имат клонове в повече от една държава членка] трябва да направят така, че "всеки от тези клонове да спазва задълженията, включени в националното приложимо законодателство" (като не е задължително, то да е това на страната на основаване на въпросния клон) (чл. 4, пар. 1, б. "а"), второ изречение);

(3) администратори, които не са установени в Общността (ЕС), трябва да спазват законите на всяка страна членка, на чиято територия "използват оборудване, автоматично или друго" (чл. 4, пар. 12, б. "в")); и тези администратори трябва да "определят представител" на тази територия (чл. 4, пар. 2).[82]

Струва си да се отбележи, че тези правила позволиха на държавите членки да защитават правата, на техните **граждани** свързани със защита на данните срещу нарушения от страна на участници извън територията им или извън ЕС. Всъщност, по силата на всички тези три правила, **данните на всички лица** ("физически лица"), обработвани от съответните администратори трябваше да се защитят, ***независимо дали субектите на данни са в ЕС или не, и независимо дали са граждани или пребиваващи в ЕС или не*** – в съответствие с принципа за *универсалност на правата на човека*.[83]

Тези правила бяха трудни за практическо приложение (особено по отношение на администратори, установени извън ЕС/ЕИП),[84] но поне предоставяха някакви указания за това как да се процедира с различните закони в различните държави членки, които теоретично биха могли да са приложими за някоя трансгранична операция за обработване на лични данни. Конвенцията за защита на данните от 1981 г. не съдържаше такава разпоредба, насочена към избягването на "стълкновение на закони".

Що се отнася до публичния сектор, определянето на приложимото законодателство на

---

[82] Приложението на това трето правило се усложняваше от употребата на различни думи в различните (но в правно отношение всички еднакво автентични) езикови варианти: оригиналният проект на директивата беше на френски език и използваше термина *moyens* – "means" на английски език. При другите официални езици от романската група се използваше лингвистичният еквивалент, като всички думи също означаваха "средства". Официалната немскоезична версия също използваше същата дума – *Mittel*. Английският текст обаче говореше за употребата на "*оборудване*", а холандската версия последвала този пример (*middelen*). Това стана причина Обединеното Кралство и Холандия да ограничат приложението на правилото до ситуации, при които администратора, който не е от ЕС/ЕИП *притежавал* местно оборудване в ЕС/ЕИП, докато други страни постановили, че дори присъствието на смарт телефон в ЕС/ ЕИП било достатъчно основание всеки администратор, "използващ такова устройство за транзит на данни" да е подчинен на Директивата. Сравни с разглеждането на "приложимото законодателство" във връзка с Директивата за правото на неприкосновеност на личния живот и електронни комуникации в раздел 1.3.3 по-долу.

[83] Вж. Дау Корф, Запазване на доверието в цифрово свързаното общество (Maintaining Trust in a Digital Connected Society), доклад, написан за Международния съюз по телекомуникации (МСТ), май 2016 г., раздел 2.3, *Универсалност на човешките права*, наличен тук: http://www.itu.int/en/ITU-D/Conferences/GSR/Documents/ITU_MaintainingTrust_GSR16.pdf

[84] Вж.: Дау Корф, *Der EG-Richtlinienentwurf über Datenschutz und "anwendbares Recht"*, в: Recht der Datenverarbeitung, година 10 (1994 г.), том № 5-6, с. 209 и сл.; *Въпросът за "приложимото право" (The question of "applicable law")*, в: Ръководство за съответствие 3 – междинен доклад (Compliance Guide 3 – Interim report) (част от Новата програма за информация и съответствие по закона за защита на данните на Обединеното Кралство от 1998 г. (New UK Data Protection Act 1998 Information & Compliance Programme)), Законите за неприкосновеността на личния живот и бизнеса (Privacy Laws & Business), ноември 1999 г.

практика беше по-ясно: всички публични органи и институции, включително дипломатически институции, бяха подчинени само на закона (или законите) за защита на данните на тяхната държава-членка.

*НОВО Надзорни органи

Друга важна новост в Директивата от 1995 г. при сравнение с Конвенцията от 1981 г.[85] беше изискването всички държави членки да определят:

> Дали един или повече държавни органи отговарят за контрола на прилагането на разпоредбите, приети от държавите членки съгласно настоящата директива
>
> (чл. 28, пар. 1, първо изречение)

За да бъдат ефективни, тези "**надзорни органи**" – в практиката по-често наричани ***органи по защита на данните*** или ***ОЗД*** – (от които имаше няколко във федералните държави членки) – трябваше да получат широки правомощия за ***разследване, намеса*** и ***управление*** (включително правомощия да разпореждат блокиране, изтриване или унищожаване на данни или въвеждане на временна или окончателна забрана за обработването им) (чл. 28, б. „3"), първо и второ тире) и трябваше да могат да "*действат напълно независимо при упражняването на свойте правомощия*" (чл. 28, пар. 1, второ изречение). Изискването за независимост е и изискване за демокрация и върховенство на закона. Тъй като изискванията за независимост не бяха записани в Директивата, се наложи Комисията да прибегне до съдебни действия срещу няколко държави членки, за да бъде изяснен въпросът. Резултатите от тези съдебни дела бяха отразени в много по-подробните разпоредби на ОРЗД в това отношение.

Властите трябваше да се **консултират с** тези органи при изработването на мерки или регламенти, свързани със защита на данните (чл. 28, пар. 2) и те трябваше да могат да "***участват в съдебни производства***", свързани с предполагаеми нарушения на тяхното национално законодателство за защита на данните (чл. 28, пар. 3, трето тире).

Също така, те отговаряха за уведомяването и "предварителната проверка", разгледани в следващата подточка.

От голямо значение е и че, освен по-формалните средства за правна защита, отбелязани в следващата подточка, на органите по защита на данните трябваше да се даде и право да "**разглеждат искове [да се разбира: да разглеждат жалби], подадени от всяко лице, или от дружество, представляващо това лице" свързани със защитата на данните** (Чл. 28, пар. 4).

Органите по защита на данните, които на ниво ЕС са работели съвместно (до 25 май 2018 г.) в рамките на "**Работната група по член 29**", разгледана в последната подточка на настоящия раздел, се превърнаха в основните защитници на правата за защита на данните в ЕС (макар пълномощията и ефективността им съгласно националните закони,

---

85 Това вече беше предвидено в необвързващото Ръководство на ООН, прието през 1990 г. (вж. бележка под линия 41 по-горе). Също, както е отбелязано в 1.2.3 по-горе, в Допълнителния протокол от 2001 г. към Конвенцията от 1981 г. беше въведено изискване към държавите да създадат независими надзорни органи при стриктно следване на насоките в Директивата за защита на данните от 1995 г. с цел да се приведе режима от Конвенцията в това отношение в съответствие с режима на Директивата на ЕО от 1995 г. (вж. чл. 1 от Допълнителния протокол) – въпреки че, разбира се, това се отнасяше само до тези държави, страни по първоначалната Конвенция, които се бяха присъединили и към Протокола (както е описано в бележка под линия 45 по-горе).

приети във връзка с имплементирането на Директивата, да се различавали).

*НОВО Уведомяване и "предварителна проверка"

*НОВО *Уведомяване:*

За да се постигне **цялостна прозрачност** при обработването на лични данни и за да подпомогне осигуряването на пълно съобразяване със законодателството за защита на данните, Директивата за защита на данните от 1995 г. предвиди и обширна система за **уведомяване** за дейности по обработването на лични данни (чл. 18, за подробности относно съдържанието на уведомлението, виж чл. 19); и определи, че дейностите по обработването, за които се уведомява, трябва да се въвеждат в ***обществено достъпен* регистър** (чл. 21(2)). Системата се основаваше на въведената първо в Швеция система от 1973 г., впоследствие възприета от много други държави членки на ЕС.

Директивата позволи на държавите членки да включат, като алтернативи на уведомяването, разпоредби за ***опростяване*** или ***освобождаване*** от общото задължение за уведомяване в (предимно) две "еквивалентни" ситуации, а именно:[86]

- когато, за "нерисково" обработване,[87] органът по защита на данните на държавата членка е публикувал "***опростени норми***", задаващи основните параметри за обработване (т.е., целите на обработване, данните или категориите данни, които се обработват, категорията или категориите субекти на данни, получателите или категориите получатели, пред които се разкриват данните и срока, за който данните ще се съхраняват) (чл. 18, пар. 2), първо тире) – с администратори, които декларират официално, че се придържат към тези опростени норми, **освободени** от уведомяване; или
- когато законодателството на държавата членка изисква назначаването на независимо ***длъжностно лице за защита на данните*** в рамките на организацията на администратора, което да отговаря за "гарантиране по независим начин на вътрешното прилагане на [националните разпоредби, приети съгласно настоящата директивата] и за воденето на регистър на извършваните от администратора дейности по обработката, който съдържа информацията, за която принципноби следвало да се уведоми органът по защита на данните (чл. 18(2), второ тире).

Първото изключение се основаваше на френската система от "*normes simplifiées*"; второто – на германската система, която изисква назначаването на длъжностни лица за защита на данните в организациите на всички администратори от публичния сектор и повечето големи администратори от частния сектор.[88] Във връзка с алтернативните

---

[86] Другите дейности, които подлежаха на освобождаване от уведомяване, бяха **обществените регистри**, които предоставяха **определени гаранции за записите за членове на и лица, свързани с политически, религиозни, философски или профсъюзни органи с нестопанска цел**, както и **ръчни досиета**(чл. 18(3) – (5)).

[87] Пълен текст: "дейностите по обработване, за които няма вероятност, като се имат предвид данните, подлежащи на обработка, че могат да окажат неблагоприятно влияние върху правата и свободите на субектите на данни".

[88] Наричани съответно *behördliche-* и *betriebliche Datenschutzbeauftragten*, да не се бъркат с държавните и федералните органи по защита на данните, *Landes-* and *Bundesdatenschutzbeauftragten*. Забележете, че макар много държави членки да приеха понятието за длъжностно лице по защита на данните в законодателството, имплементиращо директивата, това беше направено по различни начини,

системи Директивата предвижда, че администраторите (или друг орган, определен от държавата членка) трябва да направи публично налична същата информация, която иначе би била достъпна чрез регистъра на дейностите, за които е уведомено (чл. 21, пар. 3).

*НОВО *"Предварителна проверка":*

В съответствие с френския подход Директивата от 1995 г. изисква обработването, създаващо "**специфични рискове за правата и свободите на субектите на данни**" ("**рисково обработване**") да подлежи на по-широкообхватното изискване за "**предварителна проверка**" (чл. 20). Държавите членки трябваше да определят **кои видове дейности по обработване** ще се подлагат на това широкообхватно изискване (като се вземат предвид целта на обработване, видовете данни и мащаба на въпросното обработване). Държавите членки можеха да избират, също така **как и от кого** да се осъществява такава проверка, по-конкретно:

- дали да се изисква предварителна проверка ***при внасяне на уведомление***, в което се посочва, че операцията, за която се уведомява е от вид, изискващ такава проверка от страна на органът по защита на данните (френският подход, приет от повечето държави членки); или
- дали обработването ще се регламентира чрез закон или спомагателен законодателен инструмент, от органа по защита на данните при изготвянето на инструмента, или от Парламента в хода на приемането на такъв инструмент.

(Чл. 20(2) и (3)).

Вследствие на тези разнообразни възможности в Директивата, различните държави членки приеха (или по-скоро запазиха) различни режими по отношение на тези аспекти, което означаваше, че дадени дейности подлежаха на уведомление или предварителни проверки в някои от държавите членки, а в други – не.

*НОВО Специфични правни средства за защита и санкции

Конвенцията от 1981 г. определя, че държавите, страни по тази Конвенция, трябва да "установят ***подходящи санкции и правни средства за защита***" при нарушения на техните национални закони за защита на данните, но не уточнява кое би било "подходящо" в това отношение.

За разлика от тази разпоредба в Конвенцията от 1981 г., Директивата от 1995 г. предвижда, че субектите на данни трябва да имат достъп до **съдебно правно средство за защита** при всякакво (предполагаемо) нарушение на техните права (съвсем отделно от правото да се подават жалби пред съответния национален орган за защита на данните, отбелязано в предишната подточка) (чл. 22). Освен това всяко лице, претърпяло вреди в резултат на неправомерно обработване или друго действие, несъвместимо с Директивата, трябва да има правото да получи **обезщетение** от администратора (освен ако последният може да докаже, че не е отговорен) (чл. 23).[89]

с различен обхват и задачи за длъжностното лице по защита на данните, както и с различни условия за назначаването му. Както се разглежда във втора част, ОРЗД от своя страна предоставя подробни, хармонизирани указания относно назначаването им, като обвързва това с принципа на "отчетност".

[89] Обединеното кралство първоначално се опита да ограничи това само до материални щети, но в крайна сметка се прие, че Директивата изисква и лицата да могат да получат обезщетение от нематериални щети (бедствие).

Също така освен тези правни мерки за защита, от държавите членки се изискваше да предвидят допълнителни "подходящи мерки" и "санкции" независимо от всякакви индивидуални искове или жалби (чл. 24).

В много държави членки обаче действителните наказателни мерки, предвидени в съответното национално законодателство или налагани на практика бяха относително малки.[90]

*НОВО Работна група по член 29 и Комитет по член 31

Накрая Директивата за защита на данните от 1995 г. създаде два органа на ниво ЕС, наречени на името на членовете, във връзка с които са създадени:

- т.нар. „**Работна група по член 29**", независима група, състояща се от представители на органите по защита на данните на държавите членки, както и представител от Европейския надзорен орган по защита на данните (ЕНОЗД), и представител на Европейската комисия (на чело на секретариата на групата, без право на глас)), на която се възложиха задачата да допринася за по-хармонизирано прилагане на Директивата, по-специално чрез приемане на препоръки и становища (по собствена инициатива) и даване на становище по всеки проект на кодекс на поведение, разработен на равнище ЕС; и с която Европейската комисия трябваше да се съветва относно всяко предложение, свързано с "*правата и свободите на физически лица по отношение на обработването на лични данни*" (т.е., защитата на данните), както и относно всички проекти на решения за адекватността на защитата в трета държава;[91] и
- т.нар. „**Комитет по член 31**", съставен от представители на правителствата на държавите членки, но председателстван от представител на Комисията, пред който трябваше да се представят за становище всички проектомерки, които следдваше да се предприемат по силата на Директивата; при отрицателно становище на Комитета мярката следваше да се насочи към Съвета, където той можеше да отмени решението с квалифицирано мнозинство.[92]

Работната група по член 29 (РГ29) издаде **много работни документи и становища** по извънредно широк набор от въпроси, свързани с прилагането на Директивата за защита на данните от 1995 г. и Директивата за правото на неприкосновеност на личния живот и електронни комуникации от 2002 г. (разгледана в 1.3.3 по-долу).[93] Тези документи, и особено официалните становища, макар и да не са правно обвързащи, все още са много

---

[90] Нуждата от по-сериозни наказания стана явна едва след появата на интернет, контролиран до голяма степен от структури извън ЕС/ЕИП, за които беше по-слабо вероятно да се съобразят с правилата за защита на данните на ЕС само на базата на покана от страна на органите по защита на данните от ЕС. Това намери отражение в много по-строгата разпоредба в ОРЗД, че органите по защита на данните могат да налагат административни глоби до 10 000 000 евро или 2% от годишния оборот на отговорния участник или дори, в особено фрапантни случаи, до 20 000 000 евро или 4% от годишния оборот (чл. 83 от ОРЗД).

[91] За подробности, вж. чл. 30.

[92] За подробности, вж. чл. 31.

[93] Всички документи, приети от Работната група по член 29 между 1997 г. и ноември 2016 г. може да се намерят на тази архивна страница:
http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm
Актуализации и документи, приети след ноември 2016 г. до разпускането на РГ29 на 25 май 2018 г. може да бъдат намерени тук:
http://ec.europa.eu/newsroom/article29/news-overview.cfm

авторитетни по отношение на директивите. Те помогнаха действително да се осигури цялостно и строго прилагане на директивите на "високо ниво" и до известна степен смекчиха проблемите, произхождащи от различията в законите на държавите членки.

NB: Наследникът на РГ29 е Европейският комитет по защита на данните (ЕКЗД), който надгражда над работата на РГ29: в първия ден от своето съществуване – 25 май 2018 г. – той одобри редица становища на РГ29, които бяха разработени в очакване на ОРЗД.[94] Секретариатът му се осигурява от ОЗД на държавите - членки.

1.3.3 Директива за защита на данните в сектора на телекомуникациите от 1997 г., директива на ЕО за правото на неприкосновеност на личния живот и електронни комуникации от 2002 г., и допълнения от 2009 г. Директива 2002/58/ЕО

Общи положения

Директивата за защита на данните в сектора на телекомуникациите, предложена по същото време както Директивата за защита на данните от 1995 г., беше приета на 15 декември 1997 г.[95] Връзката ѝ с Директивата за защита на данните от 1995 г. е разяснена в чл. 1(2), където се казва, че разпоредбите на директивата имат функцията да "*уточнят по-подробно и да допълнят*" главната Директива. По-конкретно, специфичните по отношение на защитата на данните определения от Директивата от 1995 г., както и всички други принципи и правила в тази директива, прилагани и към администраторите и дейностите по обработване, които са обект на Директивата за защита на данните в сектора на телекомуникациите, освен когато последната не определя по-специфични правила. Също така всички разпоредби по отношение на специфични цели или услуги (сметки с описание на услугите, идентификация на входящите повиквания, указатели, и др.: виж по-долу) представляват тълкувания и прилагане на общите принципи и права от Директивата от 1995 г. С други думи, Директивата за защита на данните в сектора на телекомуникациите се яви като *lex specialis* по отношение на Директива за защита на данните от 1995 г., *lex generalis*.

Имплементирането на тази директива се отложи, отчасти защото през 1999 г. Комисията извърши общ преглед на регулаторната рамка за електронни комуникации в светлината на развиващите се нови технологии и бизнес практики. Един от резултатите от този преглед беше предложение от 2000 г. за заместване на Директивата за защита на данните в сектора на телекомуникациите с нова директива за защита на данните в

---

94 Вж. бележка под линия 248 по-долу.

95 Пълно наименование: Директива 97/66/ЕО на Европейския парламент и на Съвета от 15 декември 1997 г. относно обработката на лични данни и защита на неприкосновеността на личния живот в сектора на телекомуникациите, ОВ L24, 30.01.1998 г., стр. 1 – 8, налична на: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31997L0066&from=EN
Директивата за защита на данните в сектора на телекомуникациите се възползва в голяма степен от работата, извършена в Съвета на Европа по отношение на препоръка по същия въпрос, което доведе до приемането на Препоръка № R (95) 4 от Комитета на Министрите на Съвета на Европа към държавите членки относно защитата на личните данни в областта на телекомуникационните услуги с особено внимание към телефонните услуги, приета на 7 февруари 1995 г., налична на: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168050108e –
и от работата на органите за защита на данните от *Международната работна група по защита на данните в телекомуникациите* ("Берлинската група"), създадена през 1983 г., вж.: https://www.dataprotectionauthority.be/berlin-group

сектора на електронните комуникации.[96] Това доведе до приемането на Директивата за правото на неприкосновеност на личния живот и електронни комуникации през юли 2002 г., Директива 2002/58/ЕО, позната като „**директива за правото на неприкосновеност на личния живот и електронните комуникации („e-Privacy Directive")**".[97] В нея също се подчертава, че естеството ѝ е спомагателно и допълващо по отношение на основната Директива за защита на данните от 1995 г., по същия начин както и предхождащата я (виж чл. 1(2)).

През 2009 г. Директивата от 2002 г. беше изменена чрез отделна директива, Директива 2009/136/ЕО,[98] често наричана „**закон за бисквитките**", тъй като регламентира "бисквитките" (макар че регламентира и допълнителни въпроси и дейности по защитата на данни). В текста по-долу ще опишем правилата, както се съдържат в Директивата от 2002 г. с измененията от Директивата от 2009 г. За краткост понякога ще наричаме Директивата за защита на данните 1995 "главната директива", а Директива 2002/58/ЕО(в нейната изменена форма) – "спомагателната" директива.

Към момента на писането (декември 2018 г.) Директива 2002/58/ЕО е все още в сила, макар инструментът-"майка" – главната Директива за защита на данните от 1995 г. да беше заменена от Общия регламент относно защитата на данните. Наследник на директивата за правото на неприкосновеност на личния живот и електронни комуникации, който също ще бъде регламент (а не директива) е в процес на приемане (вж. раздел 1.4.2 по-долу). Директива 2002/58/ЕО със сигурност е все още в сила към момента, поради което тя все още получава пълно внимание в наръчника и поради което в очакване на приемането на предложения нов Регламент за правото на неприкосновеност на личния живот и електронните комуникации, ще опишем все още приложимата Директива за правото на неприкосновеност на личния живот и електронни комуникации по-долу.

Предназначение, цел и обхват на Директивата за правото на неприкосновеност на личния живот и електронни комуникации от 2002 г., с поправките от 2009 г.

Докато главната Директива за защита на данните от 1995 г. имаше общо приложение, спрямо всяко обработване на лични данни от която и да е съответна структура от публичния или частния сектор, активна в рамките на "Първия стълб" на Европейската общност, Директива 2002/58/ЕО, като спомагателен инструмент има много по-тесен (по-

[96] Предложение за директива на Европейския парламент и на Съвета относно обработването на лични данни и защитата на неприкосновеността на личния живот в сектора на електронните комуникации, Брюксел, 12.07.2000 г., COM(2000) 385 final.

[97] Пълно наименование: Директива 2002/58/ЕО на Европейския парламент и на Съвета от юли 2002 г. относно обработката на лични данни и защита на правото на неприкосновеността на личния живот в сектора на електронните комуникации, ОВ L201, 31.07.2002 г., стр. 37 – 47, налична на: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058&from=EN

[98] Пълно наименование: Директива 2009/136/ЕО на Европейския парламент и на Съвета от 25 ноември 2009 г., с която се изменя Директива 2002/22/ЕО относно универсалната услуга и правата на потребителите във връзка с електронните съобщителни мрежи и услуги, Директива 2002/58/ЕО относно обработката на лични данни и защитата на правото на неприкосновеността на личния живот в сектора на електронните комуникации и Регламент (ЕО) № 2006/2004 относно сътрудничеството между националните органи, които отговарят за прилагането на законите за закрила на потребителя ОВ L337, 18.12.2009 г., стр. 11 – 36, налична на: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32009L0136

специфично определен) обхват. По собствената й формулировка тя има отношение към:

> обработката на лични данни във връзка с предоставянето на **публично достъпни електронни комуникационни услуги в публични комуникационни мрежи** в Общността, *включително публични комуникационни мрежи, поддържащи устройства за събиране на данни и идентификация*.
>
> (Част 3 - думите в курсив са добавени при изменението от 2009 г.)[99]

Терминът "електронна съобщителна услуга" е точно и строго определен в чл. 2(в) на ревизираната Рамкова директива[100] както следва:

> „електронна съобщителна услуга" означава услуга, осигурявана обикновено срещу заплащане, която се състои изцяло или главно в пренасянето на сигнали по електронни съобщителни мрежи, включително далекосъобщителни услуги и предавателни услуги по мрежи, използвани за излъчване , но изключват услугите, осигуряващи или упражняващи редакторски контрол върху съдържанието, предавано посредством електронни съобщителни мрежи и услуги; **тя не включва услуги на информационното общество, определени в чл. 1 от Директива 98/34/ЕО,[101] които не се състоят изцяло или главно в пренасянето на сигнали по електронни съобщителни мрежи**

Простото заключение, което следва от тази разпоредба в чл. 3 и определенията в тези инструменти, беше направено от РГ29 в нейното Становище относно услугите за геолокация на смарт мобилни устройства:[102] Директивата за правото на неприкосновеност на личния живот и електронни комуникации е приложима спрямо доставчиците на електронни комуникационни услуги, като телекомуникационни оператори и доставчици на интернет достъп,но не и към доставчиците на услуги на информационното общество.[103]

---

99 Измененията от 2009 г. премахнаха изключение по отношение на аналоговите обмени, което фигурираше в оригиналната версия (от 2002 г.) на Директивата за правото на неприкосновеност на личния живот и електронни комуникации.

100 Пълно наименование: Директива 2002/21/ЕО на Европейския парламент и на Съвета от 7 март 2002 г. относно общата регулаторна рамка за електронните съобщителни мрежи и услуги (Рамкова директива), ОВ L 108, 24.04.2002 г., стр. 33 – 50, налична на: https://eur-lex.europa.eu/legal-content/ga/TXT/?uri=CELEX:32002L0021

101 Пълно наименование: Директива 98/34/ЕО на Европейския парламент и на Съвета от 22 юни 1998 г. относно определяне на процедура за предоставяне на информация в областта на техническите стандарти и правила, ОБ L 204, 21.07.1998 г., стр. 37 – 48, налична на: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A31998L0034

102 Работна група по чл. 29, Становище 13/2011 относно услуги, свързани с геолокация на смарт мобилни устройства (Работен документ 185, приет на 16 май 2011 г.), наличен на: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp185_en.pdf

103 РГ29, Становище 13/2011 относно услугите, свързани с геолокация на смарт мобилни устройства (предишна бележка под линия), раздел 4.2.1, *Приложимост на ревизираната директива за правото на неприкосновеност на личния живот и електронни комуникации* (стр. 8 – 9).
Според още по-точната формулировка в Работния документ на Комисията (бележка под линия 99 по-горе):
"*Директивата ще обхваща:*
(1) услугата трябва да бъде електронно-комуникационна,
(2) услугата трябва да се предлага по електронна комуникационна мрежа,
(3) гореспоменатите услуга и мрежа трябва да са публично налични, и
(4) мрежата или услугата трябва да е предоставена в рамките на Общността." (стр. 20)

(Както се обсъжда по-нататък в раздел 1.4.2, Комисията предлага да премахне това ограничение в предложеният Регламент в областта на правото на неприкосновеност на електронните комуникации, но докато това се случи то остава валидно.)

В рамките на този ограничен обхват Директива 2002/58/ЕО има същите цели като главната Директива: да осигури едновременно ***високо ниво на защита*** на личните данни (но в случая – специално за този сектор) и да позволи ***свободния поток на лични данни*** в рамките на Общността (в този сектор) (срв.: чл. 1(1)). Това оказа голямо въздействие върху бързоразвиващата се, все по-важна област на електронните съобщения, осигурявайки по-високо ниво на защита на данните в тази област в ЕС в сравнение с целия останал свят.

Въпреки това, независимо от привидно ясната формулировка в чл. 3, въпросът за точния обхват на Директива 2002/58/ЕО не е напълно ясен, защото някои от разпоредбите в нея се прилагат – или тълкува, че следва да се прилагат – по-широко; и защото Директива 2002/58/ЕО не съдържа изрична разпоредба по отношение на приложимото законодателство. Без да отричаме успеха на Директива 2002/58/ЕО, следва накратко да отбележим тези недоизяснени моменти.

Неяснота и липса на съгласуваност по отношение на обхвата

На първо място, има неясност по отношение на материалния обхват:

И както Комисията отбелязва в своето предложение за Регламент в областта на правото на неприкосновеност на личния живот и електронните комуникации:[104]

> Потребителите и предприятията все повече разчитат на нови базирани на интернет услуги, даващи възможност за междуличностни комуникации, като Voice over IP, предаване на съобщения в реално време и уеб-базирани услуги по електронна поща, вместо традиционни съобщителни услуги. **Тези комуникационни услуги „Over-the-Top" („OTTs") *принципно* не са в приложното поле на настоящата рамка на електронните комуникации на Съюза.**

Проучване за 2013 г., поръчано от Комисията (The SMART Study), установи, че:[105]

> **национални разпоредби по теми като бисквитки, трафик и данни за местоположението, или нежелани съобщения, приети съгласно Директивата за правото на неприкосновеност на личния живот и електронни комуникации, често имат различно приложно поле от определеното в чл. 3 от директивата за правото на неприкосновеност на личния живот и електронни комуникации**,

---

Както е разгледано по-подробно в раздел 1.4.2 по-долу, Комисията предлага да премахне това ограничение в предлагания Регламент относно правото на неприкосновеност на личния живот и електронните комуникации, но дотогава то, разбира се, остава валидно.

[104] Предложение за Регламент в областта на правото на неприкосновеност на електронните комуникации (бележка под линия 175, по-долу), раздел 1.1, стр.1, подчертаване добавено.

[105] „Директива за електронната поверителност: оценка на транспонирането, ефективността и съвместимостта с предложения регламент за защита на данните" (SMART 2013/0071) (наричана по-долу „SMART проучване"), обобщена и достъпна от: https://ec.europa.eu/digital-single-market/en/news/eprivacy-directive-assessment-transposition-effectiveness-and-compatibility-proposed-data (за пълния доклад следвайте връзките в долната част на страницата).

което е ограничено само до доставчиците на публично достъпни електронни комуникационни услуги (т.е. традиционни телекомуникационни компании). [Проучването е установило], че ограничението на приложното поле на Директивата само до доставчиците на електронни комуникационни услуги е двусмислено и може да породи неравнопоставено третиране, ако доставчиците на услуги на информационното общество, използващи интернет, за да доставят съобщителни услуги, са принципно изключени от приложното му поле.

Също така има липса на яснота относно приложимото национално право:

Докато Директивата за правото на неприкосновеност на личния живот и електронни комуникации бъде заменена от предложния Регламент в областта на правото на неприкосновеност на електронните комуникации (който може да не е в сила за определен период от време), посочените по-горе двусмислия и неясноти ще останат и ефективността на Директива 2002/58/ЕО ще продължи да бъде възпрепятствана от това.

Отношение между директивата за правото на неприкосновеност на личния живот и електронни комуникации и ОРЗД

Отношението на Директива 2002/58/ЕО беше на специален закон към общ закон спрямо Директивата от 1995 г. и следователно също е специален закон по отношение на нейния наследник ОРЗД. По отношение на въпросите, уредени в ***директивата за правото на неприкосновеност на личния живот и електронни комуникации***, следователно тя се прилага вместо ОРЗД.Отношението между ОРЗД и Директива 2002/58/ЕО, което е отношение на *общ закон към специален закон*, остава непроменено, както отношението между Директивата за защита на данните от 1995 г. и Директива 2002/58/ЕО. Това означава, че **що се отнася до <u>въпроси</u>, които са изрично уредени от Директива 2002/58/ЕО**, , тя следва да се прилага вместо разпоредбите на ОРЗД. Във всички други случаи обаче, които касаят обработването на лични данни, се прилага ОРЗД.

Следователно, правните основания на ОРЗД не са приложими, когато Директива 2002/58/ЕО предвижда по-специфични правила за обработването на лични данни. Например чл. 6 от Директива 2002/58/ЕО, който предвижда специален списък на правните основния относно обработването на данни за трафика, включително данни за трафика, които представляват лични данни, се прилага и, следователно не се прилага чл. 6 от ОРЗД. Във всички останали случаи, свързани с обработването на лични данни, се прилага ОРЗД.

Същото се отнася спрямо **<u>субекти</u>, които са или не са *„специално уредени от Директивата за правото на неприкосновеност на личния живот и електронни комуникации*”**. С оглед на становището на Работната група по член 29, че Директива 2002/58/ЕО по същество се прилага само спрямо доставчици на услуги по електронни комуникации, което означава, че също така (освен във връзка със специалните правила в чл. 5, пар. 3 и 13, които се прилагат по-широко), обработването на всякакви данни, включително данни, които са по-специфично регулирани от нея (като данни за трафика) от *субекти, различни от доставчици на електронни комуникационни услуги*, се уреждат от ОРЗД, а не от Директива 2002/58/ЕО, въпреки специалните разпоредби в нея във връзка с тези данни.

С други думи:

- доставчиците на електронни комуникационни услуги трябва да спазват Директивата за правото на неприкосновеност на личния живот и електронни

комуникации във връзка с всякакви въпроси, които са по-конкретно регламентирани в тази Директива, и ОРЗД във връзка с всички други въпроси; и

- организации, които не са доставчици на електронни комуникационни услуги, трябва да спазват разпоредбите в чл. 5, пар. 3 от Директивата за правото на неприкосновеност на личния живот и електронни комуникации по отношение на достъпа до информация на устройства и чл. 13 от тази Директива по отношение на нежеланите съобщения, и ОРЗД – във връзка с всички други въпроси (т.е., те не се уреждат от никоя от разпоредбите в тази Директива, освен тези две разпоредби).

Специфични проблеми, при които възникват горните въпроси, са отбелязани, където е уместно, в подразделите на този раздел.

Ключови характеристики на Директивата за правото на неприкосновеност на личния живот и електронни комуникации[106]

Определения

Тъй като директивата за правото на неприкосновеност на личния живот и електронни комуникации беше замислена като *специален закон* спрямо *общия закон,* Директивата за защита на данните от 1995 г., **свързаните със защитата на данните определения** от Директивата за защита на данните от 1995 г. също се прилагаха във връзка с Директива 2002/58/ЕО, както е изрично предвидено в чл. 2, първо изречение от същата. След като Директивата за защита на данните от 1995 г. беше заменена от ОРЗД, всички препращания към определенията в тази Директива следва да се тълкуват като препращания към съответните (но в определени отношения актуализирани и прецизирани) определения в Регламента. Това е отбелязано, по-долу в отделната точка"*Съгласие*".[107]

Освен това, **определенията на по-техническите термини свързани с електронните съобщения** в Рамковата директива за електронните съобщителни мрежи и услуги[108], което беше резултата от посочения по-горе преглед, в точка „*Общи положения*" – ***електронна съобщителна услуга***;[109] ***публично достъпна електронна съобщителна услуга***; ***обществена съобщителна мрежа***; и т.н. – се прилагат също към съответните технически термини, използвани в Директивата за правото на неприкосновеност на личния живот и електронни комуникации. Тук се включва терминът „**абонат**" (на електронна комуникационна услуга).

В допълнение към това, в чл. 2, Директивата за правото на неприкосновеност на личния

---

106 Много от изискванията на Директива 2002/58/ЕО, които са отбелязани тук, вече се съдържаха в Директивата за защита на данните в сферата на телекомуникациите от 1997 г. и прост бяха пренесени в Директива 2002/58/ЕО, но това не е отбелязано всеки път по-нататък. Когато въпрос или разпоредба е отбелязан(а) като „*НОВО", това означава, че той/тя е или представя нещо, което (все още) не е било уредено в Директивата за защита на данните от 1995 г..

107 ОРЗД също изяснява в някаква степен по-нататък концепцията за „лични данни", като изяснява, че дадено лице може да бъде „идентифицируемо" и чрез „онлайн идентификатор" (чл. 4, пар. 1 от ОРЗД, чл. 2, б. „а") от Директивата за защита на данните от 1995 г.. Това също следва да бъде взето предвид и при прилагането на Директива 2002/58/ЕО.

108 Бележка под линия 97, по-горе.

109 Този термин беше разгледан по-горе, в точка „*Предназначение, цел и обхват на Директива за правото на неприкосновеност на личния живот и електронни комуникации*".

живот и електронни комуникации добавя редица *НОВО **допълнителни (нови) определения**, като „***потребител***”, „***данни за трафик***”, „***данни за местонахождение***”, „***услуга с добавена стойност***”, и „***нарушение на сигурността на личните данни***” (вж. члена за подробности).

*ИЗМЕНЕНО Съгласие

Най-важното изменение в определенията на основни институти в ОРЗД в сравнение с тези в Директивата за защита на данните от 1995 г. касае определението на „**съгласие**” като законно основание за обработване на лични данни. Чл. 2, б. „е“) от Директивата за правото на неприкосновеност на личния живот и електронни комуникации предвижда, че „съгласие” на потребител или абонат както следва да се тълкува в тази Директива отговаря на съгласието на субекта на данни в Директивата за защита на данните. Защото всички препращания към Директивата за защита на данните следва да се тълкуват като препращания към ОРЗД, съгласие по директивата за правото на неприкосновеност на личния живот и електронни комуникации трябва следователно да се разбира по същия начин като съгласие по ОРЗД, където е определено като:

> ***В***сяко свободно изразено, конкретно, информирано и недвусмислено указание за волята на субекта на данните, посредством изявление или ясно потвърждаващо действие, което изразява съгласието му свързаните с него лични данни да бъдат обработени, (Чл. 4, пар. 11 от ОРЗД)

Също така,, ОРЗД

изяснява по-подробно, какви условия трябва да бъдат изпълнени, преди дадено съгласие да може да се счита за валидно и наред с другото посочва, какво означава съгласието да бъде дадено свободном, и какво може да означава устно утвърдително действие.[110] Освен това Европейският комитет за защита на данните (ЕКЗД) издаде насоки за съгласие[111]..

Тези пояснения в ОРЗД и в тези насоки са особено уместни по отношение на няколко основни разпоредби на Директивата за правото на неприкосновеност на личния живот и електронни комуникации изискват съгласие на потребителя или абоната. Сред тях са:

- Чл. 5.3 за съхраняването или събирането на информация от терминално оборудване;
- Чл. 6 и 9 за повторното използване на данни за трафика и местонахождението за услуги с добавена стойност за целите на маркетингови електронни съобщителни услуги;
- Чл. 12 за указатели на абонати; и
- Чл. 13 за нежелани съобщения.

Във връзка с тези въпроси, за да бъде валидно съгласието, сега трябва да бъде съгласно ОРЗД - и от държавите-членки се изисква да преразгледат националните закони, като

[110] Вж. Членове 7 и 8 ОРЗД и съответните съображения 32 - 33 и 42 - 43.

[111] Насоки за ЕКЗД относно съгласието съгласно Регламент 2016/679 (wp259rev.01). Тези насоки бяха приети от Работната група по член 29 (WP29) на 28 ноември 2017 г. и ревизирани на 10 април 2018 г. Впоследствие бяха одобрени от неговия приемник - Европейски съвет за защита на данните (EDPB). Те допълват предишно становище на член 29 от WP относно определението за съгласие (WP187, становище, 15/2011).

> транспонират Директивата за правото на неприкосновеност на личния живот и електронни комуникации, и националните практики за прилагане, за да гарантират, че те са в съответствие с ОРЗД.

Горепосочените въпроси са допълнително обсъдени в съответните точки по-долу.

Сигурност

Чл. 4, пар. 1 ефективно повтаря изискването на Директивата за защита на данните от 1995 г., като предвижда, че доставчиците на електронни съобщителни услуги трябва да предприемат „***подходящи технически и организационни мерки, за да защити сигурността на неговите услуги***", като същевременно добавя, че „ако е необходимо", това трябва да бъде направено „*заедно с доставчика на [съответните] публични комуникационни мрежи*". Също така, той добавя, точно като основната Директива, че нивото на сигурност трябва да бъде „***съответстващо на риска, който е налице***", като се вземат предвид достиженията на техническия прогрес и разходите за мерките. Чл. 4, пар. 1а, въведен от Директивата от 2009 г., добавя, че:

> Без да се засягат разпоредбите на Директива 95/46/ЕО, мерките, посочени в пар. 1 най-малкото:
>
> - гарантират, че достъп до личните данни може да има само упълномощен персонал за законно разрешени цели,
> - защитават съхраняваните или предавани лични данни от случайно или незаконно унищожаване, случайна загуба или промяна и неразрешено или незаконно съхраняване, обработка, достъп или разкриване, и,
> - гарантират осъществяването на политика на сигурност по отношение на обработката на лични данни.

И Директивата за правото на неприкосновеност на личния живот и електронни комуникации,[112] и ОРЗД[113] предвиждат задължение за гарантиране на сигурността, както и задължение да бъде уведомяван за нарушения на сигурността на личните данни[114] компетентният национален орган и, съответно, надзорния орган [т.е., органа по защита на данните].[115] Тези задължения ще съществуват успоредно съгласно двата последни законодателни акта, съобразно техните съответни приложни полета. Съгласно Чл. 95 от ОРЗД,не се налагат допълнителни задължения на физически или юридически лица във връзка с въпроси, за които те са обвързани от специфични задължения, предвидени в Директивата за правото на неприкосновеност на личния живот и електронни комуникации. Като *специален закон* спрямо ОРЗД , Директива 2002/58/ЕО следва да не води до по-ниско ниво на защита от защитата, предвидена от Регламента.

Също така чл. 4, пар. 1 предвижда, че:

> Съответните национални регулаторни органи са в състояние да проверяват мерките, предприети от доставчици на обществено достъпни електронни

---

112 Чл. 4. [оригинална бележка под линия]

113 Чл. 32 – 34. [оригинална бележка под линия]

114 Изискванията за уведомление за нарушение на сигурността на данните са обсъдени в тази точка, по-късно в този раздел.

115 Относно различните органи, участващи в прилагането на Директива 2002/58/ЕО, вж. следващия цитат в настоящата подточка и коментара по него, и обсъждането по последната точка в този раздел.

> комуникационни услуги, както и да издават препоръки относно най-добрите практики по отношение на нивото на сигурност, което тези мерки следва да постигнат.

Следва да се отбележи, че не се изисква тези „съответни органи" да бъдат националните органи по защита на данните. Вж. в точка „*Надзор и прилагане*", по-долу.

*НОВО Уведомяване за рискове

Чл. 4, пар. 2 от Директивата за правото на неприкосновеност на личния живот и електронни комуникации предвижда, че:

> В случай на **особен риск от нарушение на сигурността на мрежата**, доставчикът на публично достъпни електронни комуникационни услуги трябва да **уведоми** абонатите относно такъв риск и, когато рискът се намира извън обхвата на мерките, които трябва да предприеме доставчикът на услугата, относно **всички възможни средства за справяне**, включително указание за възможните свързани **разходи**. (добавено подчертаване)

Това изискване за „уведомяване за рискове" (което вече беше включено в оригиналния текст от 2002 г.) следва да бъде разграничено от по-сложните изисквания за „уведомление за нарушаване на сигурността на данните", обсъдено в следващата точка – които бяха добавени едва в измененията през 2009 г., и които се прилагат едва след като нарушението е възникнало, докато чл. 4, пар. 2 изисква уведомяване за всеки риск от *евентуално* възникване на нарушение.

*НОВО Уведомление за нарушение на данни

Директивата за правото на неприкосновеност на личния живот и електронни комуникации (изменена през 2009 г.) предвижда, че, в допълнение към изискването за „уведомяване за рискове", обсъдено по-горе, доставчиците на електронни комуникационни услуги трябва да ***уведомят „компетентния национален орган"*** за – да се чете *всяко действително* – нарушение на сигурността на лични данни „*без ненужно забавяне*" (чл. 4, пар. 3, първа точка – отбелязва, че този орган отново не се изисква да бъде органа по защита на данните).

Ако „*нарушението на сигурността на личните данни* ***има вероятност да повлияе неблагоприятно на личните данни или неприкосновеността на личния живот на абонат или отделно лице***", тогава доставчикът „***уведомява също така засегнатия абонат или лице***" за това нарушение „без ненужно забавяне" (чл. 4, пар. 3, втора точка). Това уведомление до засегнатия абонат или лице не се изисква:

> ако доставчикът е доказал в удовлетворителна степен пред компетентния орган, че е приложил подходящи технически мерки за защита и че тези мерки са приложени към данните, засегнати от пробива в сигурността. Такива технически мерки за защита правят данните неразбираеми за всяко лице, което няма право на достъп до тях. (чл. 4, пар. 3, точка трета)

С други думи, не се изисква абонатите и другите засегнати лица (по-специално, разбира се, субекти на данни, но и юридически лица, които са абонати), да бъдат информирани за нарушение на сигурността на данните, засягащо техни данни, ако доставчикът може да докаже пред „компетентния орган", че данните, които са били компрометирани (по-специално, всички данни, които може да са били неправилно разкрити или предоставени на трети лица), са били **направени напълно „неразбираеми"** за всяко

лице или лица, които може да са получили достъп в резултат от нарушението, чрез подходящи технологични мерки за защита (както е изяснено в чл. 4 от Регламент 611/2013 на Комисията).[116]

Обратното, „компетентният орган" може да „изиска" от доставчика да съобщи за нарушение на данни на съответните абонати и други засегнати лица, когато доставчикът не е сторил това – т.е., понеже органът не е съгласен с преценката на доставчика, че нарушението на сигурността на данните няма *„вероятност да повлияе неблагоприятно*" на личните данни или неприкосновеността на личния живот на тези абонати или лица, или понеже органът не счита, че изтеклите данни са действително напълно „неразбираеми" за неоторизирания(те) получател(и) (напр., тъй като ключът за декриптиране е изтекъл или може също да е изтекъл, или тъй като методът на криптиране не е бил достатъчно стабилен)[117] (чл. 4, пар. 3, четвърта точка).

Последната, пета, точка на чл. 4 пар. 3 предвижда, че:

> При уведомяване на абоната или лицето се описва най-малко какво е естеството на нарушението на сигурността на личните данни и се указва източникът, от които може да се получи повече информация, както и да се препоръчват мерки за смекчаване на евентуалните неблагоприятни последици от нарушението на сигурността на личните данни. При уведомяването на компетентния национален орган в допълнение се описват последиците от нарушението на сигурността на личните данни, както и предложените или предприетите от доставчика мерки за неговото овладяване.

Директивата за правото на неприкосновеност на личния живот и електронни комуникации, както е изменена от Директивата от 2009 г., също предвижда важни **формални изисквания**, с които да се подкрепят горепосочените нови разпоредби. По този начин:

> [Компетентните национални органи] също така имат възможност да **проверяват** дали доставчиците изпълняват задълженията си за уведомяване съгласно настоящия параграф и в случай на неизпълнение да налагат подходящи **санкции**.
>
> (чл. 4, пар. 4, първа точка, второ изречение, добавено подчертаване)

---

116 Пълно наименование: Регламент (ЕС) № 611/2013 на Комисията от 24 юни 2013 година относно мерките, приложими за съобщаването на нарушения на сигурността на личните данни съгласно Директива 2002/58/ЕО на Европейския парламент и на Съвета за правото на неприкосновеност на личния живот и електронни комуникации, ОВ L 173 на 26.06.2013 г., стр.2 – 8, може да бъде намерена на: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32013R0611
Регламентът на Комисията е приет на основание на чл. 4, пар. 5 от Директива 2002/58/ЕО, който оправомощи Комисията да го приема *„технически мерки за изпълнение относно обстоятелствата, формата и процедурите, приложими за изискванията за информация и уведомяване, посочени в настоящия член*" (чл. 4, пар. 5), след провеждане на консултация с Европейската агенция за мрежова и информационна сигурност (ENISA), Работната група по член 29 и Европейския надзорен орган по защита на данните (ЕНОЗД), и включвайки всички (други) съответни заинтересувани лица.

117 Например, слаби алгоритми като MD5 или SHA1 се считат за остарели и данни, криптирани с тях, вече не могат да се считат за направени наистина „неразбираеми" (да се чете: невъзможни за декриптиране). Вж.:
https://www.owasp.org/index.php/Cryptographic_Storage_Cheat_Sheet
Би могло да се мисли за случай, в който е нарушена сигурностат на данните от електронни съобщения, при които съдържанието на съобщенията е било напълно криптирано със силни алгоритми като SHA-256, но не и метаданните. Следва да се отбележи, че (както е посочено на споменатия по-горе уебсайт) „класификацията на „силни" криптографски алгоритми може да са измени в хода на времето".

Ефективността на тези правомощия за проверка (инспекция) и санкциониране се подкрепя от следващо изискване, предвидено във втората точка на чл. 4, пар. 4:

> Доставчиците поддържат **регистър на нарушенията по отношение на личните данни**, който съдържа фактите, свързани с подобно нарушение, последиците от него и предприетите действия за справяне с тях, които трябва да бъдат достатъчни, за да се създаде възможност за компетентните национални органи да проверят спазването на разпоредбите на пар. 3. Регистърът съдържа единствено информацията, необходима за тази цел. (добавено подчертаване)

Изменената Директива 2002/58/ЕО предвижда издаването на „**насоки**" и „**инструкции**" от „компетентните национални органи" относно „*обстоятелствата, при които от доставчиците се изисква да уведомяват за нарушения на сигурността на лични данни, формата на такова уведомяване, както и начина, по който се прави уведомяването*" (чл. 4, пар. 4, първа точка, първо изречение).

Горепосочените изисквания за уведомяване при нарушаване на сигурността на данните на Директива 2002/58/ЕО, които са ограничени от обхвата и, са предвестникът на по-общите изисквания за уведомяване за нарушение на сигурността на данните, които са сега включени в Общия регламент относно защитата на данните, и които са приложими към всяка операция по обработване на лични данни, разгледани във Втора Част, раздел 2.1 по-долу. Може да се считат за „прекалени".[118]

Специфични изисквания за обработване за специфични цели:

Вместо да повтаря общите принципи за защита на данните и списъка с основанията за законно обработване, които са предвидени в основната Директива за защита на данните от 1995 г., Директивата за правото на неприкосновеност на личния живот и електронни комуникации предвижда общо изискване за поверителност на комуникациите и редица специфични изисквания и условия за определени данни или дейности по обработване. В тях, Директивата за правото на неприкосновеност на личния живот и електронни комуникации се стреми да прилага принципите и правата на Директивата за защита на данните от 1995 г. спрямо тези специфични въпроси, с цел да хармонизира приложението на споменатите принципи и права в държавите членки, както е обсъдено в различни точки по-долу.

На първо място обаче е важно да си припомним, че, доколкото Директивата за правото на неприкосновеност на личния живот и електронни комуникации предвижда специфично правно основание за обработване за конкретни цели (както е посочено в тази директива), по-общите законни основания за обработване за различни цели, предвидени в чл. 5 и 6 от ОРЗД не се прилагат.[119]

По този начин, когато Директивата за правото на неприкосновеност на личния живот и електронни комуникации изисква съгласие – както във връзка с достъп до информация на устройства (чл. 5, пар. 3), или изпращането на нежелани маркетингови съобщения (чл. 13) – или предвижда редица законни основания и цели на обработването, както

---

[118] Работен документ на Комисията (бележка под линия 99, по-горе), Annex V: REFIT analysis of coherence of the ePrivacy Directive with the ОРЗД (Приложение V: REFIT анализ на съгласуваността на Директива 2002/58/ЕО с ОРЗД (Диаграма – коментар по чл. 4.3.; 4.4.; 4.5 – Уведомление за нарушения на сигурността на лични данни).

[119] Вж. цитата от Неофициалния технически документ на Комисията точка „*Отношение между Директива 2002/58/ЕО и ОРЗД*", по-горе.

във връзка с обработването на данни за трафика (чл. 6) – никоя организация, подчиняваща се на тези правила, която във връзка с чл. 5, пар. 3 и чл. 13 е всяка организация, а във връзка с чл. 6 са доставчици на електронни комуникационни услуги – не може да разчита на никакво друго основание или принцип, предвиден(о) в ОРЗД. По-специално, те не могат да разчитат на основанието за обработване „съвместими цели", предвидено в чл. 5, пар. 1, б. „б") от ОРЗД.

*НОВО ***Поверителност на съобщенията:***

Чл. 5, пар. 1 от Директивата за правото на неприкосновеност на личния живот и електронни комуникации подчертава основното значение на поверителността на съобщенията – закрепено в много конституции, поне по отношение на пощата и телефонните разговори (макар че сега често се разпростира изрично или чрез тълкуване и спрямо всички форми на комуникация)[120] – като предвижда, че държавите членки трябва да:

> гарантират **конфиденциалност на комуникацията и свързания трафик на данни** през публични комуникационни мрежи и публично достъпни електронни комуникационни услуги, чрез националното си законодателство. По-специално те ***забраняват слушане, записване, съхранение и други видове подслушване или наблюдение на съобщения и свързаните данни за трафика от страна на лица, различни от потребители*** без ***съгласието*** на заинтересованите потребители, с изключение на законно упълномощени да извършват това … (добавено подчертаване)

Както ясно показват думите „*слушане, записване [и т.н.] … от лица, различни от потребители*", тази разпоредба не просто се прилага спрямо доставчици на електронни комуникационни услуги. По-скоро (при условията на отбелязаните по-долу изключения), държавите членки трябва, съгласно своите национални закони, да забранят тези намеси в правото на поверителност на комуникацията от **когото и да било**, включително държавни агенции и частни лица, като дружества.

Чл. 5, пар. 1 допуска като изключение „*техническото съхранение, което е необходимо за пренасяне на комуникация, без да противоречи на принципа за конфиденциалност*". Има допълнително изключение в Чл. 5, пар. 2 във връзка със записването на съобщения и данни за трафик за осигуряване на доказателства за търговска сделка или бизнес комуникация. Т.нар. Директива за запазване на данни, обсъдена накратко в 1.3.4 по-долу, предвиждаше допълнително, широко-приложимо изключение от тази забрана за подслушване и събиране на данни от съобщения, но беше обявена за недействителна от Съда на ЕС, както е разгледано в този раздел.

*НОВО ***Използването на „бисквитки" и други натрапчиви технологии:***

Изменената Директива 2002/58/ЕО предвижда в чл. 5, пар. 3, с доста техническа терминология, че държавите членки трябва да гарантират, че:

> **съхраняването на информация или получаването на достъп до информация,**

---

120 Вж. широкото тълкуване на института „кореспонденция" в чл. 8 от Европейския съд по правата на човека в известното дело *Klass v. the Federal Republic of Germany* (решение от 6 септември 1978 г.), пар. 41, където Съдът постановява, че „*телефонните разговори … са обхванати от институтите на „личния живот" и „кореспонденцията" [в този член]*".

> **вече съхранявана в крайното оборудване на абоната или ползвателя,** е позволено само при условие, че съответният абонат или ползвател е дал своето **съгласие** след получаване на предоставена **ясна и изчерпателна информация** в съответствие с Директива 95/46/ЕО, inter alia, относно целите на обработката.

Директивата изяснява в следващото изречение в този параграф, че:

> Това не пречи на всякакво техническо съхранение или достъп с единствена цел осъществяване на предаването на съобщение по електронна комуникационна мрежа или доколкото е строго необходимо, за да може доставчикът да предостави услуга на информационното общество, изрично поискана от абоната или ползвателя.

Следва да се отбележи, че фразите „*с единствена цел*" и „*доколкото е строго необходимо*" подчертават, че това изключение трябва да бъде много тясно прилагано.

Фразата „*съхраняването на информация или получаването на достъп до информация, вече съхранявана в крайното оборудване на абоната или ползвателя*" е технически израз за технологии, които позволяват на потребителя на уебсайт да бъде разпознат от уебсайта и проследен докато използва уебсайта или, дори, в различни уебсайтове. Основните средства, използвани за това, са т.нар. „**бисквитки**" – поради което Директивата от 2009 г., която определя по строги правилата в това отношение (като е разгледано по-долу) беше първоначално наричана принципно „**Закона за бисквитките**" на ЕС, и все още понякога се нарича по този начин (като например, уебсайт на частна организация).[121]

Всъщност, има редица бисквитки , които произтичат от техническите международни стандартизирани инструменти, наречени „RFC", приети от Internet Engineering Task Force (IETF), които могат да бъдат разглеждани на ежедневен език в диапазон от силно натрапчиви „**проследяващи бисквитки на трети лица**" до **ненатрапчиви такива**, които подобряват работата на уебсайтовете без да проследяват посетителя;[122] и има други натрапчиви технологии, като „**флаш бисквитки**", **HTML5 методи за съхранение** и т.нар. „**вечни-бисквитки**".[123] Всички те са в рамките на определението за „*информация, съхранявана в крайното оборудване*" и поради това (някак проблематично) всички те са третирани като еднакви съгласно Директивата за правото на неприкосновеност на личния живот и електронни комуникации.[124]

Целта и значението на чл. 5, пар. 3 се обяснява на по-прост език в съображения 24 и 25 към Директивата за правото на неприкосновеност на личния живот и електронни

---

121 Вж., напр.:
https://www.cookielaw.org/the-cookie-law/

122 Вж. също последващите Препоръки на IETF относно бисквитките (започващи с RFC 2109 от 1997 г.), които съдържат неизчерпателна концепция за неприкосновеност на личния живот, но и включват някои полезни задължителни данни в бисквитките. Вж.:
https://tools.ietf.org/html/rfc2109 (оригиналната RFC 2109);
https://tools.ietf.org/html/rfc2965 (RFC 2965, заместваща RFC 2109, но запазваща същия списък с данни); и
https://tools.ietf.org/html/rfc6265 (RFC 6265 от 2011, отново запазваща оригиналния списък, но с въвеждането на трето лице, осъществяващо достъп до бисквитката – сега действащата препоръка).

123 Вж.:
https://webcookies.org/doc/eu-web-cookies-directive

124 Това може да се промени съгласно предложения нов Регламент в областта на правото на неприкосновеност на електронните комуникации, който би могъл да третира различните технологии по различен начин в зависимост от тяхната относителна натрапчивост.

комуникации, които изясняват, че тя се простира много отвъд „бисквитките". Струва си те да бъдат изцяло цитирани:

> Оборудването на терминалите на потребителите на електронни комуникационни мрежи и всяка информация, съхранявана в такова оборудване, се отнасят до частния живот на потребителите, изискващ защита съгласно Европейската конвенция за защита на човешките права и основните свободи. Така наречените **софтуер за наблюдение, уеб грешки, скрити идентификатори и други подобни устройства могат да влязат в терминала на потребителите без тяхното знание, за да получат достъп до информация, да съхраняват скрита информация или да проследяват действията на потребителя и могат сериозно да засягат правото на неприкосновеност на личния живот на тези потребители. Използването на такива устройства трябва да бъде позволено само за законни цели със знанието на заинтересованите потребители.** (добавено подчертаване)
>
> Такива приспособления, обаче, **например така наречените „бисквитки" (cookies)**, могат да бъдат легитимни и полезни средства, например при анализиране на ефективността на дизайна на интернет страницата и рекламиране и проверка идентичността на потребителя, ангажиран в сделки онлайн. Когато такива приспособления (например бисквитки) са предвидени за законни цели, за да се улесни осигуряването на услуги за информационно общество, тяхната употреба трябва да се разреши, при условие че потребителите са снабдени с ясна и точна информация в съответствие с Директива 95/46/ЕО, относно целите на "бисквитките", или подобни приспособления, така че да се гарантира, че потребителите са запознати с информацията, която е поставена в терминалното оборудване, което те използват. Потребителите трябва да имат възможност да откажат да имат бисквитки, или подобни приспособления, поставени в тяхното терминално оборудване. Това е особено важно, когато потребители, различни от оригиналния потребител, имат достъп до терминалното оборудване и по такъв начин — до всякакви данни, съдържащи информация, свързана с правото на неприкосновеност на личния живот, която е съхранена в такова оборудване. Информацията и правото на отказ могат да бъдат предложени веднъж за използване на различни приспособления, които ще се инсталират на терминалното оборудване на потребителя по време на същото включване, и също така обхващащи бъдещо използване, което може да се направи за тези услуги по време на следващи включвания. Методите за даване на информация[, предлагаща право на отказ] [125], или изискваща съгласие, трябва да са възможно най-лесни за ползване от потребителя. Все пак може да се направи достъп до съдържанието на специфична интернет страница, при условие на пълна информираност за приемането на приспособлението бисквитки, или подобно приспособление, ако то се използва с легитимна цел. (добавено подчертаване)

Основната промяна, въведена относно Директивата от 2002 г. беше, че тя промени режима, приложим спрямо употребата на такива технологии от такъв, при който абонатът или потребителят трябваше да бъде информиран и да получи „право да откаже" залагането на бисквитки (и т.н.),[126] на този, който е предвиден понастоящем в

---

125 Относно запазването на предложението за право на отказ, вж. бележка под линия 158, по-долу.

126 В оригиналната версия от 2002 г., първото изречение на чл. 5, пар. 3 гласи следното: *Държавите членки гарантират, че използването на електронни комуникационни мрежи, за да се съхранява информация или да се получи достъп до информация, съхранявана в терминалното оборудване на абоната или потребителя е позволено, само при условие че на заинтересования абонат или потребител е предоставена ясна и цялостна **информация** в съответствие с*

чл. 5, пар. 3, съгласно който бисквитки се позволяват, само при условие че абонатът или потребителят не само е бил информиран, но е и дал **положително, изрично съгласие**, в съответствие с условията за (валидно) съгласие, предвидени в основната Директива за защита на данните от 1995 г.,[127] която определя съгласие като:

> всяко свободно изразено, конкретно и информирано указание за волята на съответното физическо лице, с което то дава израз на своето съгласие за обработка на личните данни, които се отнасят до него. (чл. 2, б. „з“))

С оглед на замяната на Директивата от 1995 г. с ОРЗД, възниква въпросът дали това следва сега да се чете като **по-изискващата форма на съгласие, предвидена в Регламента**. Ако е така, съгласие за използване на бисквитки и такива други инструменти сега би следва да се базира на:

> свободно дадено, конкретно, информирано и **недвусмислено** указание за волята [на абоната или потребителя], чрез което той или тя, **чрез изявление или ясно потвърждаващо действие**, изразява съгласието си [за поставянето на бисквитки или използването на други инструменти][128]

Горното следва да значи, че използването на “предварително отбелязани” полета за употребата на бисквитки и т.н. вече няма да отговаря на изискванията за съгласие в Директивата за правото на неприкосновеност на личния живот и електронни комуникации.

Остава проблемът с това, че Директивата за правото на неприкосновеност на личния живот и електронни комуникации като цяло разглежда всички “бисквитки” и проследяващи инструменти по един и същи начин, без да разграничава, например, “сесийните бисквитки” от “постоянните”.

На практика разпоредбата доведе до интернет култура от вида “приемаш или се отказваш”, при която посетителите на уебсайтовете са на практика принудени да изберат “Съгласен съм” (по отношение на поставянето на обикновено неконкретизирани видове “бисквитки”), за да получат достъп до даден сайт (като тук се включват дори сайтове на публични органи). Проучването SMART установи, че:[129]

> е възможно правилата за бисквитките и подобни похвати да не са постигнали напълно целите си, предвид на това, че потребителите получават твърде много предупредителни съобщения, които не разглеждат внимателно.

Дали това ще се промени при нов регламент за електронна поверителност, остава да видим, но разбира се, тези въпроси са свързани пряко с прилагането на всички основни принципи и права за защита на данните - включително ограничаване на целите, минимизиране на данни, ограничаване на запазването и т.н. , по отношение на въпроси като например какви периоди на запазване са подходящи за различни бисквитки (в зависимост от тяхната цел), как трябва да бъде получено валидно съгласие („съгласие съгласно ОРЗД“) за използването на различни бисквитки и как субектите на данни

---

*Директива 95/46/ЕО, inter alia, относно целите на обработката и е предложено **правото да се откаже** такава обработка от администратора на данни.* (добавено подчертаване)

127 Това изменение не е отразено в съображенията, цитирани в текста, които не са изменяни от първоначалната Директива от 2002 г. и все още сочат „право на отказ”, макар той да премахнат с Директивата от 2009 г. Всъщност, тези думи са станали безпредметни.

128 Срв. Чл. 4(11) ОРЗД. Добавено подчертаване.

129 Резюме на Комисията за резултатите от проучването SMART (бележка под линия 99 по-горе).

следва да упражняват правата си и т.н. - и как тези въпроси могат и трябва да се прилагат въз основа на Защита на данните на етапа на проектиране и по подразбиране - принципът, който сега е изрично заложен в ОРЗД.

*НОВО ***Ограничения на използването на данни за трафик и местонахождение:***

Чл. 6 от Директива 2002/58/ЕО налага строги ограничения за данните и ограничения при съхранението, при обработване на данни за трафик и местонахождение от страна на доставчиците на електронни комуникационни услуги. По принцип **данните за трафик** (т.е., данни, обработвани за целта на – и необходими за – пренасяне на съобщения или за изготвяне на сметка) могат да се обработват и съхраняват от доставчика на съответната електронна комуникационна услуга само за целите на ***пренасяне*** на електронни съобщения, ***изготвяне на сметка*** за абоната за съобщенията или във връзка с ***плащания, свързани с взаимно свързване***(т.е., плащания между доставчици, когато взаимно използват мрежите си) (чл. 6, пар. 1 и пар. 2). Това обработване не изисква съгласието на абоната или потребителя на услугата, защото е необходимо за предоставянето на услугата. Когато данните вече не са нужни за тези услуги, те трябва да бъдат "изтрити или да се направят анонимни" (чл. 6, пар. 1).[130]

Данните за трафик могат да се използват само за ***маркетинг на електронни комуникационни услуги*** или за предоставянето на ***услуги с добавена стойност***, но в тези случаи само със **съгласието** на абоната или потребителя. Отново това означава, че сега, когато ОРЗД се прилага в пълна степен, съгласието трябва да отговаря на изискванията на ОРЗД за валидно съгласие, т.е., съответното съгласие сега трябва да има формата на:

> свободно дадено, конкретно, информирано и недвусмислено указание за волята [на абоната или потребителя], чрез което той или тя, чрез изявление или ясно потвърждаващо действие, изразява съгласието си [за използването на неговите или нейните данни за трафик за маркетинг от доставчици на електронна комуникационна услуга или предоставянето на конкретна услуга с добавена стойност].

В Директивата за правото на неприкосновеност на личния живот и електронни комуникации също така се предвижда, че доставчикът на услугата трябва да **информира** абоната или потребителя на услугите му относно видовете данни за трафик, които се обработват и относно продължителността на това обработване; за обработване на базата на съгласие (т.е., за маркетинг и услуги с добавена стойност: вж. по-горе) това информиране трябва да се направи ***преди получаването на това съгласие*** (чл. 6, пар. 4).

Накрая Директивата за правото на неприкосновеност на личния живот и електронни комуникации предвижда, че обработването на данни за трафик за доставчик на електронни комуникационни услуги за разнообразни **спомагателни цели,** свързани с предоставянето на услугите (***изготвяне на сметки, управление на трафик, запитвания на клиенти, разкриване на измами, маркетинг*** и предоставянето на ***услуги с добавена стойност***) от членове на персонала на доставчика или всеки обработващ, ангажиран от доставчика трябва да бъде **ограничено на база "необходимост да има достъп"**: всеки от тях трябва да има достъп само до такива данни

[130] Относно проблемите с превръщането на тези данни в анонимни вж. разглеждането на въпроса в контекста на ОРЗД във втора част, раздел 2.1 по-долу.

за трафика, които са му необходими за конкретната задача (чл. 6, пар. 5). Все пак "компетентни [външни] органи", например тези, които разрешават спорове, свързани със сметки или с плащания относно взаимно свързване, естествено трябва да получават достъп до данните за трафик при необходимост (чл. 6, пар. 6).

Директивата за правото на неприкосновеност на личния живот и електронни комуникации е дори по-строга по отношение на обработването на "**данни за местонахождение, различни от данни за трафик**", т.е. данни, обработвани в електронна съобщителна мрежа, които посочват ***географската позиция на крайното устройство на потребителя*** (например в общия случай мобилен телефон), но които ***не се обработват за целите на пренасянето на електронно съобщение или изготвяне на сметка за такова съобщение***. Такива данни могат да се обработват само, когато се направят ***анонимни***,[131] или, доколкото могат да бъдат използвани за предоставяне на ***услуга с добавена стойност***, със **съгласието** на потребителите или абонатите на такава услуга (чл. 9, пар. 1, първо изречение). Отново доставчикът на електронната комуникационна услуга трябва да **информира** потребителите и абонатите за подробностите относно обработването, преди получаването на такова съгласие (чл. 9, пар. 1, второ изречение). Тези потребители или абонати трябва също така да могат да оттеглят това съгласие по всяко време (чл. 9, пар. 1, трето изречение), и/или временно да изключат такова проследяване на местонахождението, за което да "имат прости средства и без заплащане" (чл. 9, пар. 2)). И отново, обработването на такива данни трябва да се ограничи до персонала на доставчика на електронните комуникационни услуги или на доставчика на съответната услуга с добавена стойност (или обработващ, ангажиран от някой от двамата) (чл. 9, пар. 3).

*НОВО *Изготвяне на сметки с описание на услугите*

Абонатите трябва да имат правото да изберат да получават **сметки, които не са с описание на услугите** (чл. 8, пар. 1) и държавите членки трябва да предоставят и **други решения, повишаващи неприкосновеността на личния живот** по отношение на сметките с описание на услугите (чл. 8, пар. 2, например сметки с описание на услугите, които показват само страната или регионалните кодове за изходящите обаждания, или които пропускат или скриват последните три цифри от номера, до който е повикването, за да могат едновременно да обяснят сумата на сметката и да защитят неприкосновеността на личния живот на потребителя (който може да не е абонатът или член на семейството).

*НОВО *Идентификация на входящи и изходящи повиквания, и автоматично препращане на повикване*

Доставчиците на електронни комуникационни услуги трябва да предложат на повикващите и повикваните индивиди (включително повикващи от ЕС [тогава ЕО], които се обаждат в трети държави) **опцията да предотвратят идентифицирането на повикващата линия от страна на повикваното лице**, но хората, които получават повиквания от неидентифициран номер (идващ от ЕС/ЕО или не) трябва да могат да **блокират** обаждането; и хората трябва да могат да **изключват** идентифицирането за своята собствена повикваща линия за всяко отделно повикване (чл. 8, пар. 1 – 4).

131 Вж. предишната бележка под линия.

Освен това доставчиците на електронни комуникационни услуги трябва да **информират обществеността** (и, разбира се, особено своите абонати и потребители) относно тези опции (чл. 8(6)).[132]

При спазване на съответните национални правила (и, разбира се, на общите принципи за необходимост и пропорционалност), доставчиците на електронни комуникационни услуги могат да **отменят блокирането** на идентификацията на повикващата линия или при искане на абоната ***да се проследят злонамерени или нарушаващи спокойствието повиквания*** (за да могат доставчиците и полицията да разследват жалби и да се осигурят доказателства при съдебни дела), или за да се съдейства на службите за спешна медицинска помощ и противопожарната служба ***при отзоваването на спешни повиквания*** (чл. 10, пар. 1 и пар. 2).

Абонатът трябва също така да има "*възможността, като използва безплатно прости средства, да* ***спре автоматично изпращане на повикване*** *от трета страна до терминала на абоната*" (чл. 11).

Всички горепосочени задължителни опции са пренесени в международни технически норми, така че сега могат лесно да се използват в практика по отношение на смартфони и т.н.

*НОВО ***Указатели на абонати***

В резултат на натиска от национални органи по защита на данните, Директивата за правото на неприкосновеност на личния живот и електронни комуникации включва разпоредби, според които абонатите трябва да бъдат информирани за всякакво намерение за включване на техни данни (т.е. техен стационарен или мобилен телефонен номер) в **указател на абонати**, който е или ***публично достъпен*** или ***достъпен чрез услуги за справка в указатели***; и те трябва да имат възможност да не бъдат включвани в такива указатели (т.е., **да бъдат „извадени от указателя"**), безплатно и без да е необходимо да дават причини за това (чл. 12, пар. 1 и пар. 2).[133]

Тези права се прилагат за физически лица – но държавите членки трябва също да вземат необходимите мерки, за да осигурят „законните интереси на абонати с изключение на физически лица [т.е., на „юридически лица", като дружества]" да бъдат също „достатъчно защитени" в тези отношения (чл. 12, пар. 4).

Ако даден указател е предназначен да бъде използван за "***всяка цел … освен тази за търсене на координати*** *на лица на база техните имена и когато е необходимо*

---

[132] Тези опции първоначално бяха разработени от националните органи за защита на данните. Любопитно е, че тези опции за разлика от техническите стандарти за бисквитките бяха интегрирани в техническите международни стандарти за пренос на телекомуникационния пренос (едновремешните фиксирани телефонни линии) в момента, когато услугите за "идентифициране на повикващата линия" и т.н. бяха комерсиално предложени през 80-те години на двадесети век, а след това с появата на мобилните телефони – в мобилните телефони, за да се активират опциите. Това се случи благодарение на регулаторните органи на Франция и Германия, които поставиха тези въпроси с преговарящите от страна на европейските телекоми, които тогава тласнаха тези цялостни и лесни за употреба решения на глобално ниво чрез нормите за GSM.

[133] На практика, към онзи момент невключването на телефонен указател е водело до по-малък брой обаждания – което е означавало по-малки печалби за телефонните оператори, тъй като към онзи момент телефонните обаждания са били заплащани всяко поотделно – докато около 20% от абонатите са искали да не бъдат включвани в телефонни указатели. С днешния интернет, е още по-важно потребителите да не бъдат обезпокоявани с телефонни обаждания, ако техните телефонни номера са публикувани.

минимален брой други идентификатори" – напр., ако тези данни са предназначени за използване за ***директен маркетинг***, определяне на ***кредитен рейтинг***[134] или ***политически кампании*** – от абонатите трябва да бъде поискано **допълнително съгласие**, специално за използването на данните им за такива други цели (чл. 12, пар. 3).[135]

*НОВО ***Нежелани съобщения***

Както беше отбелязано в 1.3.2, по-горе, Директивата за защита на данните от 1995 г. вече дава на субектите на данни безусловното **право на възражение** срещу използването на каквито и да е техни лични данни за целите на директен маркетинг (чл. 14, б. „б" от Директивата от 1995 г.) – като се има предвид маркетинг от каквото и да е естество, търговски, политически или друг. Към съответния момент, това е все още свързано най-вече с маркетинг по пощата. Директивата за правото на неприкосновеност на личния живот и електронни комуникации допълва към това изискването за **предварително съгласие** за използването на ***автоматизирани набиращи системи*** и ***факсове***[136] или ***email*** („електронна поща") за такива цели (чл. 13, пар. 1). Причината е, че изпращането чрез тези средства е много по-евтино от използването на традиционната поща, и поради това е вероятно да доведе до увеличение на тяхното използване. Това изискване се прилага във връзка както с физически, така и с юридически лица (физически лица и дружества, и т.н.). Нещо повече, както беше отбелязано по-рано, в точка „*Предназначение, цел и обхват на Директивата за правото на неприкосновеност на личния живот и електронни комуникации*", тази разпоредба се прилага към **каквато и да е организация**, която желае да използва такива средства за изпращане на директни маркетингови съобщения.

Ако обаче клиент предостави електронни данни за контакт (телефонен номер или адрес на електронна поща, и т.н.) на дружество в контекста на продажба на продукт или услуга, продавачът може да използва тези детайли за **маркетинг на собствени подобни продукти или услуги на такъв клиент** (т.нар. "***мобилен маркетинг чрез близко разположени системи***"), при условие, че на клиента се предлагат лесни начини да възрази на такива подходи във всяко съобщение (т.е. освен ако всяко съобщение не съдържа опция за "о**тписване**" от следващи маркетингови съобщения) (чл. 13, пар. 2).

По отношение на другите форми на директен маркетинг (т.е., директен маркетинг, различен от мобилния маркетниг чрез близко разположени системи и маркетинг, който използва средства, различни от автоматично набиране, факс машини или електронна поща), държавите членки могат да **избират** между предварително съгласие (т.е.,

---

134 Вж. "**Практика на червената черта**": практиката на различно третиране при даването на заем, настаняване, застраховане и други услуги въз основа на адреса на лицето и историята на тази зона по подразбиране – практика, обявена за незаконна в САЩ преди много години. Вж., напр.,:
https://www.investopedia.com/terms/r/redlining.asp
Също: Как расистките ефекти на практиката на червената черта траят десетилетия (*How Redlining's Racist Effects Lasted for Decades)*, NY Times, 24 август 2017, достъпно на:
https://www.nytimes.com/2017/08/24/upshot/how-redlinings-racist-effects-lasted-for-decades.html
(с карти, които илюстрират практиката)

135 Не е ясно дали това се прилага и към "юридически лица", тъй като този параграф не е споменат в четвъртия параграф на чл. 12, отбелязан по-горе.

136 "Факс машина" или "факс" е машина, която позволява изпращането на изображение (често изображение на документ) по телефонна мрежа. Понастоящем употребата им е рядка. Вж.:
https://faxauthority.com/fax-history/

"**вписване**", което се предлага към момента на събиране на личните данни) и модел на „отписване" ("информиран, но не възразил") (чл. 13, пар. 3).[137] Изпращането на директни маркетингови съобщения по електронна поща обаче *„прикриваща или скриваща идентичността на подателя, от чието име се прави комуникацията, или без валиден адрес, на който получателят да може да изпрати искане да се спрат такива съобщения*", трябва във всички случаи да бъде забранено (чл. 13, пар. 4).

Дерогации:

Чл. 15 от Директивата за правото на неприкосновеност на личния живот и електронни комуникации пояснява, че Държавите членки могат да ограничат различните права и задължения, предвидени в директивата на същото основание, както при широката клауза за дерогация „**важни обществени интереси**" в основната Директива за защита на данните от 1995 г. (чл. 13), т.е., *„когато такова ограничаване представлява необходима, подходяща и пропорционална мярка в рамките на демократично общество, за да гарантира* ***национална сигурност*** *(т.е държавна сигурност),* ***отбрана, обществена безопасност*** *и* ***превенцията, разследването, разкриването и преследването на криминални нарушения***" – към което Директивата за правото на неприкосновеност на личния живот и електронни комуникации просто добавя: „***или неразрешено използване на електронна комуникационна система***". Подчертаните думи са подсилени в Директиватачрез допълнителната изрична постановка, че:

> Всички мерки, упоменати в настоящия параграф, трябва да бъдат в съответствие с общите принципи на законодателството на Общността, включително онези, упоменати в чл. 6, пар. 1 и 2 от Договора за Европейския съюз.
>
> (чл. 15, пар. 1, последно изречение)

Посочените членове от Договора за създаването на Европейския съюз, препращат съответно към Хартата на основните права на Европейския съюз (обявена през 2000 г., т.е. след влизането в сила на Директивата за защита на данните от 1995 г.) и Европейската конвенция за правата на човека.

Докато това е желано изрично потвърждение на ключовото изискване на основните норми на ЕС за зачитане на основните права и свободи, то разбира се реално не е ново: относимите принципи за върховенство на закона са били практически (и юридически) вече прилагани още към момента на приемането на Директивата -"майка", като общи принципи на Правото на Общността.[138]

Чл. 15, пар. 1 предвижда също, че с цел да се защитят различните изброени „важни обществени интереси", но при условията на ключовото *предупреждение* за зачитането на правата на човека и основните принципи на Правото на Общността:

> Държавите членки могат, inter alia, да одобрят законодателни мерки, предвиждащи **съхранението на данни за ограничен период**, оправдани на основанията, изложени в настоящия параграф.

---

137 Моделът на ЕС за „отписване" изисква информиране на субекта на данни за: (i) намерението за използване неговите данни за директен маркетинг; (ii) правото им да се отпишат от такъв маркетинг; и (iii) подробностите за това как (просто и безплатно) да упражни това право. Отбележете, че Европейския модел на „отписване" се различава принципно от този в САЩ, който не изисква информирането на субекта на данни за тези подробности.

138 Вж. бележка под линия 63, по-горе.

(Чл. 15, пар. 1, второ изречение)

Оригиналният текст, с изричните му **ограничения, свързани с върховенството на закона, които ефективно забраняват безразборното запазване на данни**, е важен с оглед на последващите опити на Европейския законодател да наложи точно такива задължения, свързани с безразборното запазване на данни, съгласно т.нар. Директива за запазване на данни, в крайна сметка обявена за недействителна от съда на Европейския съюз, както беше обсъдено в т. 1.3.4 по-долу.

*РАЗЛИКА ***Надзор и прилагане***

Докато Директивата за защита на данните от 1995 г. е била прилагана от специализирани, независими органи по защита на данните и ОРЗД се прилага от същите тези органи, Държавите-членки на ЕС биха могли да избират да поставят надзора и прилагането на Директивата за правото на неприкосновеност на личния живот и електронни комуникации в ръцете на различен орган, или на различни органи. Това е довело до различно разпределяне на надзора на различни органи във връзка с различните въпроси, обхванати от Директивата за правото на неприкосновеност на личния живот и електронни комуникации в държавите членки. [139]

Комисията установява, че "разпределянето на компетентностите по прилагането на широк спектър от органи, които често се припокриват", също, изглежда, че "затруднява ефективността на правилата при трансгранични случаи".[140]

Прилагане на други основни елементи от Директивата за защита на данните от 1995 г.:

Накрая, в този преглед на правилата в Директивата за правото на неприкосновеност на личния живот и електронни комуникации, следва да бъде отбелязано, че изрично се предвижда, че изискванията на Директивата от 1995 г. по отношение на **съдебните средства за защита, отговорността и санкциите** (посочени по-горе, в раздел 1.3.2) следва да се прилагат и във връзка с Директива 2002/58/ЕО (чл. 15, пар. 2); освен това **Работната група по член 29** (също обсъдена в този раздел) следва да изпълнява задачите си, посочени в Директивата от 1995 г. във връзка с Директива 2002/58/ЕО (чл. 15, пар. 3); и че държавите членки трябва да предвидят „ефективни, пропорционални и възпиращи" санкции за нарушения на Директивата (чл. 15а).

Регламент (ЕО) 45/ 2001 също създаде Европейския комитет по защита на данните като независим контролен орган с отговорност за наблюдение на обработването на лични данни от европейските институции и органи и изиска определянето на длъжностно лице по защита на данните (ДЛЗД) от всяка от тези институции или органи.

Регламент (ЕО) 45/ 2001 бе отменен от Регламент (ЕС) 2018/ 1725, който влезе в сила на

---

139 Работен документ на Комисията (бележка под линия 99, по-горе), раздел 6.1.3, *Diversity of competent authorities* (Разнообразие на компетентни органи), стр.23. За подробности, вж. дългият списък на различни органи в държавите членки, на които са били възложени надзорни и изпълнителни правомощия по различни аспекти на Директива 2002/58/ЕО, в *Приложение VI* към Работния документ на Комисията.

140 *Вж*.

11 декември 2018, както е изложено в подраздел 1.4.5 по-долу.

1.3.4 7Инструменти за защита на данните в „Третия стълб.[141]

В периода от средата на 90-те до 2009 г. ЕС създаде значителен брой органи, насочени към улесняване на сътрудничеството между държавите-членки в областта на полицията и наказателното право („Правосъдие и вътрешни работи“ или ПВР) - т.нар. „Трети стълб“ на ЕС [142]- всички са съсредоточени върху създаването на общоевропейски лични бази данни и правила и процедури за достъп до тези бази данни и обмен на лични данни между държавите-членки.

Те включват Европол (1998 г.), Шенгенската информационна система, ШИС-I (2001 г., актуализиран до ШИС II през 2013 г.), Евроджъст (2002 г.), Евродак (2003 г.), Визовата информационна система, ВИС (2004 г.) и Митническата информационна система , ОНД (2009).

В този период Съветът прие около 123 инструмента в областта на ПВР. [143]През 2005 г. Прюмската конвенция беше подписана от седем държави-членки и със своето решение от 23 юни 2008 г. Европейският съвет се съгласи да интегрира основните разпоредби на Конвенцията от Прюм в правната рамка на ЕС, за да се даде възможност за по-широк обмен (между всички държави-членки на ЕС) на биометрични данни (ДНК и пръстови отпечатъци) в борбата срещу тероризма и трансграничната престъпност.

През 2008 г. от Съвета беше прието всеобхватно рамково решение за установяване на общи принципи за защита на личните данни в областта на ПВР. [144]Въпреки че много от правилата в Рамковата директива от 2008 г. са вдъхновени от Директива 95/46 / ЕО и Конвенцията на Съвета на Европа, както тогавашният ръководител на европейския надзорен орган по защита на данните Питър Хустинкс отбеляза, „нивото на защита беше много по-ниско по отношение на обхвата и същността. [145]“Що се отнася до обхвата, той посочи, че:[146]

> Решението се прилага само когато личните данни се предават или предоставят на други държави-членки и следователно не се разпростират до „вътрешна“ обработка [т.е. обработка от и в държава-членка], за разлика от Директива 95/46 / ЕО.

---

[141] За подробности относно закона в тази област вижте историческите раздели в съответните глави в: Steve Peers, (2016). Право на ЕС за правосъдие и вътрешни работи: Том I: Закон за имиграцията и убежището на ЕС (четвърто издание) и том II: Наказателно право, полицейско право и гражданско право на ЕС (четвърто издание), и двете Oxford University Press, 2016.

[142] Вижте бележка под линия 58 по-горе.

143 Вижте Емилио Де Капитани, Метаморфоза на третия стълб: Краят на преходния период за наказателно и полицейско законодателство на ЕС, блогспот на ЕС за анализ на правото, 10 юли 2014 г., достъпен на:

https://eulawanalysis.blogspot.com/2014/07/metamorphosis-of-third-pillar-end-of.html

144 Рамково решение 2008/977 / ПВР на Съвета от 27 ноември 2008 г. относно защитата на личните данни, обработвани в рамките на полицейското и съдебното сътрудничество по наказателни дела, ОВ L 350, 30 декември 2008 г., стр. 60, наличен на:

145 Peter Hustinx, Закон за защита на данните на ЕС: Прегледът на Директива 95/46 / ЕО и предложеният общ регламент за защита на данните, стр. 15, наличен на:

https://www.statewatch.org/news/2014/sep/eu-2014-09-edps-data-protection-article.pdf

[146] съображение 7 и член 1 от рамковото решение.

През 2009 г., след влизането в сила на Договора от Лисабон, който прекрати тристълбовата структура[147], започна петгодишен преходен период, по време на който правото на ЕС в сферата на ПВР трябваше да бъде прието в подходящата наднационална правно-конституционна рамка на ЕС (вж. Раздел 1.4 .2, по-долу)[148]. През 2018 г. Рамковото решение от 2008 г. беше заменено с ново решение (същото).

1.3.5 Защита на данните във „Втория стълб“.

Неформална система за „Европейско политическо сътрудничество“ (ЕПС) по външни въпроси съществуваше от 1970 г. до 1993 г. Съгласно Договора от Маастрихт, който влезе в сила през последната година, това беше официално оформено в „Обща външна политика и политика на сигурност“ (ОВППС)) - вторият стълб на ЕС. Въпреки това, до по-нататъшното развитие на ОВППС съгласно Договора от Лисабон от 2009 г. (който премахва структурата на „стълбовете“), [149]както е разгледано в раздел 1.4.4 по-долу, нямаше конкретни правила за защита на данните, приложими при обработката на лични данни в тази област (различна от законите за защита на данните на държавите-членки и Конвенцията на Съвета на Европа).

1.3.6 Защита на данните за институциите на ЕС

Нямаше цялостни или съгласувани правила за защита на данните, приложими за самите институции на ЕС до 2001 г., когато Регламент - Регламент (ЕО) 45/2001 - за първи път въведе такива правила въз основа на член 286 от ДЕС, който изискваше такива правила.[150]

Правилата за защита на данните в Регламента от 2001 г. се основават на съществуващите тогава правила на Общността за защита на данните, приложими към държавите-членки, по-специално Директивата за защита на данните от 1995 г. и Директивата за електронната поверителност от 2002 г.

Регламент 45/2001 също установява Европейския надзорен орган по защита на данните като независим надзорен орган, който отговаря за мониторинга на обработването на лични данни от институциите и органите на Общността, и изисква назначаването на длъжностно лице по защита на данните (DPO) от всяка от тези институции или тела.

Регламент (ЕО) 45/2001 беше отменен с Регламент (ЕС) 2018/1725, който влезе в сила на 11 декември 2018 г., както е разгледано в раздел 1.4.5 по-долу.

147 Вижте отново бележка под линия 58 по-горе
148 Вижте Протокол 36 към Договора от Лисабон и Emilio De Capitani, о.с. (бележка под линия 141, по-горе).
149 Вижте отново бележка под линия 58 по-горе.
150 Регламент (ЕО) № 45/2001 на Европейския парламент и на Съвета от 18 декември 2000 г. относно защитата на лицата по отношение на обработването на лични данни от институциите и органите на Общността и относно свободното движение на такива данни, ОВ L 8, 12 януари 2001 г., стр. 1–22, наличен на:
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32001R0045

1.4 Развитие на правото в областта на защита на данните в бъдеще

До края на първото десетилетие на 21 век, стана ясно, че инструментите за защита на данните от 20 век, по-горе разгледани в раздел 1.3, вече не са достатъчни: та са създадени и изготвени преди масовия достъп до интернет (или поне глобалната мрежа), повсеместното (и мобилното) изчисляване, „Големите обеми от данни", „Интернет на нещата" (IoT), задълбоченото профилиране, алгоритмичното вземане на решения и „Изкуственият интелект" (ИИ). Затова както в ЕС, така и в Съвета на Европа , бяха изготвени нови или актуализирани („осъвременени") инструменти за защита на данните, както е обсъдено в този раздел.

1.4.1 Общ регламент относно защитата на данните на ЕС

Европейската комисия предложи приемането на Общ регламент относно защитата на данните (ОРЗД) през 2012 г.,[151] който да посрещне предизвикателствата, свързани с новите технологии и услуги. Тя предвиди , че силната защита на данните на високо ниво е съществено условие за спечелването на доверие в онлайн пространството, което е само по себе си „*ключ към икономическото развитие*"; новият, актуализиран *lex generalis* (*специалния закон отменя (замества) общия*) режим на защита на данните трябваше да играе „*централна роля в Програмата в областта на цифровите технологии за Европа, и по-общо в Стратегията Европа 2020*".[152]

Предисторията, състоянието, подходът и ключовите елементи от ОРЗД са описани подробно в Част Втора от този наръчник. Достатъчно е да се отбележи, че ОРЗД значително **разширява и укрепва основните принципи и правила**; изрично **добавя генетични и биометричните данни към списъка с чувствителните данни** (това е вдъхновено от работата по „осъвременената" Конвенция на Съвета на Европа за защита на данните, разгледана по-долу в 1.4.3). Целта е да доведе до **по-голяма хармонизация** на правото в областта на защитата на данните в държавите членки на ЕС (поне в тези области, където то се прилага, което в общи линии е областта, по-рано наричана „Първи стълб" на Европейската общност), в съответствие с важната нова практика на Съда на ЕС – макар и да е предмет на широка гама от т.нар. уточняеми клаузи (т. е., клаузи, оставящи по детайлното уреждане на някои въпроси на законите на държавите членки, съобразявайки се с цялостната рамка на ОРЗД, на Договорите за Европейския съюз, както се тълкуват от Съда на Европейския съюз и на конституционните и общоправни

---

[151] Предложение за Регламент на Европейския Парламент и на Съвета относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни (Общ регламент относно защитата на данните), COM(2012) 11 final, Брюксел, 25.01.2012 г., намиращо се на:
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012PC0011&from=EN
В същото време, Комисията предложи и отделен инструмент за защита на данните, Предложение за Директива относно „защитата на физическите лица във връзка с обработването на лични данни от компетентните органи за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказателни санкции и относно свободното движение на такива данни, (COM(2012) 10 final) – но тази директива не се обсъжда в този наръчник (вж. Бележката в кутията „*Относно този наръчник*", на стр.1 от наръчника).

[152] Предложение за Общ регламент относно защитата на данните (предишна бележка под линия), стр.1 – 2 (с препратки към основните документи в Програмата в областта на цифровите технологии и Стратегията Европа 2020). Приемникът на Програмата в областта на цифровите технологии е Стратегията за цифров единен пазар („Стратегия за ЦЕП").

системи на държавите членки)[153]; Регламентът предвижда **по-силни (и някои нови) права на субектите на данни**; позволява **много по-тясно трансгранично сътрудничество** между органите за защита на данните (ОЗД) на държавите членки; и следва да доведе до **по-добро, по-последователно прилагане и изпълнение** на правилата.

По-конкретно, както вече бе отбелязано във Въведението към този наръчник, ОРЗД въвежда (или, поне, прави много по-конкретен) **– сега фундаменталния и задължителен във всички държави членки – принцип на "отчетността"**, и в много случаи (включително във връзка с всички публични органи,които попадат в обхвата на Регламента) сега ***изисква*** установяването на **назначени от администратора или обработващия лични данни длъжностни лица по защита на данните** (**ДЛЗД**).

Както е обяснено във Втора част, двете са свързани: по силата на ОРЗД длъжностните лица по защита на данните ще бъдат хората, които на практика ще трябва да осигурят спазването на принципа на отчетност от и в рамката на организациите, към които принадлежат.

1.4.2 Предложеният Регламент на ЕС в областта на правото на неприкосновеност на електронните комуникации

Въпреки че, както е отбелязано в предходния подраздел, една от основните цели на предложения Общ регламент относно защитата на данните (ОРЗД) беше да посрещне предизвикателствата, произтичащи от **липсата на доверие (по-специално, да спечели доверието на потребителите) в онлайн пространството**, на Комисията отне още пет години, за да предложи нов инструмент, който да замени правилата, които са най-конкретно свързани с тази среда, т.е., ePrivacy directive (Директива 2002/58/ЕО), разгледана по-горе в раздел 1.3.4 (която, макар и частично остава в сила).

Това става под формата на предложение, публикувано през януари 2017 г., за замяна на ePrivacy directive с регламент, **предложения Регламент в областта на правото на неприкосновеност на електронните комуникации.**[154]

Предложението е все още в началнитефази на законодателния процес: към момента на изготвяне (месец декември 2018 г.), той все още се обсъждаше вътрешно в рамките на Съвета) и е обект на голямо внимание както от вносителите (групите за граждански свободи, потребителите и групите за цифровите права)[155], така и от противниците (включително някои от големите американски „Интернет гиганти", които искат или пълно оттегляне на предложението или неговото значително смекчаване).[156] Поради

---

[153] Вж. Част втора, раздел 2.2 по-долу, подзаглавие „…но с „уточняващи разпоредби".

[154] Предложение за Регламент на Европейския Парламент и на Съвета относно зачитането на личния живот и защитата на личните данни в електронните съобщения и за отмяна на Директива 2002/58/ЕО (Регламент за неприкосновеността на личния живот и електронните съобщения), COM(2017) 10 final, Брюксел, 10.01.2017 г., намиращо се на: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017PC0010&from=EN

[155] Вж. Открито писмо до европейските държави членки относно реформата в областта на неприкосновеност на електронните комуникации, изпратено от голяма група неправителствени организации на 27 март 2018 г., намиращо се на: https://edri.org/files/eprivacy/20180327-ePrivacy-openletter-final.pdf

[156] Вж.: Corporate Europe Observatory, *Shutting down ePrivacy: lobby bandwagon targets Council* (*Закриване на неприкосновеността на електронните съобщения: лобисти атакуват Съвета*), 4 юни 2018 г., намираща се на:

това е наистина твърде рано да се обсъжда тук в детайли предложения регламент: несъмнено, окончателният вариант поне в някои отношения ще се различава значително от предложението.

Поради тази причина, за това първо издание на наръчника, ще трябва да се задоволим просто да представим **само ключовите точки на предложението на Комисията**, както са изложени от самата Комисия:[157]

> Предложението за Регламент на високо ниво на правилата за неприкосновеност за всички електронни съобщения включва:
>
> - **Нови участници:** правилата в областта на личния живот [*и защитата на данните*] ще се прилагат в бъдеще и спрямо нови [*т.нар. „Over-The-Top" или OTT*] участници, предлагащи електронни комуникационни услуги, като WhatsApp (Уотсъп), Facebook Messenger (Фейсбук месинджър) и Skype (Скайп). Това ще гарантира, че тези популярни услуги осигуряват същото ниво на защита на поверителност на съобщенията както традиционните телекомуникационни оператори.
> - **По-строги правила:** всички хора и предприятия в ЕС ще се ползват с еднакво високо ниво на защита на електронните си съобщения посредством този пряко приложим Регламент. Предприятията също ще се възползват от един общ набор от правила в целия ЕС.[158]
> - **Съдържание на съобщенията и метаданни:** гарантира се поверителността на съдържанието на съобщенията и метаданните, напр. времетраене на повикването и местонахождение. Метаданните имат висок компонент за поверителност, и трябва да бъдат анонимизирани или заличени, ако потребителите не са дали съгласието си, освен ако данните не са необходими за таксуване.[159]
> - **Нови бизнес възможности:** след като бъде дадено съгласие данни от съобщения – съдържание и/или метаданни – да бъдат обработвани, традиционните телекомуникационни оператори ще имат повече възможности да предоставят допълнителни услуги и да развиват своя

---

https://corporateeurope.org/power-lobbies/2018/06/shutting-down-eprivacy-lobby-bandwagon-targets-council

[157] https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation (удебелено - оригинал; думите в квадратни скоби и курсив и бележките под линия са допълнително добавени)
За по-подробен, критичен анализ на предложението на Комисията, вж.: E-Privacy revision: An analysis from civil society groups (Редакция на неприкосновеността на електронните съобщения: Анализ от групите на гражданското общество), което може да бъде намерено на: https://edri.org/files/epd-revision/EDRi_ePrivacyDir-final.pdf

[158] Но имайте предвид, че това ще зависи от липсата в правилата в Регламента в областта на правото на неприкосновеност на електронните комуникации на „гъвкави" разпоредби, каквито се съдържат в ОРЗД (вж. Втора част, раздел 2.1, по-долу). Ако окончателният текст на Регламента в областта на правото на неприкосновеност на електронните комуникации съдържа такива „гъвкави" разпоредби (което е много вероятно), ще бъде от решаващо значение – специално за онлайн средата, която по същността си е транснационална – да се добави разпоредба за "приложното право".

[159] Но имайте предвид, че продължаващите опити на държавите членки и на Комисията да задържат или въведат повторно задължително запазване на (мета-)данните за електронни съобщения: вж. раздел 1.3.4, по-горе.

бизнес. Например, те биха могли да произвеждат термо- карти, индикиращи присъствието на хора; те биха могли да помогнат на публичните органи и на транспортните компании при разработването на нови инфраструктурни проекти.

- **Опростени правила за „бисквитките“:** разпоредбата за „бисквитките“, която доведе до претоварване с молби за съгласие за интернет потребителите, ще бъде опростена. Новото правило ще бъде по-удобно за потребителите, тъй като настройките на браузърите ще осигуряват лесен начин за приемане или отказ на „бисквитките“ за проследяване и други идентификатори. Предложението, също така, разяснява, , че не е необходимо съгласие за (неконфиденциални) подобряващи работата в интернет бисквитки, които не нарушават неприкосновеността на личния живот (напр. за запомняне на историята на кошницата с покупки) или „бисквитките“, използвани от даден уебсайт за преброяване на броя посетители.

- **Защита срещу спам:** това предложение забранява непоисканите електронни съобщения по електронната поща, SMS (СМС-те) и автоматизираните повиквания. *В зависимост от националното законодателство* хората или ще бъдат защитени по подразбиране, или ще имат възможност да използват списък с лица, които да не бъдат набирани, за да не получават маркетингови телефонни обаждания.[160] Набиращите с маркетингова цел трябва да показват телефонния си номер или да използват специален код, указващ, че това е маркетингово обаждане.

- **По-ефективно прилагане:** прилагането на правилата за поверителност в Регламента ще бъде отговорност на органите за защита на данните, които вече отговарят за правилата по Общия регламент относно защитата на данните.

1.4.3 Директивата за защита на личните данни в полицейската и наказателната дейност от 2016 г.

Въведение

Член 10 (1) от протокол № 36 към Договорът от Лисабон от 2009 година установи транзиционен период преди пълните правомощия на Комисията и на Съда на Европейския съюз да се прилагат по отношение на актове на ЕС в областта на полицейското и на съдебното сътрудничество по наказателноправни въпроси, приети преди влизането в сила на Договора от Лисабон (предишния трети стълб на ЕС). Този транзиционен период приключи на 1ви декември 2014.

През 2012 Комисията подаде предложенията си за директива в тази област, заедно с предложението си за Общ регламент относно защитата на данните (представен в раздел 1.4.1 по-горе и разгледан по-подробно в Част Втора на този наръчник).[161] Въпреки това,

[160] Точно такава „гъвкава” разпоредба като посочената в бележка под линия 179 по-горе – и която илюстрира необходимостта от правило за „приложимото право”, което да изяснява кое от различните национални правила ще се прилага спрямо трансграничните маркетингови писма.

[161] Вж. бележка 143 по-горе.

точно както и ОРЗД, Директивата за защита на личните данни в полицейската и

наказателната дейност бе приета едва 2016 година в същия ден като ОРЗД.[162] За разлика от ОРЗД, който поради качеството си на регламент, е директно приложим в правния ред на държавите членки (въпреки че, в случая, със значителен брой клаузи, които изискват допълнително „уточняване“ в националното право),[163] Директивата за защита на личните данни в полицейската и наказателната дейност, в качеството си на директива, не се прилага директно (т.е., няма „директен ефект“), а трябва да **бъде „транспонирана“ в националното право.** Това трябваше да бъде направено в срок до две години от официалното влизане в сила на директивата, т.е., до 6 май 2018 (само няколко седмици преди ОРЗД да стане приложим на 25 май същата година).

Все пак трябва да се отбележат обширните по-дълги срокове за изпълнение предвидени в членове 61 – 63 от Директивата поради различните обстоятелства около огромния брой засегнати дейности по обработка на данни, които ще бъдат накратко обсъдени в края на този раздел относно Директивата за защита на личните данни в полицейската и наказателната дейност под заглавието „Забавено транспониране“.

Тук следва да е достатъчно да отбележим основните характеристики и изисквания на Директивата за защита на личните данни в полицейската и наказателната дейност.[164]

Директива вместо рамково решение на Съвета

Първото, което трябва да се отбележе е, че излагането на правилата за обработване на лични данни в директива е само по себе си **значително подобрение** в сравнение с това те да се съдържат в рамково решение на Съвета, като това от 2008 година, отменено от Директивата за защита на личните данни в полицейската и наказателната дейност.[165] В качеството си на директива, тя може да бъде използвана пред национални съдилища (и в краен случай пред Съда на Европейския съюз) от лица в искове срещу държавата и е предмет на изпълнителните правомощия на Комисията, които целят да осигурят, че подобни инструменти биват правилно транспонирани в националното право.

Обхват на Директивата за защита на личните данни в полицейската и наказателната дейност (Директива (ЕС) 2016/680)

i- Засегнати дейности

Относно обхвата, Директива (ЕС) 2016/680 постановява следното:

Обхват

1. Настоящата директива се прилага за обработването на лични данни от компетентните органи за целите, посочени в член 1, параграф 1.
2. Настоящата директива се прилага за обработването на лични данни изцяло или частично с автоматични средства, както и за обработването с други средства на лични данни, които са част от регистър с лични данни или са предназначени да съставляват част от такъв регистър.
3. Настоящата директива не се прилага за обработването на лични данни:

а) в хода на дейности, които са извън обхвата на правото на Съюза;

б) от институциите, органите, службите и агенциите на Съюза.[166]

[166] Обработването на лични данни от институциите, органите, службите и агенциите на ЕС за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления е предмет на специален набор правила, съдържащи се в Глава IX от новия регламент относно

В „компетентните органи“ трябва да бъдат установени точни разграничения между обработването на данни предмет на Директивата за защита на личните данни в полицейската и наказателната дейност и тези предмет на ОРЗД като се има предвид Съображение (12). Последното му изречение изяснява, че обработванията на лични дании свързани с *„други задачи“* поверени на „ компетентните органи“, чието изпълнение *„не е непременно свързано с целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления, включително предпазването от заплахи за обществената сигурност и тяхното предотвратяване“*, са предмет на ОРЗД, а не на Директивата за защита на личните данни в полицейската и наказателната дейност.

Администраторът ще трябва да отдели особено внимание на това разграничение и на други въпроси като степента, до която събирането и обработването на лични данни, свързани с “ инциденти“, за които *все още не е ясно* дали съставляват престъпление, или свързани с предприемането на мерки (включително *„принудителни мерки“*) на демонстрации и големи спортни събития, които *„могат да доведат до извършването на престъпление“* (или не), са предмет на Директивата за защита на личните данни в полицейската и наказателната дейност, тъй като отговорите на тези въпроси имат значителни последствия върху нивото на защита на данните, което трябва да бъде подсигурено, напр. относно информирането на субекти на данни, ограничение на съхранението, ограничаване на правата на субекти на данни и т.н.. В същото време длъжностните лица по защита на данните, работещи с въпросните органи трябва да се целят да подпомагат на органите по отношение на тези преценки, с оглед да се осигури подходящите нива на защита на данните във всеки контекст.

обработването на лични данни от институциите на ЕС, Регламент (ЕС) 2018/1725, както накратко е обяснено в раздел 1.4.5 по-долу.

163 Вж. Част Втора, раздел 2.2., по-долу.

164 Както е обяснено в началото на този наръчник, ние се надяваме да разгледаме по-обширно правото на ЕС относно защитата на данните извън ОРЗД във второ издание. То би разгледало по-специално правилата от Директивата за защита на личните данни в полицейската и наказателната дейност, които са резюмирани на кратко тук.

165 Вж. Steve Peers, The Directive on data protection and law enforcement: A Missed Opportunity?, Statewatch Analysis blog, април 2012 (оригинален текст), който може да бъде намерен на: https://www.statewatch.org/analyses/no-176-leas-data%20protection.pdf

166 Обработването на лични данни от институциите, органите, службите и агенциите на ЕС за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления е предмет на специален набор правила, съдържащи се в Глава IX от новия регламент относно обработването на лични данни от институциите на ЕС, Регламент (ЕС) 2018/1725, както накратко е обяснено в раздел 1.4.5 по-долу.

Понятието **„обществена сигурност“** обикновено се използва в контекста на изключения в правото на ЕС, т.е., за да посочи основания, които могат да бъдат използвани, за да оправдаят дейност, която иначе би била в нарушение на правото на Съюза. Както отбелязва Панос Котракис, *„[О]бществената сигурност представлява основание за изключения по отношение на всичките четири свободи по силата на основните правила на Съюза.“*[167]

> От всички основания за изключение от свободата на движение, **обществената сигурност е най-тясно свързана с това, което обикновено определяме като сърцевината на националния суверенитет, който е сферата от дейности, в която държавата има главната отговорност да защитава територията и гражданите си.** (добавено подчертаване)

Водещето решение на Съда на Европейския съюз по въпроса за „обществена сигурност“ е решението *Campus Oil*,[168] в което Съдът постанови, че национална мярка – в случая, национална квота за снабдяване с рафиниран нефт в Република Ирландия, е оправдана, защото рафинираният нефт се счита:

> **от фундаментално значение за съществуването на една държава**, тъй като не само нейните услуги, а най-вече нейните институции, основните й обществени услуги и дори оцеляването на жителите й зависят от него. (пар. 34, добавено подчертаване)

От това става ясно, че **от една страна, терминът „обществена сигурност“ по смисълана правото на ЕС не се ограничава до въпроси, свързани с престъпната дейност, а обхваща въпроси като защитата на „жизнено важни обществени услуги“ и мерки, целящи да осигурят „оцеляването на жителите [на една държава]“; но от друга страна, смисълът му не е толкова широк като този на „обществен ред“ – термин често използван в полицейското право като отнасящ се до въпроси като поддържането на обществения ред при демонстрации, паради и празненства.[169] По-скоро, както го формулира Съветът, въпросът, чиято сигурност трябва да бъде осигурена, трябва да е свързан с:[170]**

---

[167] Вж. Panos Koutrakis, Public Security Exceptions and EU Free Movement Law, in: Koutrakos, P., Nic Shuibhne, N. and Sypris, P. (Eds.), Exceptions from EU Free Movement Law, 2016 (pp. 190-217), p.2 (оригинален текст), който може да бъде намерен на:
http://openaccess.city.ac.uk/16192/
(Относно чл. 36 (Стоки), 45(3) и 52 (Хора), 62 (Услуги) и 65 на ДФЕС (Капитали)).

[168] Решение на Съда от 10 юли 1984 г. *Campus Oil Limited and others v Minister for Industry and Energy and others*, Дело 72/83, ECR 1984 -02727, което може да бъде намерено на:
https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=CELEX%3A61983CJ0072

[169] Срв. напр.:
http://www.lokalepolitie.be/5371/contact/diensten/20-handhaving-openbare-orde (на нидерландски)

[170] Съвет на Европейския съюз, Процедура: 2017/0228 (COD), съображение (12a), стр. 3, която може да бъде намерена на:
https://eur-lex.europa.eu/legal-content/BG/HIS/?uri=CELEX%3A52017PC0495

реална и достатъчно сериозна заплаха, засягаща един от фундаменталните интереси на обществото като например заплаха за функционирането на институциите и на жизнено важни обществени услуги и за оцеляването на населението, също както и риска от сериозно нарушение на външните отношения, на мирното съществуване на нациите или на военни интереси.

Преценката на точните граници на това, което попада или не под понятието (криминални?) заплахи за „обществената сигурност“ предизвиква трудности при преценката на специфични обстоятелства. Кога обществени безредици – например, прекъсване на полети от хора, манифестиращи срещу принудителното експулсиране на търсещи убежище – се равняват на „ заплаха за жизнено важна обществена услуга“?[171] И кога е рискът от „нарушение на външните отношения“ – да речем, при демонстрация срещу посещението на държавен глава от друга държава – достатъчно „сериозен“, за да бъде определен като риск за обществената сигурност? При все това отговорът на тези въпроси определя дали Директивата за защита на личните данни в полицейската и наказателната дейност се прилага по отношение на обработването на лични данни свързани с тези действия или не.

Въпреки че много образувания – особено тези в публичния сектор като местни власти или органи за защита на околната среда, за социална защита или за защита на животните – получават някои публични правомощия по отношение на (някои) престъпления и (някои) заплахи за обществената сигурност, основните задачи на тези власти не са свързани с разследването (и т.н.) на престъпления в границите на техните компетенции или на заплахи за обществената сигурност (без значение дали е замесено престъпление или не).

Длъжностни лица по защита на данните в подобни публични власти или органи трябва внимателно да преценят до каква степен може да се каже, че обработването на лични данни от тяхната организация или организации, е предмет на ОРЗД, и до каква степен то е предмет на Директива (ЕС) 2016/680. Това често няма да е лесен за изясняване проблем и ДЛЗД следователно трябва да работи по това заедно с администратора, съответния правен отдел и компетентния надзорен орган. В допълнение, лични данни обработвани в дейности по обработване предмет на Директива (ЕС) 2016/680 обикновено трябва да бъдат разделени от лични данни обработвани в дейности предмет на ОРЗД със специфични правила и политики относно кога лични данни от една категория/ за една цел могат да бъдат използвани в друга категория/ за друга цел.[172]

И накрая, възниква проблем във връзка с границата между дейностите на държавите членки на ЕС в сферата на *„предотвратяването, разследването, разкриването или наказателното преследване на престъпления“ и на „предпазването от заплахи за*

[171] В Обединеното кралство имаше спор относно съдебното преследване и осъждане точно на такива манифестиращи по силата на закон против тероризма – т.е., по силата на закон за „обществената сигурност“ – а не по силата на наказателен закон за нарушаване на граници, вж.: https://www.theguardian.com/global/2019/feb/06/stansted-15-rights-campaigners-urge-judge-to-show-leniency (на английски)
Решението е предмет на обжалване.

[172] Срв. също с разискването в подраздел 1.4.6 по-долу относно обмена на лични данни между различни органи, работещи под различни режими за защита на данни в ЕС.

обществената сигурност и тяхното предотвратяване" от една страна, и дейностите на държавите членки засягащи **националната сигурност** и дейностите на агенциите и или подразделенията на държавите членки занимаващи се с въпросите на националната сигурност, от друга страна. Границите между тези две сфери – първата номинално напълно включена в правото на ЕС, втората официално напълно извън него – са нарастващо неясни (особено във връзка с не много точно очертаните категории на „тероризъм", „компютърни престъпления", „киберсигурност" и т.н.).[173] В действителност:[174]

> В някои държави самите органи стават хибридни, с двойни роли за борба с криминалната дейност и защита на националната сигурност. Федералното бюро по разследванията на САЩ (ФБР) е основен пример[175], но в Обединеното кралство Правителствените комуникационни служби също работят все по-близко с правоприлагащите органи.[176]

Проблемът не може да бъде обсъден в детайл тук, но ще бъде засегнат в раздел 1.4.6 по-долу относно предаването на лични данни от администратор в сфера, регулирана от една категория право на ЕС относно защитата на данните, на администратор субект на друга категория право на ЕС – или в случая на органите за национална сигурност, напълно извън обхвата на правото на ЕС.

От друга страна, разликата между обработване на лични данни предмет на Директивата

---

[173] Douwe Korff, Ben Wagner, Julia Powles, Renata Avila and Ulf Buermeyer, Boundaries of Law: Exploring Transparency, Accountability, and Oversight of Government Surveillance Regimes, comparative report covering Colombia, DR Congo, Egypt, France, Germany, India, Kenya, Myanmar, Pakistan, Russia, South Africa, Turkey, UK, USA, prepared for the World Wide Web Foundation, January 2017, в частност section 2.3.1, който може да бъде намерен на:
https://ssrn.com/abstract=2894490

[174] В същия, стр. 27. Нарастващата роля на полицията в „превантивната" дейност не е нова. Вж. Ian Brown & Douwe Korff, Privacy & Law Enforcement, FIPR study for the UK Information Commissioner, 2005, Paper No. 4, The legal framework, section 3.1. По-скорошните развития, най-вече също свързани с размиването на границите между полицейските дейности и дейностите свързани с националната сигурност, са отбелязани в Douwe Korff, Protecting the right to privacy in the fight against terrorism, Issue Paper written for the Commissioner for Human Rights of the Council of Europe, 2008, който може да бъде намерен на:
https://wcd.coe.int/ViewDoc.jsp?Ref=CommDH/IssuePaper(2008)3

[175] Страница на интернет сайта на ФБР относно „Заплахите за националната киберсигурност" изрично отбелязва, че ФБР е натоварено и със защитата на националната сигурност на САЩ, и с това да бъде основният национален правоприлагащ орган, добавяйки че *„тези роли са допълващи се, тъй като заплахите за националната киберсигурност могат да произлизат от отделните щати, терористични организации и международни престъпни организации; като границите между тях често са неясни."* Вж.:
www.fbi.gov/about-us/investigate/cyber/addressing-threats-to-the-nations-cybersecurity
ФБР наскоро промени Списъка с факти за ФБР като вече описва „основната си функция" не като „правоприлагане", а като „национална сигурност". Вж.: The Cable, 5 януари 2014 на:
https://foreignpolicy.com/2014/01/05/fbi-drops-law-enforcement-as-primary-mission/#sthash.4DrWhlRV.dpbs
За опасностите от подобна неясност на границите, вж.:
https://foreignpolicy.com/2013/11/21/meet-the-spies-doing-the-nsas-dirty-work/

[176] Вж.: Computer Weekly, "*GCHQ and NCA join forces to police dark web*", 9 ноември 2015, на:
http://www.computerweekly.com/news/4500257028/GCHQ-and-NCA-join-forces-to-police-dark-web

за защита на личните данни в полицейската и наказателната дейност и обработване на лични данни от институциите, органите, службите и агенциите на ЕС е ясна, като второто е предмет на нов регламент приет през 2018, както е обсъдено в раздел 1.4.6 по-долу.

ii- Засегнати лица

Също във връзка с въпроса на обхвата, юДиректива (ЕС) 2016/680 определя **„компетентния орган“** споменат в член 1(1) като:

> а) всеки публичен орган, който е компетентен за предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания, включително предпазването от заплахи за обществената сигурност и тяхното предотвратяване; или
>
> б) всякакъв друг орган или образувание, който по силата на правото на държава членка разполага с публична власт и публични правомощия за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания, включително предпазването от заплахи за обществената сигурност и тяхното предотвратяване;
>
> (член 3(7))

Както вече е отбелязано, това може да се отнася до много други органи освен полицията и други първостепенни органи по правоприлагане като включва, в зависимост от националния конституционален подход, местни и регионални публични органи, органи по защита на здравето и по сигурността, надзорни органи на финансови институции, органи по защита на животните и на околната среда, данъчни и митнически органи, и много други – винаги когато са им дадени „публични правомощия“ във връзка с престъпления и заплахи за обществената сигурност, които може да се отнасят до престъпна дейност в техните сфери на компетентност.

Както вече също е отбелязано, обработката на лични данни от подобни органи във връзка с дейности несвързани с престъпни въпроси е предмет на ОРЗД, а не на Директивата за защита на данните в полицейската и наказателната дейност, и същото може да се отнася за обработването на лични данни от подобни власти във връзка с заплахи за обществената сигурност, които не включват престъпления – като бури, наводнения, епидемии или надзора на спортни събития във връзка с различни от възможни престъпления цели.

iii- Засегнати дейности по обработване

Относно средствата използвани за обработване, по същия начин като другите инструменти на ЕС за защита на данните, Директива (ЕС) 2016/680, се прилага за:

> обработването на лични данни изцяло или частично с автоматични средства, както и за обработването с други средства на лични данни, които са част от регистър с лични данни или са предназначени да съставляват част от такъв регистър.

С други думи, Директива (ЕС) 2016/680 се прилага за **всички обработвания на данни с автоматични средства** и за обработването на всички лични данни пазени в **структурирани регистри**, които са в обхвата ѝ относно дейностите и лицата предмет на Директивата.

Важно е да се отбележи, че за разлика от Рамковото решение от 2008 г. обсъдено по-горе в раздел 1.3.6, **Директива (ЕС) 2016/680 се прилага** не само за лични данни предавани между държави членки, но **и за вътрешното обработване на лични данни за целите на правоприлагането**. Както подчертава Комисията, Директивата следва за

„улесни сътрудничеството на полицейските и съдебните власти в ЕС“.[177]

Свободно движение на данните между компетентните власти в различни държави членки

Въпреки че Директивата *„ не трябва да прави невъзможно за държавите членки да осигурят по-висока защита от тази установена в тази Директива“* (чл. 1(3)), всяка една държава членка, която предвиди подобни по-високи стандарти, не следва да се позовава на тях, за да **„ограничава или забранява“** свободния обмен на лични данни между държави членки, който съставлява самата цел на Директивата (чл. 1(2)(б)). От друга страна, ако държава членка в националното си право предвиди „специални **условия**“ за определени категории обработване (напр. при профилиране) – или за обработването на някои категории данни (напр. биометрични данни) – то тогава държавата членка не само може, но и трябва („следва“) също да предвиди, че:

> предаващият компетентен орган уведомява получателя на тези лични данни, за тези условия и за изискването получателя да се съобразява с тях.
>
> (чл. 9(3))

Въпреки това, държавите членки не следва, по силата на тази разпоредба, да налагат условия на получатели в други държави членки засегнати относно съдебни или полицейски въпроси, различни от тези, които налагат при „подобно предаване на данни“ до вътрешни получатели от същата категория (чл. 9(4)).

(По въпроса за предаване на лични данни на трети държави, виж под съответното заглавие по-долу.)

Съдържание

Много от разпоредбите в Директива (ЕС) 2016/680са подобни на разпоредбите в ОРЗД – но само до определена степен, за да отразяват специалния контекст на правоприлагането и предотвратяването на престъпни заплахи за обществената сигурност.

Определенията на основните понятия в член 3 – *„лични данни“, „обработване“, ограничаване на обработването“, „профилиране“, „псевдонимизация“, „регистър с лични данни“, „администратор“, „обработващ лични данни“, “получател“, „нарушение на сигурността на лични данни“, „генетични данни“, „биометрични данни“, „данни за здравословното състояние“* – са действително идентични на определенията на същите понятия в ОРЗД.[178]

Основните принципи изложени в член 4 също са подобни. Именно принципът за **„законосъобразност“**, който липсваше в Кадровото решение от 2008 г., сега е изрично включен в член 4(а) доразвит в член 8(1) - заедно с принципа на „прозрачност“ (който е директно свързан с принципа на законосъобразност и добросъвестност в ОРЗД) до някъде отразен в член 8(2) *(„В правото на държавата членка, регламентиращо*

---

[177] Европейска Комисия, Списък с факти – Как реформата на защитата на данни ще помогне с битката срещу международната престъпност?, 30 април 2018, който може да бъде намерен на: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_bg

[178] Странно, но въпреки че представя всички горе посочени определения с идентични по същество думи на тези от ОРЗД, Директивата за защита на личните данни не дава определение на „трета страна“ – въпреки че друго определение (на „получател“) изрично споменава трети страни.

обработването, попадащо в обхвата на настоящата директива, се посочват най-малко общите цели на обработването, личните данни, които се обработват, и конкретните цели на обрабо-тването.“) и в разпоредбите относно информирането на субектите на данни и относно правото им на достъп до техните данни (въпреки че специално в контекста на Директивата за защита на личните данни в полицейската и наказателната дейност тези права са предмет на по-широки ограничения).

Принципът на ограничение на целите е отслабен, тъй като лични данни събрани от който и да било от гореспоменатите компетентни органи за целите на правоприлагането или на обществената сигурност **могат да бъдат използвани за всякаква друга цел стига това да *„е разрешено от правото на Съюза или правото на държава членка.“*** (чл. 9(1), първо изречение) предмет на разпоредбата в чл. 9(1), второ изречение, според която:

> Когато личните данни се обработват за такива други цели се прилага Регламент (ЕС) 2016/679 [ОРЗД] освен ако обработването се извършва в хода на дейност, която е извън обхвата на правото на Съюза.[179]

От това следва, че всички данни по правоприлагането, които са направени достъпни по силата на подобен „разрешаващ“ закон все пак трябва да са ограничени до това, което е „подходящо“ и „необходимо“ за „легитимната цел“ преследвана от разрешаващия закон. **По принцип тук е важна ролята на ДЛЗД, които работят съответно за разкриващия и получаващия орган.** Въпреки това е възможно законът в някои държави просто да постановява, че някои данни по правоприлагането трябва при някои определени обстоятелства (напр. когато това е разрешено от служител от висше равнище) да бъдат направени достъпни за органи, които нямат функции по правоприлагане.[180]

Директивата изисква от държавите членки да наложат **ограничения на съхранението на данни** обработвани в обхвата на Директивата (чл. 5); и да правят **ясни разграничения** между лични данни от **различни категории субекти на данни** като лица под съмнение, осъдени за престъпления, жертви, свидетели и т. н. (чл. 6); и постановява, че *„[д]ържавите членки предвиждат доколкото е възможно да се прави разграничение между лични данни, основани на факти, и лични данни, основани на лични оценки“* (чл. 7(1)).

Директивата за защита на личните данни в полицейската и наказателната дейност също (както и ОРЗД) изисква от администраторите да възприемат **„подходящи“ мерки за защита** съобразени с контекста и целите на обработването (чл. 29(1)) и за тази цел да извършат **оценка на риск**а, за да се определи какво ниво на сигурност е подходящо (чл.

---

179 Вж. също член 9(2). Това също е по-подробно обсъдено в подраздел 1.4.6 по-долу.

180 Срв. с дебата относно (тогава предложения) широк обмен на данни на непълнолетни в Обединеното кралство между органите по социална защита, по образование и полицейските власти в Ross Anderson *et al.*, Children’s Databases – Safety and Privacy: A Report for the Information Commissioner, prepared by the UK Foundation for Information Policy research (FIPR), 2006, (на английски), съдържащ резюмета от Дау Корф не само на релеватните законови правила за защита на данните в Обединеното кралство (*Data Protection Rules and Principles Relating to Data Sharing*, p. 100ff.), но и (в Допълнение) преглед на Правната рамка на други места в Европа, най-вече в Германия и Франция, който може да бъде намерен на:
https://www.cl.cam.ac.uk/~rja14/Papers/kids.pdf

29(2)). Тя също изисква вземането технически и организационни мерки по сигурността (в същия) и налагането на **задължения за поверителност** на служителите (чл. 23).

Също както и в ОРЗД, **нарушенията на сигурността на личните данни** трябва да бъдат докладвани на надзорния орган в рамките на 72 часа (ако не е направено в този период, забавянето трябва да бъде обосновано) (чл. 30); и субектите на данни трябва да бъдат информирани за тях *„без излишно забавяне“, „когато има вероятност нарушението на сигурността на личните данни да доведе до висок риск за правата и свободите на физическите лица“* (чл. 31).

Правилата в Директивата за защита на личните данни в полицейската и наказателната дейност относно обработването на **чувствителни данни** – т. е., на „лични данни, разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения или членство в синдикални организации“, генетични и биометрични данни (за целите единствено на идентифицирането на физическо лице), „данни за здравословното състояние“ и „данни за сексуалния живот или сексуалната ориентация на физическото лице“ – са оформени донякъде различно от тези в ОРЗД (чл. 9),[181] тъй като Директивата за защита на личните данни позволява обработването на подобни лични данни:

> **само** когато това е **абсолютно необходимо** и при **подходящи гаранции** за правата и свободите на субекта на данни и само ако:
>
> а) е **разрешено** съгласно **правото** на Съюза или **правото** на държава членка;
>
> б) трябва да бъдат защитени **жизненоважни интереси** на субекта на данните или на друго физическо лице; или
>
> в) обработването касае данни, които **очевидно са направени обществено достояние от субекта на данните**.
>
> (чл. 10 от Директивата за защита на личните данни в полицейската и наказателната дейност, добавено подчертаване)

Последните две условия отговарят на изключения в ОРЗД (съответно чл. 9(2)(в) и (д)).[182]

Когато държава членка се позовава на другото условие – **разрешение от закона** – тя

---

[181] Разбираемо е, че Директивата за защита на личните данни в полицейската и наказателната дейност не съдържа разпоредба като тази от член 10, първо изречение, на ОРЗД, постановяваща, че обработването на лични данни, свързани с присъди и нарушения, „се извършва само под контрола на официален орган или когато обработването е разрешено от правото на Съюза или правото на държава членка, в което са предвидени подходящи гаранции за правата и свободите на субектите на данни“: Директивата за защита на личните данни в полицейската и наказателната дейност и релевантните национални закони подсигуряват това. По същия начин, в Директивата няма нужда да се повтаря разпореждането от последното изречение на член 10 на ОРЗД, че „[п]ълен регистър на присъдите по наказателни дела се поддържа само под контрола на официален орган.“

[182] Освен факта, че изключението относно обработването на лични данни, за да бъдат защитени жизненоважните интереси на субекта на данните или на друго физическо лице по силата на чл. 9(2)(в) от ОРЗД се прилага само ако „субектът на данните е физически или юридически неспособен да даде своето съгласие“ – което не се изисква по силата на Директива (ЕС) 2016/680.

трябва да може да докаже, че обработването на данните е „***абсолютно необходимо***“ и че всяко ограничение на правата на субектите на данни е „***предмет на подходящи гаранции***“. В допълнение (за разлика от ситуацията по времето на Рамковото решение на Съвета от 2008 г.), сега лицата могат да се позовават на Директивата, за да отстояват правата си, като се има предвид, че Съдът на ЕС може накрая да се произнесе дали национален закон, приет в този контекст, отговаря на стандарта за „*абсолютна необходимост*“ и дали включва „*подходящи гаранции*“; и като се има предвид, че Комисията е оправомощена да взима изпълнителни действия ако прецени, че законът на държава членка, позволяващ обработването на чувствителни данни за целите на правоприлагането/ на общедтвената сигурност не отговаря на тези стандарти.

Директивата за защита на личните данни в полицейската и наказателната дейност също като ОРЗД урежда **автоматизирано вземане на решения**, включително профилирането, но с някои разлики. По-точно, тя постановява, че подобно обработване трябва *„да бъде разрешено от правото на Съюза или правото на държава членка“* и да е предмет на *„подходящи гаранции“,* които трябва да включват *„най-малко правото на човешка намеса от страна на администратора“*. Въпреки това, за разлика от от ОРЗД, Директива (ЕС) 2016/680 не постановява, че когато има подобна „човешка намеса“, субектът на данни трябва да може да *„изрази гледната си точка и да оспори [автоматизираното/ основано на профилиране] решението“.*

Трябва да се отбележи, че Директива (ЕС) 2016/680, постановява, че:

> В съответствие с правото на Съюза **се забранява профилирането, което води до дискриминация на физически лица въз основа на специалните категории лични данни, посочени в член 10.** (добавено подчертаване)

Във връзка с въпроса за „разрешението от закон“, важно е да се вземе предвид, че съответния **надзорен орган по защита на данните на държавата членка трябва да бъде консултиран** в процеса на изготвяне на законово предложение по тези въпроси (чл. 28 (2)).

ДЛЗД в съответните органи трябва да обмислят внимателно как тези важни нови изисквания на Директива (ЕС) 2016/680 – човешка намеса и задължение за недискриминация – могат да бъдат действително и ефективно приложени на практика в различни контексти.

Поради сферата си на приложение, Директивата позволява широки **ограничения на правата на субекта на данни** да бъде информиран за обработването, да му бъде даден достъп до данните и на правото на коригиране и изтриване на данни, които не отговарят на релевантните стандарти за качество на данните или които биват обработвани по друг начин противостоящ на правилата представени в инструмента – но тези ограничения все пак трябва да се свеждат до това, което е „необходимо“ и „пропорционално“ в едно демократично общество (вж. чл. 12 – 16 на Директивата и най-вече чл. 15). Директивата също позволява упражняването на тези права да бъде извършено **индиректно** чрез съответния надзорен орган (член 17). *„[К]огато личните данни се съдържат в съдебно решение, регистър или досие, обработвани в хода на наказателно разследване и наказателно производство“*, правата могат да бъдат упражнявани в съответствие с релевантното национално право (чл. 18). Обикновено **полицейските закони** и **наказателните процесуални кодекси** уреждат достъпа на заподозрян, обвиняем или осъден човек до определени части от релевантните досиета в определени фази на процеса (обикновено позволявайки ограничен достъп в ранните

фази на процеса и широк достъп по-късно, особено след като човекът е официално обвинен) – и подобни мерки следователно могат да бъдат възприети.

Практически и формални изисквания

В много други отношения също Директивата въвежда практически и формални изисквания подобни на тези в ОРЗД.

В частност, важно е да се отбележи, че Директината като ОРЗД съдържа новия **„принцип на отчетност“** (чл. 4(4))[183] и изисква от всички администратори в обхвата на Директивата *„като отчитат естеството, обхватът, контекстът и целите на обработването, както и рисковете с различна вероятност и тежест за правата и свободите на физическите лица“* да прилагат:

> …подходящи технически и организационни мерки, **за да гарантира и да е в състояние да докаже**, че обработването се извършва в съответствие с настоящата Директива.
>
> (чл. 19(1), добавено подчертаване)

Този член добавя, че *„[т]ези мерки се преразглеждат и актуализират при необходимост“* и че *„[к]огато това е пропорционално“,* те трябва да включват (изготвянето, приемането и) прилагането на *„подходящи политики за защита на данните“* от администратора (чл. 19(1), последно изречение и (2)).

Също както и ОРЗД, Директива (ЕС) 2016/680 изисква подробно **държане на регистри и записи** (чл. 24 и чл. 25), които са важни мерки, за да се подсигури проверката на законосъобразността на обработването – което е особено предизвикателство в сферата на прилагане на Директивата.

Директивата излага същите изисквания като ОРЗД във връзка със **„съвместните администратори“** (чл. 21(1)) и с използването на обработващи данни (чл. 22).

Директивата изисква извършването на Оценка на въздействието върху защитата на данните (ОВЗД**, чл. 27) в подобни обстоятелства, като тези предвидени в ОРЗД, т. е.:**

> [к]огато съществува вероятност определен вид обработване, по-специално при което се използват нови технологии, и предвид естеството, обхвата, контекста и целите на обработването, да **породи висок риск за правата и свободите на физическите лица**… (чл. 27, добавено подчертаване)

Съответния **надзорен орган** (който може да бъде основният национален надзорен орган за защита на данните, но също може да бъде отделен орган, при условие че изискванията за независимост са спазени: вж. по-долу) **трябва да бъде консултиран**, когато ОВЗД *„покаже, че обработването ще породи висок риск, ако администраторът не предприеме мерки за ограничаване на риска“* или когато (независимо от подобни мерки) *„видът обработване, по-специално когато се използват нови технологии, механизми или процедури, включва висока степен на риск за правата и свободите на субектите на данните“*(чл. 28(1)(а) и (б)).

Като средство да подсигури ефективното си прилагане особено във връзка с принципа на отчетност, Директива (ЕС) 2016/680 постановява определянето на **длъжностно лице по защита на данните (ДЛЗД)** от всеки администратор (чл. 32), изяснява позицията на ДЛЗД (чл. 33) и изброява задачите на ДЛЗД (чл. 34). Това също съответства на ОРЗД,

[183] Разискан подробно в Част Втора, раздел 2.3 по-долу.

който изисква определянето на ДЛЗД от всички органи от публичния сектор в обхвата му.[184] Въпреки това Директивата не постановява изрично, че ДЛЗД трябва да може да действа по независим начин.[185]

ДЛЗД в органите по правоприлагане и в други органи в обхвата на Директивата ще имат главна роля във връзка със съответствието на своите организации с принципа на отчетност и с релевантните постоянни преразглеждания на взетите мерки за съответствие с принципа; с изготвянето на „договореностите“ между съвместни администратори и на договорите с обработващи данни; с консултациите с надзорния орган; и с извършването на ОВЗД по силата на Директивата.[186]

Международни предавания на данни до компетентни органи в трети държави

Поради високата чувствителност на контекста и на личните данни в тази сфера, Глава V от Директива (ЕС) 2016/680 поставя редица условя за предаването на лични данни на държави извън ЕС („трети държави“) или международни организации, подобни на условията за предаване в обхвата на ОРЗД, но с допълнителни правила относно предавания на трети държави или международни организации от държава членка на ЕС получател на лични данни от друга държава членка и относно следващи предавания от и до получателя трета държава до друга трета държава или международна организация – и с по-специфични изключения по определени причини, както е разгледано по-долу.

Важно е да се отбележи въпреки това, че особено във връзка с международните прехвърляния на данни, Директивата позволява по-дълги срокове до пълната приложимост на правилата, разгледани по-долу, поради определени причини, обсъдени под заглавието *„Забавено транспониране“* в края на този раздел относно Директива (ЕС) 2016/680.

Общи предварителни условия за подобно предаване:

Чл. 35 от Директивата излага **три предварителни условия** за предавания до трети държави (но е важно да се отбележи, че *две от тези могат да не се вземат под внимание при някои обстоятелства*, както е посочено):

- предаването трябва да е **„необходимо“** за целите, посочени в чл. 1(1), т. е., за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания, или за предпазването от заплахи за обществената сигурност и тяхното предотвратяване;
- предаването трябва да е до **орган в трета държава или до международна организация компетентни относно споменатите по-горе цели** (като се има предвид че международната организация на криминалната полиция, Интерпол, е изрично включена в съображение (25)). Точно както „компетентните органи“ в ЕС не се свеждат до първостепенните органи по правоприлагане, органите в трети държави, до които могат да бъдат предавани данни също няма нужда да бъдат първостепенни органи по правоприлагане при условие че (също) са компетентни

---

184 Вж. Част Втора, раздел 2.4.2 по-долу.

185 Срв. с чл. 38(3) от ОРЗД, който предвижда, че:

„Администраторът и обработващият лични данни правят необходимото длъжностното лице по защита на данните да не получава никакви указания във връзка с изпълнението на тези задачи. Длъжностното лице по защита на данните не може да бъде освобождавано от длъжност, нито санкционирано от администратора или обработващия лични данни за изпълнението на своите задачи. Длъжностното лице по защита на данните се отчита пряко пред най-висшето ръководно ниво на администратора или обработващия лични данни.“

186 Срв. с подробното разглеждане на задачите на ДЛЗД по силата на ОРЗД в Част Трета на този наръчник.

във връзка с релевантни престъпни въпроси.

Забележете, че *това предварително условие може да не се прилага* в определени ситуаци, при определени условия, както е обсъдено по-долу под заглавието *„Предаване на други органи“* .

- *когато се предават или се предоставят лични данни от друга държава членка, тази държава членка е дала своето **предварително разрешение** за предаването в съответствие с националното си право* (предмет на изключение, както е отбелязано по-долу).

  (чл. 35(1)(а) - (в))

  Това последно постановление е свързано с предаването от една държава членка до трета държава или международна организация на данни първоначално получени от друга държава членка, т. е., последващото предаване на подобни данни изисква „предварителното разрешение“ на държавата членка, която първоначално е предоставила данните.

  Забележете, че *това предварително разрешение не се изисква ако*:

  > предаването на личните данни е **необходимо за предотвратяването на непосредствена и сериозна заплаха за обществената сигурност на държава членка или на трета държава, или за основните интереси на държава членка** и предварителното разрешение не може да бъде получено своевременно.

  В такъв случай *„[о]рганът, отговорен за даването на предварително разрешение [да се чете: органът, чието предварително разрешение е трябвало да бъде поискано ако не бе имало подобна непосредствена заплаха], **се уведомява** незабавно“* (чл. 35(2), добавено подчертаване).

Когато тези предварителни условия са изпълнени, лични данни могат да бъдат предадени на трета държава или международна организация **ако се прилага едно от следните три условия:**

- Комисията е приела **решение относно адекватното ниво на защита на личните данни** от получателя трета държава или миждународна организация (както е подробно указано в чл. 36).

  Но забележете, че *Европейската Комисия все още не е взела нито едно подобно решение относно адекватното ниво на защита по смисъла на Директивата*, така че тази разпоредба все още не може да бъде използвана.

  Или:

- съществуват **„подходящи гаранции“**, за да се подсигури, че след предаването личните данни ще продължават да бъдат обработвани като са предмет на „подходящи“ гаранции за защита на данните.

  Това е разяснено в чл. 37, които постановява, че въпросните гаранции трябва да се съдържат или в **правно обвързващ инструмент** (който може да бъде договор между държави или международни организации или правно обвързващо административно споразумение) (чл. 37(1)(а)), или *„администраторът [трябва да]е извършил оценка на всички обстоятелства около предаването на лични данни и е стигнал до заключението, че по отношение на защитата на личните данни съществуват подходящи гаранции“* (чл. 37(1)(б)) – но в този последен случай, **надзорният орган** трябва да бъде информиран за „категориите предавания“ осъществени на основанието на това постановление. В допълнение, всяко подобно предаване трябва да *„се документира и*

документацията е достъпна за надзорния орган при поискване, включително датата и момента на предаване, информация относно получаващия компетентен орган, обосновка на предаването и предадените лични данни" – чл. 37(3)).

Забележете, че споменатите **„правно обвързващи инструменти"** включват *„международни споразумения, включващи предаването на лични данни на трети държави или международни организации, които са били сключени от държавите членки преди 6 май 2016"*, както е отбелязано в чл. 61 на Директива (ЕС) 2016/680. Тези споразумения, както постановява този член, *„остават в сила, докато не бъдат изменени, заменени или отменени"* при условие че *„са в съответствие с правото на Съюза"* приложимо преди тази дата. Директивата не посочва дата, до която тези споразумения, които не са в съответствие с правилата на Директивата, трябва да бъдат изменени или отменени – и дори не посочва дали държавата членка трябва да ги преразгледа в този смисъл. Това е по-подробно обсъдено по-долу под заглавието *„Забавено прилагане"*.

Забележете също, че алтернативните **„подходящи гаранции"** се отнасят само до защитата на данните: няма изискване (така както е наложено по силата на другите две изключения обсъдени след това) да се извърши оценка на възможните последици за другите „основни права и свободи" на субекта на данните, и ако такива съществуват, тези може би да *„надделеят над обществените интереси в предаването";*

Или:

- (при липса на решение относно адекватното ниво на защита на личните данни съгласно чл. 36 и на подходящи гаранции съгласно чл. 37) ако се прилага **дерогация за особени случаи.** Чл. 38 позволява подобни дерогации ако предаването е **„необходимо"** в **пет случая**, два от които изискват „балансиране" на интереси. В разлечен ред от този в члена, особените случаи и условията са както следва:

  - **Лични данни могат да бъдат предавани на трета държава без решение относно адекватното ниво на защита и без подходящи гаранции ако това е „необходимо" за която и да е от целите изложени в чл. 1(1), т. е., за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания или на предпазването от заплахи за обществената сигурност и тяхното предотвратяване (чл. 38(1)(г)) – освен:**

    ако предаващият компетентен орган реши, че основните права и свободи на въпросния субект на данните надделяват над обществения интерес от предаването (чл. 38(2))

  - **Лични данни могат да бъдат предавани на трети държави без решение относно адекватното ниво на защита и без подходящи гаранции ако това е „необходимо" за установяването, упражняването или защитата на правни претенции, свързани с която и да било от гореспоменатите цели (чл. 38(1)(д)) – отново освен:**

    ако предаващият компетентен орган реши, че основните права и свободи на въпросния субект на данните надделяват над обществения интерес от предаването (чл. 38(2))

Забележете, че двата случая по-горе са свързани със ситуации поставящи сериозни дилеми относно човешките права и свободи: от една страна, предаването е „необходимо" за главен обществен интерес, но от друга страна, то засяга основните права и свободи на субекта на данни – може би по ужасен начин, както когато информацията на заподозрян, на свидетел или на жертва е предадена на органите на държава , която нарушава сериозно човешките права; и няма

„подходящи гаранции“ дори относно (последващото) обработване на личните данни на субекта. **Ясно е, че ДЛЗД на въпросния орган трябва да бъде консултирано относно подобни предавания и то ще носи тежко бреме относно съветите в това отношение.**

- Лични данни могат да бъдат предавани на трети държави без решение относно адекватното ниво на защита и без подходящи гаранции ако това е **„необходимо“ за предотвратяването на непосредствена и сериозна заплаха за обществената сигурност на държава членка или на трета държава** (чл. 38(1)(в)) – *в този случай изглежда независимо от вземането предвид на основните права и свободи на субекта на данни (освен ако това не се подразбира от изискването за “необходимост“ ?).*
- Лични данни могат да бъдат предавани на трети държави без решение относно адекватното ниво на защита и без подходящи гаранции ако това е **„необходимо“ за да бъдат защитени жизненоважни интереси на субекта на данни или на друго лице** (чл. 38(1)(а)).
- Лични данни могат да бъдат предавани на трети държави без решение относно адекватното ниво на защита и без подходящи гаранции ако това е **„необходимо“ за да бъдат защитени легитимни интереси на субекта на данните,** *когато законодателството на държавата членка, която предава данните, предвижда това* (чл. 38(1)(б)).

Данните, предадени на базата на някое от гореспоменатите основания, трябва да бъдат сведени до **„строго необходимото“** (Съображение (72)), **документирани** и:

> документацията **се предоставя на надзорния орган при поискване**, включително датата и момента на предаване, информация относно получаващия компетентен орган, обосновка на предаването и предадените лични данни. (чл. 38(3), добавено подчертаване)

Целта на тази документация и нейното предоставяне на надзорния орган е за позволи на надзорния орган да осъществи (ретроспективно) *„наблюдение на законосъобразността на предаването“* (Съображение (72)). Съображение (72) допълва:

> Тези дерогации следва да се **тълкуват стеснително** и **да не се позволява често, масово и структурно** предаване на лични данни или мащабно предаване на данни, а то следва да бъде ограничено до строго необходимото.

Още веднъж всяко ДЛЗД в съответните органи ще носи основни отговорности във връзка с тази документация и с контакта по релевентните въпроси с надзорния орган.[187]

Предаване до други органи в трети държави

Както е отбелязано по-горе, по принцип всички гореспоменати категории предавания могат да се извършват само до органи в съответната трета страна, които имат компетенции във връзка с целите, изброени в чл. 1(1) от Директивата, т. е., във връзка с *„целите на предотвратяването, разследването, разкриването или наказателното*

187 Вж: Част Трета от този наръчник, *Задачи на ДЛЗД*, Задачи 1-5 и 12.

преследване на престъпления или изпълнението на наказания, включително предпазването от заплахи за обществената сигурност и тяхното предотвратяване" (чл. 35(1)(б)) (въпреки че получателите няма нужда да бъдат точно органи по правоприлагането в тесния смисъл; те могат да включват други публични органи с определени задачи и правомощия свързани с престъпността или обществената сигурност).

Въпреки това чл. 39 от Директива (ЕС) 2016/680 позволява **изключения** от това правило под заглавието *„Предаване на лични данни на получатели, установени в трети държави"* (като се има предвид получатели различни от органите, които в съответната трета страна са компетентни по въпросите, изброени в чл. 1(1)на Директивата).

Съображение (73) разяснява причините за тези изключения (добавени разстояния между параграфите и добавено подчертаване):

> Компетентните органи на държавите членки прилагат действащите двустранни или многостранни международни споразумения, сключени с трети държави в областта на съдебното сътрудничество по наказателноправни въпроси и полицейското сътрудничество, за обмена на съответната информация, за да им се даде възможност да изпълняват своите задачи, възложени от закона. По принцип това се извършва посредством или поне в сътрудничество с компетентните органи на засегнатите трети държави за целите на настоящата директива, понякога дори ако няма сключено двустранно или многостранно споразумение.
>
> **При все това в отделни, специфични случаи редовните процедури, според които се изисква да бъде установен контакт с такъв орган в третата държава, могат да бъдат неефективни и неподходящи, по-специално когато предаването не би могло да се осъществи навреме или когато този орган в третата държава не зачита принципите на правовата държава или международните норми и стандарти за правата на човека, така че компетентните органи на държавата членка биха могли да решат да предадат личните данни пряко на получателите [да се чете: различни от органи по правоприлагане], установени в тези трети държави.**
>
> Такъв може да е случаят, когато спешно се налага лични данни да бъдат предадени с цел спасяване на живота на лице, което е заплашено да стане пострадал от престъпление, или в интерес на предотвратяването на непосредствено предстоящо престъпление, включително тероризъм.
>
> Дори такова предаване между компетентните органи и получателите, установени в трети държави, да се извършва само в отделни конкретни случаи, настоящата директива следва да предвиди условия за уреждането на тези случаи.
>
> Тези разпоредби не следва да се разглеждат като дерогации от съществуващи двустранни или многостранни международни споразумения в областта на съдебното сътрудничество по наказателноправни въпроси и полицейското сътрудничество. Тези правила следва да се прилагат в допълнение към другите правила от настоящата директива, по-специално свързаните със законосъобразността на обработването, и правилата от глава V.

Чл. 39(1) може да бъде парафразиран както следва:[188]

> Правото на Съюза или на държава членка може да предвиди възможността за органите по правоприлагане в отделни и специфични случаи да предават лични данни пряко на получателите, установени в трети държави и които не са компетентни по въпроси, свързани с престъпността и обществената сигурност, но само ако всички други разпоредби на Директивата са спазени и само ако всички от следните условия са изпълнени: …

Директива (ЕС) 2016/680 не се произнася по въпроса кои са същностно релевантните „други органи". Като се има предвид че чл. 39 се прилага в случаи, които са особено чувствителни във връзка с човешките права и свободи (вж. подчертаното изречение в цитата от съображение (37) по-горе), се предполага, че това което е предвидено са получатели в третата страна, в които предаващият орган в съответната страна членка на ЕС има **специално доверие.** По-точно, предаващият орган трябва да е сигурен, че получателят в третата страна, който не е орган по правоприлагане, няма да прехвърли информацията на орган по правоприлагането в третата страна, който *„не зачита принципите на правовата държава или международните норми и стандарти за правата на човека".* Въпросната преценка случай по случай винаги ще е особено деликатна за извършване и ще трябва поне да бъде **внимателно документирана** (включително причините позволяващи да се предположи, че данните могат да бъдат предадени на довереният орган без страх за това да се озоват в ръцете на неподходящ орган в засегнатата трета държава).

Относно предавания, които не са по силата на международни споразумния (както е разискано отделно по-долу), чл. 39(1) поставя **пет кумулативни условия** за въпросните предавания. Данните могат да бъдат предадени на релевантен орган получател, несвързан с правоприлагането, в трета държава ако (добавени подчертаване, разяснения в скоби и бележки под разпоредбите):

а) предаването е **строго необходимо** за изпълнението на задача на предаващия компетентен орган [в съответната държава членка на ЕС], както е предвидено в правото на Съюза или на държава членка за целите, посочени в член 1, параграф 1[т. е., **във връзка с въпроси по престъпността и обществената сигурност в ЕС или в държава членка**].

б) предаващият компетентен орган реши, че **никои основни права и свободи на въпросния субект на данни не надделяват над обществения интерес, който налага предаването в конкретния случай.**

Забележете, че тази преценка не се свежда до интересите за защита на данните на субекта на данни, а по-скоро трабва да се съобразява с това дали съответната трета държава и специални органи в тази държава *„зачитат принципите на правовата държава или международните норми и стандарти за правата на човека".* В допълнение, решението трябва да е взето на базата на преценка **случай по случай.**

---

188 Текстът на чл. 39(1) е следният:
„Чрез дерогация от член 35, параграф 1, буква б) и без да се засяга никое международно споразумение, посочено в параграф 2 от настоящия член, правото на Съюза или на държава членка може да предвиди възможността компетентните органи, посочени в член 3, точка 7, буква а), в отделни и специфични случаи да предават лични данни пряко на получателите, установени в трети държави, само ако са спазени останалите разпоредби на настоящата директива и е изпълнено всяко едно от следните условия:…"

в) предаващият компетентен орган счита, че **предаването на орган, който е компетентен в третата държава по отношение на целите, посочени в член 1, параграф 1** [целите на битката срещу престъпността и на обществената сигурност], е **неефективно или неподходящо**, по-специално тъй като *предаването не може да се осъществи навреме-*

или, може да се добави, защото бе било „неподходящо“ по други причини: вж. бележката под следващата разпоредба.

г) **органът на третата държава, който е компетентен за целите, посочени в член 1, параграф 1, е уведомен** без излишно забавяне, освен ако това е **неефективно или неподходящо**.

Забележете, че при споменаването на предаване до орган по правоприлагане, което по принцип би било най-ефективно и подходящо, **„неподходящо“** може да бъде разбирано като отнасящо се до ситуация, в която този *орган „[не] зачита принципите на правовата държава или международните норми и стандарти за правата на човека“.* Споменаването на **„неефективността“** на този орган може да се отнася до това, че е *по-принцип е неефикасен, бавен, некомпетентен или може би корумпиран*.

д) **предаващият компетентен орган уведомява получателя за конкретната цел или цели, единствено за които последният обработва личните данни, *при условие че такова обработване е необходимо.***

Забележете, че това предполага, че органът получател в третата държава трябва да осигури (силни и обвързващи) **гаранции**, че ще се подчинява на тези разпоредби и че наистина ще използва данните предадени от органите по правоприлагането от ЕС за специфичните и изрично споменати цели или цел и за никаква друга; и че дори и в този случай ще изпозва данните само до степен, която е (крайно) необходима за предвидените цели или цел.

В допълнение на съобразяването с тези специални разпоредби, както е отбелязано, чл. 39(1) подчертава, че *„[всички] други разпоредби на Директивата“* трябва също да бъдат спазени (вж. също последното изречение в съображение (73), цитирано по-горе, което подчертава, че това включва „особено [разпоредбите] за законосъобразност на обработването и Глава V, т. е., другите разпоредби за предаването на данни).

Всичко горепосочено е при все това **„без да се засяга никое международно споразумение“** (чл. 39(1)), с което се има предвид:

> всяко двустранно или многостранно международно споразумение, което е в сила между държави членки и трети държави в областта на съдебното сътрудничество по наказа-телноправни въпроси и полицейското сътрудничество. (чл. 39(2))

Това трябва да бъде четено заедно с чл. 61 относно *„Връзка[та на Директива (ЕС) 2016/680] с по-рано сключени международни споразумения в областта на съдебното сътрудничество по наказателноправни въпроси и полицейското сътрудничество“,* който разпорежда, че:

> Международните споразумения за предаване на лични данни на трети държави или международни организации, които са сключени от държавите членки преди

> 6 май 2016 г. и които са в съответствие с правото на Съюза, приложимо преди посочената дата, остават в сила, докато не бъдат изменени, заменени или отменени.

Директивата не определя дата, до която тези споразумения, ако не са в съответствие с правилата на Директивата, трябва да бъдат изменени, заменени или отменени – и дори не споменава, че държавите членки трябва да ги преразгледат с цел да ги приведат в съответствие с Директивата.[189] Въпреки това чл. 62 на Директивата постановява, че:

> До **6 май 2022 г.** и на всеки четири години след това **Комисията** представя на Европейския парламент и на Съвета **доклад относно оценката и прегледа на настоящата директива**. Докладите се оповестяват публично. (добавено подчертаване)

Тези преразглеждания трябва да включва *„по-специално прилагането и действието на глава V относно предаването на лични данни на трети държави или международни организации“* (чл. 62(2)), като се обърне „специално внимание“ на решенията относно адекватността на нивото на защита съгласно чл. 36(3) и на предаванията до „други органи“ съгласно чл. 39, както обяснихме преди малко. В допълнение, Комисията в този контекст „може да поиска информация от държавите членки и надзорните органи“ (чл. 62(3)) включително относно гореспоменатите международни споразумения, които са сключили. Също така се предполага, че Комисията може на базата на първото преразглеждане да предложи промени по тези споразумения или поне да даде предложения по какъв начин биха могли да се приведат в съответствие с правилата на Директива (ЕС) 2016/680 – но това не е предвидено в Директивата (за разлика от това във връзка с актове на Съюза в тази сфера).[190]

Според Комисията Директивата ще доведе до **„засилено международно сътрудничество“**:[191]

> Сътрудничеството между полицейски и съдебни наказателни органи от ЕС с държави извън ЕС също ще бъде засилено [от Директивата], тъй като ще има по.ясни правила за международните предавания а данни свързани с престъпления. Новите правила ще подсигурят, че предаванията се осъществяват при адекватно ниво на защита на данните.

Въпреки това, както е отбелязано по-долу под заглавието *„Забавено транспониране“*, ще отнеме известно време преди новите правила действително да се прилагат изцяло.

Надзор и прилагане

Глава VI от Директивата за защита на лични данни в полицейската и наказателната

---

189 Също не се знае дали съществуват преразглеждания направени преди приемането на Директивата или дали международните споразумения включващи предаването на лични данни на трети държави или международни организации, които са били сключени от държавите членки преди това, са съответствали на тогава приложимото право на ЕС.

190 Чл. 62(6) постановява, че до 6 май 2019 Комисията трябва да е извършила *„преглед на други правни актове, приети от Съюза, които регламентират обработването от компетентните органи за целите, посочени в член 1, параграф 1, включително на посочените в член 60, за да прецени необходимостта от привеждането им в съответствие с настоящата директива и, ако е целесъобразно, да изготви необходимите предложения за изменение на тези актове, така че да се осигури съгласуван подход към защитата на личните данни от обхвата на настоящата директива.“* Вж. по.подробно под заглавието *„Забавено транспониране“.*

191 Европейска Комисия, Списък с факти – Как реформата на защитата на данни ще помогне с битката срещу международната престъпност? (бележка 199 по-горе)

дейност изисква установяването на **независими надзорни органи** в държавите членки, натоварени с наблюдението и прилагането на разпоредбите на националните закони приети за прилагането („транспонирането“) на Директивата и с други свързани задачи (вж. чл. 41 – 46 от Директивата). Въпросният надзорен орган или органи може да бъде, но не е задължително да бъде общия надзорен орган или органи, установени съгласно ОРЗД (чл. 41(3)): в някои държави ими специални надзорни органи за обработванията от полицейските и правоприлагащите органи, докато в други общият надзорен орган е натоварен с тези задачи. В допълнение, в някои държави (особено във федералните) има различни национални (федерални) и местни или регионални органи.

Като общите надзорни органи определени съгласно ОРЗД, надзорните органи компетентни във връзка с въпросите предмет на Директива (ЕС) 2016/680 трябва да получат **широки правомощия**, включително правото да изискват (и получават) ***„достъп до всички лични данни**, които се обработват, и до **цялата информация,** необходима за изпълнението на неговите задачи“;* правото да отправят ***предупреждения*** към администратори или обработващи, да ***разпореждат*** на администратора или на обработващия лични данни да ***приведат операциите по обработване на данни в съответствие*** с Директивата, *„ако е уместно, по указан начин и в определен срок, по-специално като разпорежда[т] коригирането, изтриването на лични данни или ограничаването на обработването“*; да налагат ***„временно или окончателно ограничаване, включително забрана, на обработването“***; и правото да ***инициират съдебни производства*** срещу администратори и обработващи, които се твърди, че действат в противоречие с Директивата или да сведат подобни въпроси до знанието на съответните (съдебни) органи (чл. 47(1), (2) и (5) от Директивата). Надзорните органи също имат важни **съветни функции** и трябва да им бъде дадено правото да:

> издава[т] по собствена инициатива или при поискване на **становища до своите национални парламенти и своето правителство** или, в съответствие с националното право, до други институции и органи, както и до обществеността по всякакви въпроси, свързани със защитата на личните данни.
>
> (чл. 47(3), добавено подчертаване)

Те трябва също да публикуват **годишен доклад** относно дейностите си, *„който може да включва списък на видовете докладвани нарушения и видовете наложени наказания“* (чл. 49).

Решенията на надзорните органи трябва, въпреки това, да бъдат предмет на *„подходящи гаранции, в т.ч. ефективни средства за съдебна защита и справедлив съдебен процес, определени в правото на Съюза и на държавите членки в съответствие с Хартата“* (чл. 47(4)).

Забележете, че Директивата постановява, че:

> Държавите членки предвиждат, че компетентните органи въвеждат ефективни механизми за насърчаване на поверителното докладване за нарушения на настоящата директива. (чл. 48)

Тази разпоредба съответства на скоро приетата Директива относно защитата на лица,

подаващи сигнали за нарушения на правото на Съюза.[192]

Чл. 50 предвижда **взаимно сътрудничество** между надзорните органи на държавите членки на ЕС, компетентни във връзка с обработването на лични данни предмет на Директивата.

В допълнение, **Европейският комитет по защита на данните**, създаден по силата на ОРЗД, също има компетенции във връзка с обработването в обхвата на Директивата (чл. 51). Това включва издаването на ***насоки, препоръки и добри практики*** по всеки въпрос от Директивата и издаването на:

> **становище за оценка на адекватността на нивото на защита на данните в трета държава, територия или един или повече конкретни сектори в тази трета държава или международна организация**, включително за оценка на това дали дадена трета държава, територия, конкретен сектор, или международна организация са престанали да осигуряват адекватно ниво на защита (чл. 51(1)(ж)).

Комитетът трябва да представи своите становища, насоки, препоръки и добри практики на Комисията (и на Комитетът създаден по силата на чл. 93 от ОРЗД) и трябва да ги направи публично достъпни (чл. 51(3); и Комисията трябва на свой ред да информира Комитетът за действията, предприети в отговор (чл. 51(4)).

Средства за правна защита, отговорност за причинени вреди и наказания

Глава VIII представя средствата за правна защита, отговорността за причинени вреди и наказанията, които трябва да се установят в националните закони за транспониране на Директива (ЕС) 2016/680.

На кратко, в съответствие с ОРЗД, всеки субект на данни трябва да има **правото да подаде жалба** до съответния надзорен орган, ако смята, че обработването на негови лични данни е в нарушение на разпоредбите приети съгласно Директивата (чл. 52), както и правото да получи **ефективна съдебна защита** срещу правно обвързващо решение на надзорен орган, което го засяга (чл. 53), и срещу администратор или обработващ лични данни предмет на (националното право транспониращо) Директивата, *„ако считат, че правата им, установени в разпоредби, приети съгласно настоящата директива, са нарушени вследствие на обработването на личните им данни при неспазване на посочените разпоредби“* (чл. 54). В допълнение, (ощеведнъж в съответствие с ОРЗД):

> субектът на данни има право да възложи на **орган, организация или сдружение с нестопанска цел**, което е учредено правомерно в съответствие с правото на държава членка, има уставни цели от обществен интерес и развива дейност в областта на защитата на правата и свободите на субектите на данни по отношение на защитата на техните лични данни, да **подаде жалбата от негово име и да**

[192] Директива на Европейския парламент и на Съвета относно защитата на лица, подаващи сигнали за нарушения на правото на Съюза, 2019. По времето на изготвянето на този наръчник, текстът все още не бе публикуван в Официалния вестник (и съответно все още не бе номериран), но текстът, както е приет от Европейския парламент на 16 април 2019 (,който е финалния текст предмет на езикова редакция и превод), може да намерите на:
http://www.europarl.europa.eu/doceo/document/TA-8-2019-0366_BG.html

> **упражни от негово име правата, посочени в членове 52, 53 и 54**. (чл. 55, добавено подчертаване)

Субектите на данни също имат **право на обещетение** за материални и нематериални вреди причинени от обработване в нарушение на Директива (ЕС) 2016/680 (чл. 56).

Накрая, държавите членки трябва да предвидят **„ефективни, пропорционални и възпиращи“** наказания за всяко нарушение на Директивата (чл. 57).

Забавено транспониране

Както вече е споменато в предишните подраздели, не всяко обработване на лични данни за целите на правоприлагането и на обществената сигурност трябва вече да бъде в съответствие с Директивата или с националните закони за транспониране на Директивата: тя съдържа редица разпоредби позволяващи на някои инструменти и операции да бъдат приведени в съответствие с Директивата на определена по-късна дата (или дори в неопределеното бъдеще). Разпоредбите позволяващи забавеното прилагане са свързани с „правните актове“ в ЕС; с договорите между страни членки на ЕС и трети държави или международни организации (включително Интерпол); и със специални автоматизирани системи за обработване на дължавите членки в сферата на наказателното право и на обществената сигурност.

Забавено прилагане във връзка с правни актове в ЕС:

Чл. 60 на Директива (ЕС) 2016/680 постановява относно приблизително 123 инструменти в ЕС („законови актове“ от различен вид) свързани с въпросите на Правосъдието и Вътрешните работи[193], че:

> Специалните разпоредби за защита на личните данни, съдържащи се в **правни актове на Съюза, които са влезли в сила на или преди 6 май 2016 г.** в областта на съдебното сътрудничество по наказателноправни въпроси и полицейското сътрудничество, с които се регламентира обработването между държавите членки и достъпът на определени органи на държавите членки до информационни системи, създадени съгласно Договорите, и които попадат в обхвата на настоящата директива, **остават незасегнати**. (добавено подчертаване)

Въпреки това, чл. 62(6) от Директивата постановява, че **до 6 май 2019**, Комисията трябва да е **прегледала**:

> [всички] други правни актове, приети от Съюза, които регламентират обработването от компетентните органи за целите, посочени в член 1, параграф 1, включително на посочените в член 60, за да **прецени необходимостта от привеждането им в съответствие с настоящата директива и, ако е целесъобразно, да изготви необходимите предложения за изменение на тези актове,** така че да се осигури съгласуван подход към защитата на личните данни от обхвата на настоящата директива. (добавен подчертаване)

От това следва, **че тези 123 или въпросни „други правни актове“ няма нужда да бъдат прведени в съответствие с Директивата до 6 май 2019**: единственото, което се изисква, е те да бъдат ***прегледани*** до тогава, с цел да се ***предложат*** промени по тях, където е нужно. **Няма определена дата за извършването на нужните в действителност изменения** или дори за представянето на релевантните детайлни предложения

193 Вж. Емилио Де Капитани (бележка 136 по-горе)

инструмент по инструмент.[194]

През това време, както разпорежда чл. 60, правилата за защита на данните в тези 123 правни актове продължават да са в сила и могат да служат като основание за предавания на лични данни в сферата на наказателното право и обществената сигурност дори и да не съответстват на изискванията на Директива (ЕС) 2016/680 при условие, че **трите предварителни условия** за подобни предавания на данни представени в Директивата са изпълнени: ако предаването е (според предаващия орган от ЕС) „необходимо“ за целите на наказателното право и обществената сигурност; ако предаването е извършено до орган в третата държава, който е компетентен в тези сфери (освен ако органът е неефективен, бавен или в най-лошият случай незачитащ човешките права и свободи); и ако, случай, че предадените данни са били първоначално получени от държава членка, тази държава членка е позволила предаването (или в спешни случаи поне е била информирана за това); и при условие че **или** релевантния правен инструмент съдържа „подходящи“ гаранции за защита на данните, **или** (ако инструментът не съдържа подобни гаранции) компетентният орган от ЕС прехвърлящ данните прецени, че *„основните права и свободи на засегнатия субект на данни“* не *„надделяват над обществения интерес в предаването“*.

Особено важно е, че в съответствие с новия принцип на **„отчетност“**, **преценката направена от органа** – т. е., дали релевантният правен инструмент съдържа „подходящи“ гаранции за защита на данните или дали и защо общественият интерес надделява над необходимостта за защита на основните права и свободи на субекта на данни – трябва да бъде **записана** и, при поискване, предоставена на европейския надзорен орган по защита на данните (и на Съда).

Всяко ДЛЗД в релевантния компетентен орган в ЕС трябва разбира се да играе важна роля в това: първо, като обръща вниманието на организацията към нужната да се извършват тези преценки, и следователно като вътрешно проверява дали те са приложени и дали са приложени правилно – и като се консултира с европейския надзорния орган за защита на данните ако е нужно в случай на вътрешно разногласие или въпроси в тази сфера.

Забавено приложение във връзка с договори между държави членки на ЕС и трети държави или международни организации:

Както е отбелязано по-рано, чл. 61 разпорежда, че:

> Международните споразумения за предаване на лични данни на трети държави или международни организации, които са сключени от държавите членки преди 6 май 2016 г. и които са в съответствие с правото на Съюза, приложимо преди посочената дата, остават в сила, докато не бъдат изменени, заменени или отменени.

Предавания съгласно който и да било договор преди май 2016 между държава членка и трета държава или международна организация следователно също може да продължат при условие, че трите предварителни условия за подобни предавания представени в Директива (ЕС) 2016/680 са изпълнени: ако предаването е (според предаващия орган от ЕС) „необходимо“ за целите на наказателното право и обществената сигурност; ако предаването е извършено до орган в третата държава,

[194] По времето на последната редакция на това първо издание на наръчника в началото на май 2019, все още не е имало подобни предложения представени от Комисията.

който е компетентен в тези сфери (освен ако органът е неефективен, бавен или в най-лошият случай незачитащ човешките права и свободи); и ако, случай, че предадените данни са били първоначално получени от държава членка, тази държава членка е позволила предаването (или в спешни случаи поне е била информирана за това); и при условие че **или** релевантния правен инструмент съдържа „подходящи“ гаранции за защита на данните, **или** (ако инструментът не съдържа подобни гаранции) компетентният орган от ЕС прехвърлящ данните прецени, че *„основните права и свободи на засегнатия субект на данни“* не *„надделяват над обществения интерес в предаването“.*

Но още веднъж, в съответствие с новия принцип на **„отчетност“**, **преценката направена от органа** – т. е., дали релевантният правен инструмент съдържа „подходящи“ гаранции за защита на данните или дали и защо общественият интерес надделява над необходимостта за защита на основните права и свободи на субекта на данни – трябва да бъде **записана** и, при поискване, предоставена на надзорния орган по защита на данните (и на съдебните власти).

И още веднъж, всяко ДЛЗД в релевантен компетентен орган на държава членка ще има важна роля в това.

Забавено прилагане във връзка със специални автоматизирани системи за обработване в сферата на наказателното право и обществената сигурност

Чл. 63, който специално урежда транспонирането на Директивата за защита на данните в полицейската и наказателната дейност в националното право, постановява в първия си параграф, че:[195]

> Държавите членки приемат и публикуват до 6 май 2018 г. законовите, подзаконовите и административните разпоредби, необходими, за да се съобразят с настоящата Директива. Те незабавно съобщават на Комисията текста на тези разпоредби. Те прилагат посочените разпоредби **от 6 май 2018 г.** (добавено подчертаване)

По принцип от това следва, че въпросните „законови, подзаконови и административни разпоредби“ трябва да бъдат приведени напълно в съответствие с Директивата до тази дата.

Въпреки това членът предвижда следното **изключение** в следващия параграф, предмет на условия:

> Чрез дерогация от параграф 1 дадена държава членка може да ***предвиди по изключение, когато това предполага несъразмерни усилия,*** системите за автоматизирано обработване, създадени преди 6 май 2016 г., да се привеждат в съответствие с член 25, параграф 1 **до 6 май 2023 г**. (добавено подчертаване)

Третият параграф позволява още по дълги срокове, предмет на допълнителни условия:

> Чрез дерогация от параграфи 1 и 2 от настоящия член дадена държава членка може, ***при изключителни обстоятелства***, да приведе дадена система за

[195] Последният четвърти параграф разпорежда, че: *„Държавите членки съобщават на Комисията текста на основните разпоредби от националното право, които те приемат в областта, уредена с настоящата директива.“* По-специфичната разпоредба в първия параграф подчертава, че пълното приложение на Директивата е в действителност прогресивно действие, което трябва да се извърши в продължение на няколко години, а не е еднократно транспониране.

> автоматизирано обработване, посочена в параграф 2 от настоящия член, в съответствие с член 25, параграф 1 в **рамките на определен срок** след срока, посочен в параграф 2 от настоящия член, ***ако в противен случай това би причинило сериозни затруднения за функционирането на тази конкретна система за автоматизирано обработване.*** Съответната държава членка уведомява Комисията за основанията за тези сериозни затруднения и за основанията за определения срок, в рамките на който тя привежда тази конкретна система за автоматизирано обработване в съответствие с член 25, параграф 1. Определеният срок в никакъв случай не е по-късно от **6 май 2026 г.** (добавено подчертаване)

Всичко горепосочено означава, че пълното прилагане на всички изисквания на Директива (ЕС) 2016/680, включително най-вече тези свързани с предаването на данни до трети държави и международни организации, ще отнеме време.

Въпреки това през това време си струва да припомним, че съгласно Директивата (за разлика от ситуацията съгласно предишното Рамково решение на Съвета) съответствието на правилата и действията на Съюза и на държавите членки свързани с въпросите на престъпността и обществената сигурност сега е обект на съдебен контрол. Това включва на последно място проверката дали тези правила и действия съответстват на Директивата – включително дали гореспоменатите преценки (дали договор между държави съдържа „подходящи“ гаранции за защита на данните или дали отговаря на правото на Съюза от преди май 2016; или дали в определен случай общественият интерес в предаването наистина надделява над необходимостта от защита на основните права и свободи на субекта на данни) са извършени; и във връзка с всяко забавяне по привеждането на гореспоменатите дейности в съответствие с Директивата, дали специалните условия за подобно забавяне, представени в цитираните по-горе параграфи, са изпълнени.

1.4.4 Нови инструменти за защита на данните в сферата на Общата външна политика и политиката на сигурност (ОВППС)

Както обяснява Комисията: [196]

> Договорът от Лисабон от 2009 г. направи много за да засили дейностите на Съюза в областта на външните дейности. Първо, създаде поста на **Върховен представител (ВП) на Европейския съюза по въпросите на външните работи и политиката на сигурност. ...**
>
> И второ, Договорът **създаде Европейската служба за външна дейност (ЕСВД).** Работеща от 2011 г., тя по същество е новата дипломатическа служба на ЕС, подпомагаща ВП при провеждането на външната политика на ЕС. По-специално, ЕСВД ръководи мрежата от **141 делегации на ЕС** по целия свят.

[196] Виж:

https://ec.europa.eu/fpi/about-fpi_en

> ЕСВД работи за осигуряване на последователност и координация на външните дейности на Съюза, като подготвя предложения за политики и ги прилага след одобрението им от Европейския съвет. ...
>
> Наред с ЕСВД беше създадена нова служба на Комисията - **службата за инструменти в областта на външната политика**, която да поеме отговорността за оперативните разходи.
>
> Днес, под ръководството на [ВП], като работи в тясно сътрудничество с делегациите на ЕСВД и ЕС, службата за инструменти в областта на външната политика има задачата да ... изпълнява бюджета на Общата външна политика и политика на сигурност (ОВППС) [и редица други инструменти и действия]. ...[197]
>
> Бюджетът за широкия спектър от дейности, управлявани от службата за инструменти в областта на външната политика, възлиза на 733 милиона евро през 2014 г.

Работата, извършена от ВП, ЕСВД и персонала на службата за FPR, често включва обработка на лични данни, например във връзка с налагането на санкции срещу физически лица или замразяването на техните активи.[198]

Подобна обработка обаче не е предмет на същите правила на договора на ЕС, както и обработването от субекти, които са обект на ОРЗД, Директива (ЕС) 2016/680 или дори на другите институции на ЕС. Всички останали са обхванати от общата гаранция за защита на личните данни, заложена в член 16 от ДФЕС:

> Член 16
>
> 1. Всеки има право на защита на личните му данни.
>
> 2. Европейският парламент и Съветът, като действат в съответствие с обикновената законодателна процедура, определят правилата за защита на физическите лица по отношение на обработката на личните данни от страна на институциите, органите, службите и агенциите на Съюза, както и от държавите-членки при извършване на дейности, които попадат в обхвата на правото на Съюза, както и по отношение на свободното движение на тези данни. Спазването на тези правила е предмет на контрол от страна на независими органи.

Това обаче не се отнася за обработването на лични данни от споменатите по-горе органи на ОВППС, тъй като след гореизложеното, последното изречение в член 16 от ДФЕС предвижда:

---

[197] За списък с връзки към всеки конкретен инструмент или действие вижте уебсайта, посочен в предишната бележка под линия.

198 Вж. становищата и коментарите на ЕНОЗД по такива въпроси, изброени тук:

https://edps.europa.eu/data-protection/our-work/subjects/common-foreign-and-security-policy_en

> Правилата, приети въз основа на настоящия член, не засягат специфичните правила, предвидени в член 39 от Договора за Европейския съюз.

Последният член от ДЕС предвижда следното:

> **Член 39**
>
> В съответствие с член 16 от Договора за функционирането на Европейския съюз и чрез дерогация от параграф 2 от него **Съветът приема решение за установяване на правилата относно защитата на лицата по отношение на обработването на лични данни от държавите-членки, когато извършват дейности, които попадат в обхвата на настоящата глава** [т.е. във връзка с ОВППС], и правилата, свързани със свободното движение на такива данни. Спазването на тези правила подлежи на контрол на независимите органи.

Това не е мястото за обсъждане на тези въпроси по-нататък.[199] Достатъчно е да се отбележи, че в областта на ОВППС се прилага регламентът, който обхваща обработката на лични данни от институциите на ЕС (и т.н.), Регламент 2018/1725, обсъден в следващия раздел, но само в ограничена степен; и че за да се знаят специфичните правила за защита на данните, свързани с всяка дейност по обработка на данни в контекста на ОВППС, включително кой орган за защита на данните е компетентен за какво и дали трябва да бъде определен ДЛЗД, е необходимо да се знае конкретното решение на Съвета, свързано с него.

1.4.5 Защита на данните за институциите на ЕС: нов Регламент

Както бе отбелязано в раздел 1.3.6 по-горе, първият инструмент на ЕС за защита на данните във връзка с обработката на лични данни от самите институции на ЕС, Регламент 45/2001, беше отменен с Регламент (ЕС) 2018/1725, който влезе в сила на **11 декември 2018 г.** [200](но с някои **изключения** и някои **забавяния в прилагането**, както е

---

[199] За допълнителна дискусия вижте:

- писмо на ЕНОЗД от 23 юли 2007 г. до председателството на МПК относно защитата на данните съгласно Договора за реформа (както бе наричан Договора от Лисабон при изготвянето му).

- ЕНОЗД, Съвместно становище относно уведомленията за предварителна проверка, получени от служителя по защита на данните на Съвета на Европейския съюз относно обработката на лични данни за ограничителни мерки във връзка със замразяването на активи, Брюксел, 7 май 2014 г. (2012-0724 , 2012-0725, 2012-0726), стр. 10, наличен на:

https://edps.europa.eu/sites/edp/files/publication/14-05-07_processing_personal_data_council_en.pdf

200 Регламент (ЕС) 2018/1725 на Европейския парламент и на Съвета от 23 октомври 2018 година относно защитата на физическите лица във връзка с обработването на лични данни от институциите, органите, службите и агенциите на Съюза и относно свободното движение на такива данни и за отмяна на Регламент (ЕО) № 45/2001 и Решение № 1247/2002/ЕО, ОВ L 295, 21 ноември2018 г., стр. 39–98, достъпно на:

отбелязано в тези рубрики по-долу).

Два режима

Тези изключения и забавяния настрана, Регламент 2018/1725 всъщност създава **два отделни режима за защита на данните**: един за всички **институции и органи на ЕС, които не участват в полицейското и съдебното сътрудничество**, и един за **институциите и органите на ЕС, които участват в такова сътрудничество** (вж. Чл. 2, пар. (1) и (2))

- **Режимът на защита на данните, приложим за институциите и органите на ЕС, които не участват в полицейското и съдебното сътрудничество:**

Този режим, посочен в глави I до VIII от новия регламент, **до голяма степен е същият като режима, установен от Общия регламент за защита на данните (ОРЗД)** за обработка, предмет на този последен инструмент. По този начин Регламент 2018/1725, подобно на ОРЗД, включва новия принцип на **„отчетност“** (чл. 4, пар. 2; вж. Също чл. 26) и определя **задълженията на администраторите и обработващите (глава IV) на практика същите условия като тези на администраторите и обработващите, предмет на ОРЗД.**

По-специално глава IV включва разпоредби относно принципа „защита на данните при проектиране и по подразбиране“ (чл. 27); относно договореностите, които трябва да се въведат по отношение на „съвместни контролери“ (чл. 28), обработващи (чл. 29) и лица, действащи под ръководството на администратора или обработващия лични данни (чл. 30); относно задължението („отчетност“) да поддържа подробна документация за дейностите по обработка (чл. 31); относно сигурността на обработването (чл. 33), уведомяване за нарушения на данните на Европейския надзорен орган по защита на данните (ЕНОЗД) (който е надзорният орган по отношение на институциите и органите на ЕС) (чл. 34) и съобщаване на нарушения на данните на субектите на данни (Чл. 35) - всички по същите линии като ОРЗД.

По-специално глава IV включва разпоредби относно принципа за „защита на данните при проектиране и по подразбиране“ (чл. 27); относно договореностите, които трябва да се въведат по отношение на „съвместни администратори“ (чл. 28), обработващи (чл. 29) и лица, действащи под ръководството на администратора или обработващия лични данни (чл. 30); относно задължението („отчетност“) да поддържа подробна документация за дейностите по обработка (чл. 31); относно сигурността на обработването (чл. 33), уведомяване за нарушения на данните на Европейския надзорен орган по защита на данните (ЕНОЗД) (който е надзорният орган по отношение на институциите и органите на ЕС) (чл. 34) и съобщаване на нарушения на данните на субектите на данни (Чл. 35) - всички по същите линии като ОРЗД.

Регламент 2018/1725 (подобно на своя предшественик, Регламент 45/2001, обсъден в раздел 1.3.6 по-горе) изисква от всяка институция или орган на Съюза да назначи служител по защита на данните (DPO) (чл. 43) - което също отново е на линия с изискването в ОРЗД по отношение на контролерите в публичния сектор. Разпоредбите относно позицията на DPO (чл. 44) и за задачите на DPO (чл. 45) също са в съответствие с ОРЗД, с някои допълнителни разпоредби за достъп до DPO от всеки и защита срещу предразсъдъци за извършване така (чл. 44) (7) и относно срока за назначаване на DPO

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1725

(чл. 45, пар. 8); и по отношение на задачата на DPO, малко по-строго условие (не се намира в ОРЗД), че DPO „гарантира по независим начин вътрешното приложение на настоящия регламент“ (чл. 45, пар. 1, буква б)).[201]

Регламент 2018/1725 също изисква извършването на оценка на въздействието върху защитата на данните (DPIA), при същите обстоятелства, както е предвидено в ОРЗД, т.е. във връзка с обработването, „което може да доведе до висок риск за правата и свободите на физически лица ”(чл. 39); и предвижда, че трябва да има „предварителна консултация“ с ЕНОЗД при подобни обстоятелства, както е предвидено за предварителна консултация със съответния надзорен орган в ОРЗД, т.е. ако DPIA посочи, че тези рискове не могат да бъдат достатъчно смекчени (чл. 40) Последното изречение на член 40 от полза добавя, че „администраторът трябва да потърси съветите на служителя по защита на данните относно необходимостта от предварителна консултация“, но това, разбира се, е препоръчително и при обработката по ОРЗД.)

Що се отнася до съществото съдържание, Регламент 2018/1725 също се основава на същите определения (чл. 3) и основни принципи (чл. 4) като ОРЗД и съдържа фактически същите правила по въпроси като съгласие и други правни основания за обработка на не - чувствителни и чувствителни данни (вж. чл. 5 - 13), но с някои допълнителни подробности относно „съвместимото обработване“ (чл. 6) и предаването на лични данни на получателите в държавите-членки (чл. 9); [202]и права на субектите на данни (чл. 14 - 24), включително във връзка с вземането на напълно автоматизирани решения и профилиране (чл. 24).

Той също така предвижда по същество същите допустими ограничения за правата на субектите на данни и задължението за съобщаване на нарушение на личните данни на субекта на данните (чл. 25, пар. 1), но разширява и задължението за гарантиране на поверителността на електронните съобщения (отбелязано по-долу) и, което е по-важно, определя по-конкретни правила за това, което всеки „правен акт или вътрешно правило“, предвиждащ такива ограничения, трябва да изясни конкретно (вж. чл. 25, пар. 2). Освен това, Европейският надзорен орган по защита на данните трябва да бъде консултиран относно проектите на подобни правила (чл. 41, пар. 2), което представлява значителна гаранция, че те наистина ще бъдат ограничени до „необходимото и пропорционално ... в демократичното общество“.

Регламент 2018/1725 включва специален раздел (глава IV, раздел 3) **относно поверителността на електронните съобщения. Това предвижда това**

> Институциите и органите на Съюза **гарантират поверителността на електронните съобщения**, по-специално като осигуряват сигурността на своите електронни съобщителни мрежи (чл. 36, добавен акцент)

[201] Това е по-силно, защото, въпреки че ОРЗД предвижда, че „[администраторът и обработващият данни трябва да гарантира, че служителят по защита на данните не получава никакви инструкции относно изпълнението на тези задачи „и че“ той/тя няма да бъдат уволнени или санкционирани от администратора или обработващия за извършване на неговитое задачи “(чл. 38, пар. 3 от ОРЗД), който ефективно гарантира, че ДЛЗД може да действа по„ независим начин “, ОРЗД казва, че ДЛЗД трябва да„ следи за спазването на [ОРЗД и други съответни правила] “и„ информира и съветва „администратора и неговите служители (и всички обработващи) за техните задължения (съответно чл. 39, пар. 1, букви б) и а), ОРЗД не изисква от ДЛЗД да„ осигурява “вътрешно спазване, законовата отговорност остава на администратора.

[202] Вижте подраздел 1.4.6 по-долу.

и че те:

> **Защитават** информацията, предавана към, съхранявана в, свързана с, обработвана и събирана от крайните устройства на ползвателите, осъществяващи достъп до техните обществено достъпни уебсайтове и мобилни приложения в съответствие с член 5, параграф 3 от Директива 2002/58/ЕО [т.е. Директива за електронната поверителност, обсъдена в раздел 1.3.3 по-горе] (чл. 37, акцент).

Последният член в този раздел се отнася до **указатели на ползвателите**, както са дефинирани в чл. 3, пар. 24, т.е. всяка:

> публично достъпни указател на ползвателите или вътрешни указатели на ползвателите, налични в институция или орган на Съюза или споделени между институции и органи на Съюза, независимо дали в печатна или електронна форма.

В това отношение член 38 предвижда, че личните данни, съдържащи се в такива указатели, трябва да бъдат „ ограничени до степента, която е строго необходима за специфичните цели на указателите “ (чл. 38, пар. 1) и че институциите и органите трябва да:

> предприемат всички необходими мерки за предотвратяване на използването на съдържащите се в посочените указатели лични данни за целите на директния маркетинг, независимо дали те са достъпни за обществеността или не..

Правилата в този раздел отразяват някои от правилата в Директивата за електронна поверителност, обсъдени в раздел 1.3.3 по-горе.

Правилата за **прехвърляне на лични данни на трети страни или международни организации,** съдържащи се в глава V от Регламент 2018/1725, отново следват същата схема, която се съдържа в ОРЗД: такива трансфери могат да се извършват само:

- въз основа на решение за адекватното ниво на защита от Комисията съгласно ОРЗД; или

- ако „ подходящи гаранции “ са осигурени чрез:

  • правно обвързващ и приложим инструмент между публичните органи;

  • стандартни клаузи за защита на данните, приети от Комисията;

  • стандартни клаузи за защита на данните, приети от ЕНОЗД и одобрени от Комисията;

  • във връзка с прехвърляния на обработващ, който не е институция или орган на Съюза: Обвързващи корпоративни правила (ОКП), кодекси за поведение или сертификати, издадени съгласно ОРЗД; или

  предмет на разрешение от ЕНОЗД:

  • договорни клаузи между съответните образувания; или

  • разпоредби за защита на данните, включени в административни договорености (споразумения) между публичните органи или органи.

(Член 48)

Регламент 2018/1725 също съдържа уговорката, идентична на тази в ОРЗД, че:

> Всяко решение на съд или трибунал и всяко решение на административен орган на трета държава, с което от администратор или обработващ лични данни се изисква да предаде или разкрие лични данни, могат да бъдат признати или да подлежат на изпълнение по какъвто и да било начин само ако се основават на международно. (Чл. 49)

И накрая, в това отношение член 50 от Регламент 2018/1725 предвижда трансфери въз основа на „**дерогации за конкретни ситуации**“, по същия ред, като този, посочен в ОРЗД, т.е. когато субектът на данни „**е изрично съгласен**“ към предложеното прехвърляне (чл. 50, пар. 1, буква а)) или когато прехвърлянето е „**необходимо**“ в **договорен контекст** (чл. 50, пар. 1, букви б) и в) **по важни причини от обществен интерес признати в правото на Съюза** (чл. 50, пар. 1, буква г), прочетено с чл. 50, пар. 3), за установяване, упражняване или защита на **правни искове** (чл. 50, пар. 1, буква д) или за защита на **жизнените интереси на субекта на данни или на други лица,** когато субектът на данни е физически или юридически неспособен да даде съгласие (чл. 50, пар. 1, буква е) или когато прехвърлянето се извършва от **публично достъпен регистър** (при условие че в конкретния случай са изпълнени предвидените в правото на Съюза условия за извършване на) (чл. 50, пар. 1, буква ж)).

Регламент 2018/1725, подобно на ОРЗД във връзка с публичните органи, предвижда, че първите три от тези специални дерогации (изрично съгласие на субекта на данните; в контекста на договор) „не се прилага за дейности, извършвани от институциите и органите на Съюза при упражняването на техните публични”(чл. 50, пар. 2).

Глава VI от Регламент 2018/1725 обхваща **създаването, правилата, позицията, задачите и задълженията на ЕНОЗД.** По същество ЕНОЗД изпълнява във връзка с обработването на лични данни от институциите и органите на Съюза същата функция като надзорните органи (органи по защита на данните, ОЗД), създадени съгласно ОРЗД, изпълняват във връзка с обработването на лични данни от съответните национални публични органи в държавата-членка (или регион на държава-членка), за която те са компетентни.

Глава VII обхваща **сътрудничеството между и координирания надзор от Европейския надзорен орган по защита на данните и националните надзорни органи.** Регламентът, също като ОРЗД, **насърчава сътрудничеството с трети страни и международни организации** за защита на личните данни (чл. 51).[203]

И накрая, глава VIII се занимава с средства за **правна защита, отговорност и санкции,** които отново са подобни на тези, изисквани от ОРЗД. Достатъчно е да се отбележи, че всеки субект на данни, чиито лични данни са или са обработени от институция или орган на ЕС, може да подаде жалба до ЕНОЗД (чл. 63) (също както всеки субект на данни може да се оплаче съгласно ОРЗД на съответния национален ОЗД) и (отново като ОРЗД) има право на обезщетение за всякакви материални или неимуществени вреди, причинени от всяко нарушение на регламента (чл. 65). Освен това, както според ОРЗД, субектите на данни в такива случаи могат да бъдат представлявани от организации с нестопанска цел, действащи по отношение на личните данни (чл. 67), към които Регламентът добавя

[203] Както в ОРЗД, съответната разпоредба (чл. 50 от ОРЗД) е някак странно поставена в главата, която се занимава с пренос на данни, а не в тази относно задачите и правомощията на надзорните органи.

допълнителна разпоредба относно жалбите от служители на ЕС (чл. 68). Обратно, вяко длъжностно лице на ЕС, което не изпълни задълженията, наложени с регламента, подлежи на дисциплинарно наказание (чл. 69).

Съдът на ЕС е компетентен по всеки спор, свързан с Регламента, включително по отношение на обезщетението (чл. 64). **ЕНОЗД може да налага административни глоби** на институциите и органите на Съюза, които не спазват регламента (чл. 66) (въпреки че размера на глобите е много по-ниско от нивото, предвидено в ОРЗД).[204]

Като се има предвид, че основният режим на защита на данните съгласно Регламент 2018/1725 е толкова тясно приведен в съответствие с ОРЗД, - често много подробни и практични - насоки и възгледи, издадени от Европейския надзорен орган по защита на данните към институциите и органите на ЕС, които са обект на този режим, също да има пряко значение за администраторите/обработващи лични данни съгласбо ОРЗДФ, особено в публичния сектор, и следователно трябва да бъдат внимателно проучвани от всяко ДЛЗД, което работи за такъв администратор (заедно, разбира се, с ръководствата и становищата на Европейския комитет за защита на данните. , чийто член е ЕНОЗД: мненията на ЕНОЗД и ЕКЗД се вписват взаимно)

- **Режимът на защита на данните, приложим за институциите и органите на ЕС, които участват в полицейското и съдебното сътрудничество:**

Общи приложения:

Както бе отбелязано по-горе, Регламент 2018/1725 създава **отделен режим на защита на данните за институциите и органите на ЕС, които участват в полицейското и съдебното сътрудничество** (т.е. участващи в „дейности, които попадат в обхвата на глава 4 или глава 5 от дял V от част трета от ДФЕС "). Този отделен режим е установен **в глава IX от Регламента**, включващ членове 70—95 (при което чл. 2, пар. 2 пояснява, че **определенията**, посочени в члл 3, се прилагат и за тази глава).[205]

Специалният режим регулира обработването от страна на съответните институции или органи на „**лични данни от оперативен характер**". Те са дефинирани в член 3, параграф 2 като:

> всички лични данни, които се обработват от органи, служби или агенции на Съюза при извършването на дейности, които попадат в обхвата на

[204] Максималните глоби, които ЕНОЗД може да наложи на институциите или органите на ЕС за неспазване на Регламент 2018/1725, съответно са 25 000 евро за нарушение и до общо 250 000 евро годишно за някои нарушения и 50 000 евро за нарушение и до общо 500 000 евро годишно за някои нарушения (вж. чл. 66, пар. 2 и 3). Това се сравнява с административни глоби до 10 000 000 евро, или в случай на предприятие (частна компания) до 2% от общия годишен оборот в световен мащаб (който е по-висок) за някои нарушения, и до 20 000 000 евро или в случай на предприятие до 4% от общия годишен оборот в световен мащаб (който е по-висок) за някои нарушения, които могат да бъдат наложени съгласно ОРЗД (чл. 83, пар. 4 и 5) - въпреки че ОРЗД също така позволява на държавите-членки да намалят тези суми или дори напълно да изключат публичните органи и органи, установени на тяхна територия, от административни глоби изцяло (чл. 83, пар. 7) (но тези органи, освободени от глоби или подлежащи на намаляване на глобите, все още трябва да останат при спазване на правомощията на съответните ОЗД съгласно чл. 58, пар. 2 от ОРЗД).

[205] Относно въпроса дали и ако да, до каква степен главите VII и VIII се прилагат за обработка съгласно глава IX, вижте по-долу, под заглавията „Права, надзор и изпълнение".

част трета, дял V, глава 4 или глава 5 от ДФЕС, за постигане на целите и изпълнение на задачите, определени в правните актове за създаване на тези органи, служби или агенции.

По принцип обработката на такива **лични данни от оперативен характер** е предмет на специалния режим в глава IX, докато обработването на всички „неоперативни“ лични данни - като например данни за човешките ресурси, свързани с персонала на съответните институции и органи - подлежи на основният режим, посочен в по-ранните глави на Регламент 2018/1725, както е описано в предишното подзаглавие.

В това предишно подзаглавие отбелязахме, че правилата за основния режим са тясно приведени в съответствие с ОРЗД. По същия начин правилата в глава IX от Регламент 2018/1725 често са в съответствие сДиректива (ЕС) 2016/680 , обсъдена в раздел 1.4.3 по-горе (или с тази Директива и с ОРЗД и правилата за основните режим съгласно Регламент 2018/1725) - но глава IX не е толкова тясно свързана с Директива (ЕС) 2016/680, колкото основният режим е с ОРЗД. Въпросите могат да бъдат доста сложни.[206]

Като се има предвид, че този наръчник е насочен към ДЛЗД в публичните органи в държавите-членки, подробностите за съответствието или разминаването между правилата в глава IX и тези в по-ранната част на Регламент 2018/1725 - и тези в основните инструменти на ЕС за защита на данните , ОРЗД и Директива (ЕС) 2016/680 - не трябва да се обсъждат тук. Два следващи въпроса обаче могат да бъдат отбелязани в следващите подзаглавия.

Права, надзор и прилагане:

В глава IX няма **позовавания** на правото на субекта на данни на **обезщетение за вреди, причинени от неправомерно обработване** (което в случая би означавало обработка в противоречие с разпоредбите на тази глава), на правото на субектите на данни да бъдат **представлявани** от –организация с нестопанска цел или на правомощията на ЕНОЗД да налага административни глоби.

Разпоредбите на глава IX споменават многократно задължение от страна на администратор, предмет на глава IX, да **информира субектите на данни** за тяхното **право да подадат жалба до ЕНОЗД** (вж. Чл. 79, пар. 1, буква г), 80 (е) и 81 (2)) и реалната възможност да се предяви **съдебен иск пред Съда на ЕС** (чл. 81, пар. 2. Администраторите, предмет на глава IX, могат също така да осигурят **правата на субектите на данни** в някои случаи да бъдат „упражнявани чрез Европейския Надзорен

[206] Да дадем само един пример: тясно свързан с новия принцип на „отчетност“, който се прилага за всички съвременни инструменти на ЕС за защита на данните, е задължение на администраторите да водят записи и регистри. Въпреки това ОРЗД и правилата, приложими към основния режим съгласно Регламент 2018/1725, изискват воденето на подробна документация за всички операции по обработка (чл. 30 от ОРЗД; чл. 31 от Регламент 2018/1725), но не изискват запазването им от трупи. Директива (ЕС) 2016/680 изисква както подробни записи, така и регистрационни данни (чл. 24 и 25). Но глава IX от Регламент 2018/1725 изисква само да се съхраняват регистрационни файлове във връзка с обработката на лични данни от оперативен характер (чл. 88), без да се споменават записи.

орган по защита на данните "(чл. 84, пар. 1, т.е. само косвено; и в този случай те също трябва да:

> **информира субекта на данните за възможността да упражнява правата си чрез Европейския надзорен орган по защита на данните** в съответствие с параграф 1. (чл. 84, пар. 2)

Администраторът също така трябва да предостави **записите** на своите операции по обработка **на разположение на ЕНОЗД** при поискване (чл. 88, пар. 3) и да **докладва за ЕНОЗД нарушения на личните данни** (чл. 92, пар. 1 и 4).

От член 2, параграф 2 обаче ясно, че главата от регламента, която действително предвижда обработването на жалби от ЕНОЗД и юрисдикцията на Съда на ЕС, както и изпълнителните действия от страна на ЕНОЗД, също и в случаите на нарушенията на личните данни (глава VIII) и главата, която действително излага задачите и правомощията на ЕНОЗД във връзка с това (глава VI), не се прилагат за обработка на оперативни данни, които са предмет само на глава IX.

Изглежда, че на практика ЕНОЗД поема надзорни и консултативни правомощия, също и във връзка с обработването налични данни от оперативен характер от институции и органи на ЕС съгласно глава IX от Регламент 2018/1725 и ще бъде готов да приема жалби от субектите на данни във връзка с такава обработка. Дали той ще позволи на субектите на данни да бъдат представлявани от НПО в такива случаи, или би желал да постанови обезщетение или дори да наложи административни глоби на съответните институции и органи - и дали Съдът на ЕС ще одобри такова упражняване на правомощията на ЕНОЗД в връзка с такава обработка - предстои да видим.

Изключения от/и забавено прилагане на Регламент 2018/1725

По принцип Регламент 2018/1725 се прилага за **цялата обработка на лични данни от всички институции и органи на Съюза** (чл. 2, пар. 1) - макар и, както видяхме, чрез създаване на два различни правни режима. Регламентът съдържа също някои изключения от прилагането му и предвижда забавено прилагане на неговите разпоредби в контекста на някои ситуации, както е обсъдено по-нататък.

- **Изключения:**

Член 2, параграф 4 предвижда:

> Настоящият регламент не се прилага за обработването на лични данни от мисиите, посочени в член 42, параграф 1 и членове 43 и 44 от ДЕС. (Акцент е добавен)

Мисиите и задачите, обхванати от изключенията, са:

- мисии извън Съюза за поддържане на мира, предотвратяване на конфликти и укрепване на международната сигурност в съответствие с принципите на Устава на Организацията на обединените нации (чл. 42, пар. 1); и
- съвместни операции по разоръжаване, хуманитарни и евакуационни мисии, мисии за съвет и помощ във военната област, мисии за предотвратяване на конфликти и поддържане на мира, мисии на военни сили за управление на кризи, включително умиротворителни

> мисии и стабилизиращи операции след края на конфликти. Всички тези задачи (чл. 43, на който чл. 44 се разширява).

Второто изречение на член 43 добавя, че всички операции и задачи, споменати в този член, „могат да допринесат за борбата срещу тероризма, включително чрез подкрепата, оказвана на трети страни, за да се борят с тероризма на своя територия “.

- **Забавено прилагане:**

Освен горепосоченото изключване на прилагането на Регламента във връзка с конкретни операции, за които могат да бъдат определени конкретни правила, Регламентът също така определя процесите за привеждане на операциите по обработка на някои други институции и органи на ЕС в съответствие с Регламент 2018 / 1725, със срокове за съответните прегледи (но не и за действителното привеждане в съответствие на тези операции с регламента). По-конкретно, член 2, параграф 3 гласи:

> Настоящият регламент не се прилага за лични данни от оперативен характер от страна на Европол и Европейската прокуратура, преди [пред-лисабонските регламенти, които обхващат тяхната дейност] [207]да бъдат адаптирани в съответствие с член 98 от настоящия Регламент. (акценти са добавени)

Освен това член 98 предвижда:

> 1. **До 30 април 2022 г.** Комисията **преразглежда** правни актове, приети въз основа на договорите, които регулират обработката на лични данни от оперативен характер от органи, служби или агенции на Съюза при извършване на дейности, попадащи в обхвата на глава 4 или глава 5 от дял V от трета част от ДФЕС [т.е., които се отнасят до полицейското или съдебното сътрудничество], с цел да:
>
> а) **оценява** тяхното съответствие с [Директива (ЕС) 2016/680 (както е разгледано в раздел 1.4.3 по-горе)] и глава IX от настоящия Регламент;
>
> б) **идентифицира** всякакви различия, които могат да възпрепятстват обмена на лични данни от оперативен характер между органи, служби или агенции на Съюза при извършване на дейности в тези области и компетентните органи; и
>
> в) **идентифицира** всички различия, които могат да създадат правна фрагментация на законодателството за защита на данните в Съюза.

[207] Съответно: Регламент (ЕС) 2016/794 на Европейския парламент и на Съвета от 11 май 2016 г. относно Агенцията на Европейския съюз за сътрудничество в областта на правоприлагането (Европол) и замяна и отмяна на решения на Съвета 2009/371 / ПВР, 2009/934 / ПВР , 2009/935 / ПВР, 2009/936 / ПВР и 2009/968 / ПВР, ОВ L 135, 24 май 2016 г., стр. 53 и Регламент (ЕС) 2017/1939 на Съвета от 12 октомври 2017 г. за прилагане на засилено сътрудничество при създаването на Европейската прокуратура (the„EPPO“), ОВ L 283, 31 октомври 2017 г., стр. 1.

2. Въз основа на прегледа, за да се осигури еднаква и последователна защита на физическите лица по отношение на обработването, **Комисията може да представи подходящи законодателни предложения, по-специално с оглед прилагането на глава IX от настоящия Регламент към Европол и Офиса на европейската Прокуратура** и включително адаптации на глава IX от настоящия Регламент, ако е необходимо.

(добавени акценти)

С други думи, регламентите, обхващащи работата на Европол и Европейската прокуратура, както и на всички други институции и органи, обхванати от член 98, трябва да бъдат преразгледани до 30 април 2022 г. и след това Комисията може да предложи нови правила с оглед привличане на личните данни данни от тези органи в съответствие с Директива (ЕС) 2016/680 (обсъдени в раздел 1.4.3 по-горе) и със специалните правила в глава IX от Регламента (обсъдени по-горе). Не е определена обаче дата за действителното приемане на такива нови правила, които ще изискват законодателни действия от страна на Министерския съвет и евентуално новия Европейски парламент и получаване на становища от Европейския надзорен орган по защита на данните и Европейския съвет за защита на данните - като всичко ще отнеме известно време. Докато тези регламенти не бъдат изменени с тази цел - т.е. поне през следващите няколко години - обработването на лични данни от Европол и Европейската прокуратура (и всякакви други институции или органи, обхванати от чл. 98 от Регламент 2018/1725) ще остане под тяхната собствена , действащи (преди 2018 г.) правила за защита на данните.

1.4.6 Предаване на лични данни между различни режими на защита на данните в ЕС

I. Различните режими за защита на данните

От различните по-ранни раздели ще стане ясно, че всъщност съществуват значително множество **различни, общи или по-специфични режими за защита на данните в основните инструменти и рамки за защита на данните на ЕС, както и някои други извън тях** (и дори извън **законодателството на ЕС**), включително посочените по-долу. Кой режим се прилага за определена дейност или операция по обработка, ще зависи от оценката на всяка такава дейност или операция и нейната специфична цел, по-специално дали въпросът попада в компетенцията на ЕС или не, дали се осъществява в частния или публичния сектор, независимо дали тя включва европейски или национални институции, действащи във връзка с икономически или наказателни дела, и т.н.

Общ регламент за защита на данните:

- Режимът на ОРЗД, приложен към обработката от частни субекти.
- Режимът на ОРЗД, прилаган за обработване от публични субекти, които не участват в наказателно-правна или обществена сигурност или въпроси на националната сигурност (или когато не са замесени в такива въпроси) (при което „обществената сигурност“ трябва да се чете като много ограничена категория) ,

Директива за електронната поверителност / предложен Регламент за електронна поверителност

- Специфичните правила, приложими към доставчиците на услуги за електронна комуникация (а в бъдеще и за други доставчици, като например плейъри „Over-The-Top“).
- Специфичните правила, приложими за всички уеб хостове (включително публичните органи със собствени уеб страници) във връзка с поверителността на комуникациите, използването на „бисквитки“ и др.

Директива (ЕС) 2016/680:

- Директива (ЕС) 2016/680, както се прилага към публичните субекти („компетентните органи“), когато обработват лични данни „за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наложените наказания, включително предпазването от заплахи за обществената сигурност “, или като тяхна основна задача, или от време на време, встрани от други обществени задачи.

Зони, освободени от Директива (ЕС) 2016/680 (към настоящия момент):

- Правилата в приблизително 123 правни инструмента на ЕС, отнасящи се до така наричаните преди въпроси относно, „правосъдие и вътрешни работи“ (ПВР), влезли в сила преди 6 май 2016 г. (които продължават да се прилагат, дори ако все още не са в съответствие с Директивата).
- Правилата в „международни споразумения за предаване на лични данни на трети държави или международни организации, които са сключени от държавите членки преди 6 май 2016 г. и които са в съответствие с правото на Съюза, приложимо преди посочената дата“ (които също продължават да се прилагат дори ако все още не съответстват на Директивата).
- Правилата за използването на „автоматизирани системи за обработка, създадени преди 6 май 2016 г.“ в държавите-членки, ако те все още не са приведени в съответствие с Директивата, защото това би включвало „непропорционални усилия“.

Обработка на лични данни в областта на ОВППС:

- Обработка от Върховния представител на ЕС по въпросите на външните работи и политиката на сигурност, Европейската служба за външни действия (ЕСВД) и 141 делегации на ЕС по целия свят, службата за инструменти на външната политика и обработката от държавите-членки във връзка с тези въпроси (включително във връзка с приемането на решения на Съвета в областта на ОВППС) - които все още не са обект на конкретен инструмент на ЕС за защита на данните. [Но имайте предвид третото тире под следващото заглавие]

Обработка на лични данни от институции или органи на ЕС съгласно Регламент 2018/1725:

- Режимът на защита на данните, приложим за институциите и органите на ЕС, които не участват в полицейското и съдебното сътрудничество.

- Режимът на защита на данните, приложим за институциите и органите на ЕС, които участват в полицейското и съдебното сътрудничество.
- Обработка от секретариата на Съвета при прилагане на решенията на Съвета за ОВППС - ограничената област на дейност, свързана с ОВППС, която е предмет на правила за защита на данните, т.е. Регламент 2018/1725.

Зони, освободени от Регламент 2018/1725 (засега):

- Обработка на лични данни от мисии на ЕС, насочени към **поддържане на мира**, предотвратяване на конфликти и укрепване на международната сигурност, или натоварени със съвместни операции по **разоръжаване, хуманитарни и спасителни задачи**, военни съвети и задачи за подпомагане, задачи за **предотвратяване на конфликти и поддържане на мира**, задачи за **бойни сили в управлението на кризи**, включително мироопазващи мисии **и следконфликтната стабилизация** (включително когато тези задачи са свързани с борбата срещу тероризма, включително чрез подкрепа на трети страни в борбата с тероризма на техните територии).
- Обработка на лични данни от Европол и Европейската прокуратура (ЕРРО) и други „органи, служби или агенции на Съюза при извършване на дейности, които попадат в обхвата на глава 4 или глава 5 от дял V на част трета от ДФЕС [т.е. които се отнасят до полицейското или съдебното сътрудничество] ", което ще продължи да се осъществява въз основа на правните инструменти на ЕС, свързани с Европол или Европейската прокуратура, или по друг начин с полицейското или съдебното сътрудничество, приети преди Регламент 2018/1725.

Национална сигурност:

- Обработване на лични данни от държавите-членки във връзка с националната сигурност - **което е извън обхвата на правото на ЕС,** дори извън обхвата на Хартата на основните права (въпреки че такова обработване, разбира се, е предмет на Европейската конвенция за правата на човека и юрисдикция на Европейския съд по правата на човека).[208]

Не винаги е лесно да се очертаят ясни граници между тези множество различни режими, например между полицейски действия срещу престъпността, действия на полицията за осигуряване на реда, действия на полицията и други органи за гарантиране на „вътрешна сигурност", „обществена сигурност" и „национална сигурност

[208] Европейският съд по правата на човека постанови няколко важни решения в това отношение. Вижте: Европейски съд по изследвания на правата на човека, отдел „Национална сигурност и европейска съдебна практика", Съвет на Европа, 2013 г., достъпен на:

https://www.echr.coe.int/Documents/Research_report_national_security_ENG.pdf

Те обаче не могат да се прилагат от институциите на ЕС във връзка с такива дейности.

“И между тези действия и действията на ЕС във връзка с„ тероризма “[209], гореспоменатите задачи на мисиите на ЕС и„ международната сигурност “.

Това не е мястото за изследване на тези различия в дълбочина. Достатъчно е да се отбележи, че когато различни режими се прилагат към различните дейности (дейности, попадащи в повече от една от посочените горе категории), може би дори от едни и същи участници, това ще бъде важно за съответните участници като администратори (а често и като обработващи, например, когато подкрепят други такива участници), **за да изяснят за себе си кой законов режим се прилага към коя операция за обработка на лични данни и към какви лични данни, чрез анализ на всяка конкретна въпросна операция по обработка на данни.** Законосъобразността на обработването и обхватът и изключенията на такива важни въпроси като правата на субектите на данни винаги са крайно зависими от такива пояснения.

Публичните органи, участващи в различни дейности, които са обект на различни режими за защита на данните, винаги трябва внимателно да разграничават техните различни дейности, различни операции за обработка и различни лични данни, използвани за различните операции, в техните записи за обработка на лични данни и в техните оценки на такава обработка.[210] Служителите по защита на данните в такива публични органи ще трябва да играят решаваща роля в това отношение.[211]

II. Предаване на лични данни

Специални проблеми възникват, когато се предлага или се иска личните данни, получени за една конкретна цел съгласно правилата в един от гореспоменатите правни режими, да бъдат използвани от същия администратор за различна цел, за обработка при различен правен режим; или да бъдат предадени или предоставени по друг начин на друг орган (друг администратор) за такава различна цел, за обработка при различен правен режим.[212]

Например, образователният отдел на местната власт може да събира лични данни на ученици за образователни цели съгласно ОРЗД, но може да бъде поискан достъп от местната полицейска агенция до (някои от) тези данни, за да помогне в разрешаването на местната престъпност (например, за да проверите кои деца са отсъствали от училище в определен ден). Предлаганото обработване на данните за втора цел би било по силата на Директива (ЕС) 2016/680 (или по-точно - националните правни разпоредби, транспониращи Директивата, както и съгласно съответния полицейски или наказателен процесуален закон). Понякога приложимите закони или правни норми пояснят кога могат да се извършват такива оповестявания (например само във връзка с определени престъпления или само ако е имало основателно подозрение към идентифицирани деца или само ако съдия е издал заповед). Но често това ще бъде решено от съответната местна власт в спрямо правилата в различните приложими инструменти. **ДЛЗД на местната власт ще има важна роля при консултирането по този въпрос (и ако има някакво съмнение, трябва да се консултира с ОЗД).**

предмет на дейност към разли чни режими за защита на данните.

[211] Вижте част трета от това ръководство.

[212] ВЖ.

Регламент 2018/1725 предоставя някои насоки относно предаването на лични данни от институция или орган на ЕС на „ установени в Съюза получатели, различни от институции и органи на Съюза“ - обикновено публични органи на държавите-членки. Институциите и органите на ЕС имат право да предават данни на образувание в държава-членка, изискващо данните, при условие че:

a) получателят [т.е. образуването в държава-членка, поискала данните] установи, че данните са необходими за изпълнението на задача от обществен интерес или при упражняването на предоставени на получателя официални правомощия [т.е. в това образувание]; или
b) получателят установи, че е необходимо данните да бъдат предадени за конкретна цел от обществен интерес, а администраторът, [т.е. институцията или органът на ЕС, помолен да предостави данните] ако има някакво основание да се предполага, че законните интереси на субекта на данните могат да бъдат накърнени, установи, че е пропорционално личните данни да бъдат предадени специално за тази цел, след като е претеглил по безспорен начин различните противоречащи си интереси.

(Чл. 9, пар. 1)

Институциите или органите на ЕС имат право да предават (изпращат) такива данни на образувания в държавите-членки, без да бъдат поискани, т.е. служебно, ако могат:

> демонстрират, че предаването на лични данни е необходимо и пропорционално на целите на предаването чрез прилагане на критериите, определени в пар. 1, букви а) или б).
>
> (Чл. 9, пар. 2)

Но няколко въпроса трябва да бъдат взети под внимание в това отношение. На първо място, гореспоменатото се отнася за институциите и органите на ЕС, които не участват в обработката във връзка с полицейското и съдебно сътрудничество, т.е., това се отнася само за обработване - и предаване - в рамките на "главния режим", създаден с Регламент 2018/1725 за институциите и органите на ЕС; и както е отбелязано в раздел 1.4.5 по-горе, "основния" режим за защита на данните в този Регламент е тясно свързан с ОРЗД. Не съществува правило относно предаване на лични данни на органите в държавите-членки, посочени в глава IX от Регламент 2018/1725, който обхваща

обработката на "оперативните" лични данни от институциите и органите на ЕС, които участват в полицейското и съдебно сътрудничество.

Второ, правилата в член 9, цитирани по-горе, са „без да се засягат“ основните принципи за защита на данните, включително ограничаване на целта и правило за „съвместима“ обработка (вж. Чл. 6 от Регламента, който добавя значителни условия към това) , уместност на данните и т.н., както и към разпоредбите за законно обработване (виж уводната клауза към чл. 9, пар. 1). Те също не засягат специалните правила за обработка на чувствителни лични данни.

Все пак член 9 от Регламент 2018/1725 илюстрира, че всеки път, **когато личните данни, които се обработват по един от гореспоменатите режими, трябва да бъдат предадени на друго образувание (или дори използвано от същото) за обработка при друг режим, трябва да се обърне внимание на важни въпроси относно целта, уместността и адекватността на данните, както и относно законосъобразността, необходимостта и пропорционалността на промяната в предназначението.**

Във връзка с това е важно да се помни, че на първо място „предаването“ на данни, подобно на всяка друга форма на „разкриване“ на лични данни (включително „предоставяне на [лични данни] на разположение“), например онлайн), представлява форма на обработка (виж чл. 4, пар. 2 от ОРЗД, повторено дословно във всички останали инструменти на ЕС за защита на данните). Второ, важното е, че всяко „предаване“ на лични данни между различни образувания винаги има два аспекта:

- за предаващото образувание това е форма на **разкриване** на данните (виж по-горе); но
- за получаващото образувание представлява **събиране** на лични данни - което е отделен акт, обхванат от общата концепция за „обработка“, различна от „разкриване“, „предаване“ или „предоставяне“ на лични данни.

Ако във връзка със съответните си дейности, свързани с предаването на данни, двете образувания се подчиняват на различни режими за защита на данните, всяко следва да оцени съвместимостта на съответното си действие с правилата за защита на данните, които се прилагат към тях.

По този начин в горния пример, местният образователен институция ще бъде подчинен на ОРЗД и на всякакви „допълнителни спецификации“ за това как трябва да се прилагат разпоредбите на ОРЗД, посочени в съответния национален закон за защита на данните (или може би в подходящ раздел за защита на данните в закона за задачите и правомощията на местните образователни институции, които все още трябва да съответстват на ОРЗД).

От друга страна, местната полицейска служба ще се подчинява на националните законови разпоредби, приети за прилагане на Директива (ЕС) 2016/680 (както и на всички съответни правила в националните полицейски или наказателни процесуални закони, които следва да бъдат в съответствие с Директивата).

(cc)

В този случай местната образователна институция трябва да провери (с помощта на своето ДЛЗД и ако има нужда със съвет от съответното ОЗД) дали правилата за

Често съответните правила ще бъдат взаимно съвместими и всъщност ще препращат едно към друго. Например полицейският закон може да предвижда, когато и при какви условия, местната полицейска служба може да изисква от „други публични органи“ информация (като цяло и / или за децата); и правилата, приложими към образователната институция, могат да предвиждат, че отделът може - или трябва да предоставя информация, поискана от „друг публичен орган“ (или конкретно от полицията), при условие че искането е законосъобразно. Това все още ще изисква полицейската служба да спазва правилата и да отговаря на съответните условия, а образователната институция да иска поне уверения (и доказателства), че искането от полицията е законно и отговаря на съответните условия. Но това настрана, няма проблем по отношение на предаването на данните.

Когато както предаващата агенция/институция, така и тази която изисква данните са предмет на най-новите правила на ЕС за защита на данните, описани по-горе - по-специално ОРЗД, Директива (ЕС) 2016/680 и Регламент 2018/1725 - обикновено няма проблеми в това отношение (въпреки че отделните случаи все още могат да изискват сериозен анализ и внимание).

Въпросите са по-малко ясни, когато едно образувание - по-специално образувание което изисква данни- не се подчинява на най-новите правила, но все пак само на по-малко взискателните наследствени правила - въпреки че те все още ще се основават поне на общите принципи за защита на данните, които са в основата на всички закони на ЕС за защита на данните.

Въпросите обаче на практика могат да бъдат сериозно усложнени, когато запитващият субект изобщо не е обект на подходящи правила за защита на данните - какъвто е случаят, както видяхме, по отношение на въпросите на ОВППС, свързани с опазването на мира в ЕС или други военни мисии или националната сигурност. В този контекст „подходящи“ правила са правила, които ясно се основават и признават общите принципи за защита на данните; които се отклоняват от обикновените правила, изградени върху тези принципи, само до степента, конкретно предвидена в подходящ (публично достъпен, ясен и прецизен) правен инструмент, който е „предвидим“ при

прилагането му, и само до степента, която е „строго необходима“ за съответните цел, при всякакви такива отклонения ясно „пропорционални“ на специалния контекст;[213] и които осигуряват контрол върху спазването на специалните правила от независим орган.[214]

Това не е мястото да обсъждаме това подробно. Но може да се направят някои общи изводи.

По този начин всяко предаване на лични данни от национален публичен орган (или институция или орган на ЕС), което е обект на новите правила на ЕС за защита на данните (т.е. ОРЗД, Директива (ЕС) 2016/680 или Регламент 2018/1725) на всяко национално или европейско образувание което не е обект на подходящ закон за защита на данните, потенциално е толкова ерозивен за защитата на данните на ЕС, колкото всяко прехвърляне на такива данни в държава без подходящи („адекватни“) правила за защита на данните - което по принцип е забранено, освен ако „ подходящи гаранции “са приети (вж. Глава V от ОРЗД).

Следователно образуванията, обект на който и да е от горепосочените нови инструменти на ЕС за защита на данните, трябва да бъдат внимателни, преди да предоставят лични данни, които обработват и са предмет на тези инструменти, на образуването което ги изисква, което не е предмет на подходящи правила за защита на данните. Те трябва внимателно да проверяват - както винаги, с помощта на своя ДЛЗД и ако е необходимо, като се консултират със съответния орган за защита на данните - дали инструментът, който се прилага за тях, позволява такова прехвърляне (изобщо) или го забранява или налага условия; в такъв случай, следва да откажат трансфер на данните, освен ако това не е разрешено при достатъчно ясни условия съгласно приложимия за тях инструмент.

Не е достатъчно образуването изискващо данните, което не е обект на подходящи правила за защита на данните, да посочи на образуването от което ги изисква, че то (запитващото/изискващото образувание) има разрешение да получи (събере) данните, които иска съгласно правилата, които се прилагат за нег: това може да легитимира събирането на данни по отношение на тези правила, но не легитимира разкриването на данни („предаване“) от запитаното образувание съгласно правилата за защита на данните, които се прилагат към запитания субект (особено ако тези правила са установени или приети съгласно горепосочените нови инструменти на ЕС за защита на данните).

Понякога държавите все още имат закони, които дават на някои от техните агенции - по-специално техните **разузнавателни агенции** - правото да изискват информация или достъп до информация, включително лични данни, в най-общи (леки) условия; а понякога законите са формулирани по такъв начин, че да отменят всякакви ограничения за разкриване на лична информация от други субекти, които са обект на закони за защита на данните, и които (общите закони предвиждат), че трябва да отговарят на тези

[213] Това са изискванията за върховенство на закона, разработени от Европейския съд по правата на човека и прилагани еднакво от Съда на ЕС и отразени в Хартата на основните права на ЕС, които трябва да се спазват от всяка демократична държава във всяка държавна дейност, която може да засегне основните права и свободи на личността.

[214] Както изрично е предвидено в чл. 8 (3) от Хартата

изисквания, независимо какво казват съответните правила за защита на данните, които обикновено се прилагат за тях. Това включва закони в държавите-членки.[215]

По отношение на националните агенции за сигурност, съответната държава-членка може да твърди, че правилата, съгласно които тези агенции могат да изискват информация (или достъп до бази данни), са извън обхвата на правото на ЕС - и че предаването на данни на тези агенции съгласно нейните правила е следователно също извън обхвата на правото на ЕС и извън правомощията на органите за защита на данните или Съда на ЕС.

Но това би било неправилно тълкуване на правната ситуация. Дори ако събирането на лична информация от такива агенции е извън обхвата на правото на ЕС (или правомощията на органите за защита на данните или на Съда на Европейския съюз), предаването на данните на такива агенции от всички образувания, които са обект на инструменти за защита на данните на ЕС, е в рамките на обхвата на правото на ЕС. Администраторите на такива образувания и техните ДЛЗД трябва да са запознати с това и да се консултират със своите ОЗД, когато възникнат подобни спорни случаи.

1.4.7 „Модернизираната" Конвенция на Съвета на Европа за защита на данните от 2018 г.

Въпреки че Конвенцията на Съвета на Европа от 1981 г. да беше (в общи линии) приведена в съответствие с Директивата за защита на данните на ЕО от 1995 г. чрез добавянето на правила за трансграничните потоци от данни и от независимите органи за защита на данните, в нейния Допълнителен протокол, приет през 2001 г. (както беше обсъдено по-горе в 1.3.2), тя все пак, подобно на тази Директива, губеше актуалност към края на първото десетилетие на 21 век. Работата за „осъвременяването" на Конвенцията започна през 2011 г. и „Осъвременената Конвенция" беше приета и готова за подписване на 10 октомври 2018 г.[216] Към момента на написване (декември 2018 г.), тя все още не е влязла в сила: това ще се случи три месеца след присъединяването на пет държави-членки на Съвета на Европа към осъвременената Конвенция (чл. 26, пар. 2) – но, разбира се, тогава само по отношение на тези държави членки; по отношение на другите държави-страни по Конвенцията от 1981 г. (и, където е приложимо, нейният Допълнителен протокол), старата Конвенция (и Протокол ще продължава да се прилага).[217]

Самият Съвет на Европа е предоставил много полезен **преглед на новото в**

---

[215] Вижте Дау Корф, Граници на правото (бележка под линия 172 по-горе), част 4.

[216] Вж.:
https://www.coe.int/en/web/data-protection/background-modernisation
„Модернизираната Конвенция" е в голяма степен готова до 2014 г., но формалното ѝ откриване за подпис е забавено, от части за да се даде възможност за съгласуване с ОРЗД, и отчасти – за да се обърне внимание на притеснения, изразени от една основна държава членка на Съвета на Европа.
Протоколът за изменение на Конвенцията за защита на лицата при автоматизираната обработка на лични данни, CETS 223 може да бъде намерена на:
https://www.coe.int/en/web/conventions/search-on-treaties/-/conventions/treaty/223
Консолидираният текст на МодернизиранатКонвенция може да бъде намерен на:
https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf –

[217] До средата на декември 2018 г. Модернизираната Конвенция беше подписана от 22 държави, но все още не беше ратифицирана от нито една. Вж.:
https://www.coe.int/en/web/conventions/search-on-treaties/-/conventions/treaty/223/signatures?p_auth=ZmXAeCCF

Модернизираната Конвенция, който даден по-долу:[218]

Основните новости[219] на модернизираната Конвенция могат да бъдат представени, както следва:

Предмет и цел на Конвенцията (чл. 1)

Съгласно чл. 1 целта на Конвенцията е ясно подчертана, а именно да гарантира на всички лица под юрисдикцията на една от страните (независимо от тяхната националнсот или местопребиваване) защитата на личните им данни при извършване на обработка, като по този начин допринася за спазването на техните права и основни свободи и, по-специално, правото им на личен живот.

Използвайки тази формулировка, Конвенцията подчертава факта, че обработването на лични данни може положително да се отрази и да даде възможност за упражняването на други основни права и свободи, които по този начин могат да улеснени чрез гарантиране на правото на защита на данните.

Определения и приложно поле (чл. 2 и 3)

Макар съществени понятия като определението за лични данни и това за субекти на данните да не се изменени изобщо,[220] са предложени други изменения в дефинициите: понятието за „регистър ” („file”) е изоставено. “Администратор на регистър с данни” е заменен с „администратор на данни”, в допълнение към което са използвани термините „обработващ лични данни” и „получател”.

Приложното поле включва както автоматизирано, така и неавтоматизирано обработване на лични данни (ръчно обработване, при което данните представляват част от структура, която прави невъзможно търсенето по субект на данни според предварително зададени критерии), което е в юрисдикция на страна по Конвенцията. Сборният (омнибус) характер на Конвенцията е запазен и приложното й поле естествено продължава да обхваща обработването в частния и публичния сектор, без разграничение, тъй като това е едно от големите предимства на Конвенцията.

От друга страна, Конвенцията вече не се прилага спрямо обработване на данни, извършвано от физическо лице за упражняването на чисто лични (собствени) битови дейности.[221]

Освен това, Страните вече нямат възможността да правят декларации, насочени към освобождаване от прилагането на Конвенцията на определени видове обработване на данни (напр. за целите на националната сигурност и отбраната).

---

218 Взето от:
https://rm.coe.int/modernised-conv-overview-of-the-novelties/16808accf8
Пълни подробности за всички специфични изменения в текста под формата на сравнителна графика могат да бъдат намерени на:
https://rm.coe.int/cahdata-convention-108-table-e-april2018/16808ac958 (26 страници)

219 Този [обзор] представя новостите и не повтаря разпоредбите, които вече съществуват след Конвенцията от 1981 г. и допълнителния протокол към нея от 2001 г. За цялостен поглед върху осъвременената Конвенция, моля прочетете консолидираната версия, публикувана на уебсайта на [Съвета на Европа]. (първоначална бележка под линия с редакции)

220 Но имайте предвид, че е добавен обширен коментар в Обяснителния меморандум към Осъвременената конвенция (добавена бележка под линия).

221 Такова „чисто лично обработване” беше изключено за пръв път от правилата за защита на данните в Директивата за защита на данните от 1995 г., за да се осигури зачитана на правото на личен живот; това е повторено в ОРЗД. (добавена бележка под линия).

Задължения на страните (чл. 4)

Всяка Страна трябва да приеме във вътрешното си законодателство необходимите мерки, за прилагане на разпоредбите на Конвенцията.

Освен това, всяка Страна следва да докаже, че такива мерки са реално предприети и са ефективни, както и да приеме, че Комитета по Конвенцията може да провери изпълнението на тези изисквания. Този [*нов*] процес на оценка на Страните („механизъм за последващи действия") е необходим, за да се гарантира, че нивото на защита, установено от Конвенцията, е реално предоставено от Страните.

Важно е да се отбележи, че международните организации, както и Европейският съюз сега имат възможността да се присъединят към Конвенцията (Чл. 27 (Чл. 26).

Законност на обработването на данни и качество на данните (чл. 5)

Чл. 5 разяснява приложението на принципа на пропорционалност, за да подчертае, че той следва да се прилага по време на цялото обработване, и, по-специално, по отношение на средствата и методите, използвани при обработването. Освен това е допълнително утвърденот принципа на свеждане на данните до минимум.

Въведена е нова разпоредба, която ясно да заложи правното основание за обработването: съгласието (което, за да бъде действително, трябва да отговаря на няколко критерия) на субекта на данни или някое друго законно основание, предвидено от закона (договор, жизнено важен интерес на субект на данни, правно задължение на администратора и т.н.).

Чувствителни данни (чл. 6)

Списъкът на чувствителните данни е разширен, като включва генетични и биометрични данни (които повлияха на ЕС), както и данни, обработвани за информацията, която те разкриват във връзка с членство в профсъюзни организации или етнически произход (последните две категории се добавят към съществуващата [*принципна*] забрана за обработването на лични данни, разкриващи расов произход, политически възгледи или религиозни или други убеждения, лични данни относно здравето или сексуалния живот и лични данни във връзка с престъпления, наказателни производства и осъждания).

Сигурност на данните (чл. 7)

По отношение на сигурността на данните, е въведено изискването за незабавно уведомяване за каквито и да е нарушения на сигурността на данните. Това изискване се ограничава до случаи, които може сериозно да нарушат правата и основните свободи на субектите на данни, които следва да бъдат съобщени, най-малкото, на надзорните органи.

Прозрачност на обработването (чл. 8)

Администраторите ще имат задължението да гарантират прозрачност на обработването на данни и за тази цел ще трябва да предоставят необходимата информация, по-специално във връзка с тяхната самоличност и обичайно местопребиваване или място на установяване, за правното основание и целите на обработването, получателите на данните и за категориите обработвани лични данни. Освен това, те следва да предоставят всякаква допълнителна информация, която е необходима, за да се гарантира добросъвестно и прозрачно обработване. Администраторът е освободен от задължението да предоставя

такава информация, когато обработването изрично е предвидено от закона или това е невъзможно или изисква несъразмерни усилия.

Права на субекта на данни (чл. 9)

На субектите на данни се дават нови права, така че да имат по-голям контрол върху своите данни в дигиталната ера.

Модернизираната Конвенция допълва списъка с информацията, която се предава на субектите на данни, когато упражняват правото си на достъп. Освен това, субектите на данни имат право да узнаят причините за обработването на данни, резултатите от което се прилагат спрямо тях. Това ново право е особено важно от гледна точка на профилирането на физически лица.[222]

То следва да бъде свързано с друга новост, а именно правото да не подлежи на решение, което засяга субекта на данните и, което е базирано изключително на автоматизирано обработване, без да са взети предвид вижданията на субекта на данни.

Субектите на данни имат право да възразят във всеки един момент срещу обработването на личните им данни, освен ако администраторът покаже убедителни законни основания за обработването, които са над техните интереси или права и основни свободи.

Допълнителни задължения (чл. 10)

Осъвременената Конвенция налага по-широки задължения на лицата, които обработват данни или от името на които се обработват данни.

Отчетността става неразделна част от системата за защита, като задължение е на администраторите да бъдат в състояние да докажат спазване на правилата за защита на данните.

Администраторите следва да предприемат всички подходящи мерки – включително когато обработването е възложено на външни изпълнители – за да гарантират, че е обезпечено правото на защита на данните (неприкосновеност на етапа на проектирането, преглед на вероятното въздействие на планираното обработване на данни върху правата и основните свободи на субектите на данни („оценка на въздействието върху неприкосновеността на личните данни") неприкосновеност на етапа на проектирането).

Изключения и ограничения (чл. 11)

Правата, предвидени в Конвенцията, не са абсолютни и могат да бъдат ограничени, когато това е предвидено по закон и представлява необходима мярка в демократичното общество въз основа на конкретни и ограничени основания. Сред тези ограничени основания сега са включени „важни цели от обществен интерес", както и препращане към правото на свобода на изразяване.

Списъкът с разпоредби на Конвенцията, които могат да бъдат ограничени, е леко разширен (вж. препращания към членове 7.1 за сигурността и 8.1 за прозрачност в Чл. 11.1) и нов параграф от този член специално урежда дейностите по обработване за целите на националната сигурност и отбраната, за които могат да бъдат ограничени правомощията за „наблюдение" на Комитета, както и някои

222 По тази тема, вж. Препоръка (2010)13 за защита на лицата при автоматизирана обработка на лични данни в контекста на профилиране и нейния Обяснителен меморандум. (оригинална бележка под линия)

мисии на надзорните органи. Изискването дейностите по обработване за целите на националната сигурност и отбраната да подлежат на независим и ефективен преглед и надзор е ясно предвидено.

Важно е да се припомни още веднъж, че – противно на предходните разпоредби на Конвенция 108, Страните по осъвременената Конвенция вече няма да могат да изключват от приложното поле на Конвенцията определени видове обработване.

Трансгранични потоци лични данни (чл. 14)[223]

Целта на тази разпоредба е да улесни, където е приложимо, свободния поток от информация, независимо от границите, като същевременно гарантира подходяща защита на лицата по отношение на обработването на личните им данни.

При липсата на хармонизирани правила за защита, споделяни от държавите, принадлежащи към регионална международна организация и управляващи потоци от данни (вж. например уредбата на защитата на данните на Европейския съюз), потоците данни между Страните следва да се движат свободно.

Що се отнася до трансграничните потоци от данни към получател, който не попада под юрисдикцията на дадена Страна, трябва да бъде гарантирано надлежно ниво на защита в Държавата или организацията на получателя. Тъй като това не може се предположи, след като получателят не е Страна, Конвенцията установява два основни начина, по които да гарантира, че нивото на защита на данните е наистина подходящо; по закон или чрез ad hoc или одобрени стандартизирани предпазни мерки, които са законно обвързващи и подлежат на принудително изпълнение (по-специално договорни клаузи или обвързващи корпоративни правила), както и са надлежно приложени.

Надзорни органи (чл. 15)

Съгласно чл. 1 от допълнителния протокол, модернизираната Конвенция допълва списъка с правомощията на властите с разпоредба, според която, в допълнение към правомощията им да се намесват, да разследват, да се ангажират в съдебни производства или да свеждат до вниманието на съдебните органи нарушения на разпоредбите за защита на данните, властите имат и задължение да повишават осведомеността, да предоставят информация и да образоват всички засегнати участници (субекти на данни, администратори, обработващи лични данни и т.н.). Освен това, тя позволява на властите да вземат решения и да налагат санкции. Припомня се, още, че надзорните органи следва да бъдат независими при упражняването на тези задължения и правомощия.

Форми на сътрудничество (чл. 17)

Модернизираната Конвенция урежда и въпроса за сътрудничеството (и взаимопомощта) между надзорните органи.

Надзорните органи трябва да координират своите разследвания, да провеждат съвместни действия и да си предоставят взаимно информация и документация за тяхното законодателство и административни практики във връзка със защитата на данните.

[223] В това отношение, Осъвременената Конвенция се базира на Допълнителния протокол и правилата на ЕС.

Обменът на информация между надзорните органи ще включва лични данни, само когато тези данни са от съществено значение за сътрудничеството или когато субектът на данни е дал изрично, свободно и информирано съгласие.

Накрая, Конвенцията предвижда форум за засилено сътрудничество: надзорните органи на Страните трябва да формират мрежа, за да организират своето сътрудничество и за да изпълняват задълженията си, посочени от Конвенцията.

Комитет по Конвенцията (членове 22, 23 и 24)

Комитетът по Конвенцията има съществена роля при тълкуването на Конвенцията, насърчаването на обмена на информация между Страните и разработването на стандарти за защита на данните.

Ролята и правомощията на този Комитет се засилват с Модернизираната Конвенция. Те вече не са ограничени до „консултативна" роля, но включват и правомощия по оценка и наблюдение. [*Освен че предоставя*] становище[*а*] относно нивото на защита на данните, осигурявано от дадена държава [*както преди, сега ще прави това и по отношение на*] международна[*и*] организация[*и*] преди присъединяването им към Конвенцията. Комитетът [*сега*] има възможността и да оценява съответствието на националното законодателство на съответната Страна и да определя ефективността на предприетите мерки (съществуване на надзорен орган, отговорности, съществуване на ефективни правни средства за защита).

Също така е в състояние да прецени дали правните норми, регулиращи трансфера на данни, предоставят достатъчна гаранция за подходящо ниво на защита на данните.Не е тук мястото да се анализират подробно тези новости. Достатъчно е да се отбележи, че **те приближават новият, „осъвременен" режим по Конвенция до новия режим, установен за ЕС по ОРЗД**. Това означава, че когато ЕС оценява „адекватността" на нивото на защита на данните в трета държава (както се разглежда в Част втора, раздел 2.1), фактът, че тази трета държава е страна по Модернизираната Конвенция би бил основен въпрос, който следва да бъде взет под внимание.

Действително, от гледна точка на **приложното поле**, Модернизираната Конвенция излиза извън обхвата на ОРЗД, доколкото, както е много ясно показано и в текста на Модернизираната Конвенция и в горния обзор, държавите страни по нея няма да могат вече да изключват никакви видове обработване от своите задължения – като ***национална сигурност*** и ***отбрана***, които са въпроси извън приложното поле на инструментите на ЕС в областта на защитата на данните.[224]

Дали в други отношения Осъвременената Модернизираната Конвенция – или, по-точно, националните закони на Държавите страни по нея, които прилагат тази Конвенция – винаги ще бъде в пълно съответствие с ОРЗД – , както ще бъде тълкуван и прилаган в бъдеще от Европейския комитет по защита на данните на ЕС, органите по

[224] Вж. раздел 1.3.1, по-горе, в точката „*Естество и ограничения на директивите на ЕО*", що се отнася до това ограничение във връзка с директивите на ЕО за защита на данните от 1995 г. и 2002 г., и Част Втора, раздел 2.1, по-долу, що се отнася до ОРЗД. Във връзка с обработването за целите на правоприлагането (и т.н.), и обработването от самите институции на ЕС, ЕС, разбира се, има въведени правила, които по същество са в съответствие със стандартите на ОРЗД (и – по този начин – с Осъвременената конвенция) (или във връзка с институциите на ЕС – ще има след като те бъдат приведени в съответствие с ОРЗД).

защита на данните на държавите членки на ЕС, Европейската комисия и Съда на ЕС – е разбира се нещо, кото предстои да видим.

Например, новите правила за трансграничните потоци от данни в Модернизираната Конвенция позволяват трансфери в трети държави, които осигуряват „***подходящо***" ниво на защита (чл. 14) – което, на пръв поглед, може да изглежда подобно на изискването за „***адекватно***" ниво на защита в ОРЗД (както и по Директивата за защита на данните от 1995 г.) – но не е гарантирано, че новият Комитет по Конвенцията ще следва Съда на ЕС, като счита, че терминът „подходящо" следва да се тълкува в смисъл, че въпросната трета държава трябва да предостави „***по същество равностойна/еквивалентна/***" защита (както постановява Съдът на ЕС при тълкуването на термина „адекватно").[225]

В други отношения, напр. що се отнася до **съгласие от деца**, Модернизираната Конвенция не е толкова подробна или конкретна, колкото ОРЗД.

Но като оставим тези въпроси настрана, е ясно, че между тях, Съветът на Европа Европейският съюз са водещи в определянето на глобалните „златни стандарти" за защита на данните – както приложимите в рамките на държавите, така и по отношение на транснационални потоци от данни.

Накрая, следва да бъде отбелязано, че Модернизираната Конвенция (за разлика от предшестващата я) е отворена за присъединяване от международни организации – и поради това ЕС също може официално да се присъедини към нея.

- o – O – o -

[225] Съд на ЕС, решение по *Schrems* (бележка под линия 70, по-горе), параграф 73.

ЧАСТ ДВЕ

Общият регламент относно защитата на данните

2.1 Въведение

Както вече е отбелязано в 1.4.1, по-горе, Общият регламент относно защитата на данните (ОРЗД или „Регламентът") бе приет отчасти защото Директивата за защита на данните от 1995 г. не доведе до достатъчно ниво на хармонизация на законите в държавите членки; отчасти в отговор на масираното разрастване на дейността по обработване на лични данни след въвеждането на Директивата за защита на данните от 1995 г.; и отчасти в отговор на съдебната практика на Съда на ЕС. Остава да се види дали той ще бъде достатъчен да се справи изцяло с развитието на все по-натрапчиви технологии, като „Големи масиви от данни" (Big Data), „Интернет на нещата" (Internet of Things), алгоритмично вземане на решения и използването на изкуствен интелект.

Регламентът се основава на Директивата от 1995 г. за защита на данните, но значително я допълва и, при това, значително затяга основния режим на ЕС за защита на данните. Той води до *по-голяма хармонизация*, *засилени права на субектите на данни права*, *по-тясно сътрудничество между органите по защита на данните*, *по-големи правомощия за изпълнение*и още.

Приложение 1 към този наръчник съдържа *Индекс на главите, разделите и членовете на ОРЗД*, за лесна справка. Приложение 2 предоставя пълния текст на Регламента, както е публикуван в Официалния вестник на ЕС, включително съображенията.

Раздел 3.2 разяснява статута и подхода на ОРЗД и разглежда с определена степен на детайл последиците от факта, че той съдържа много клаузи, позволяващи доразвиване на уредбата на национално равнище (като по този начин в известна степен възпрепятства целта за по-пълна хармонизация).

Раздел 3.3 предоставя преглед по глави, раздели и членове на ОРЗД.

След това се обръщаме към двата основни въпроса за длъжностните лица по защита на данните: новия принцип на „отчетност" (задължение да се докаже съответствие) (раздел 3.4) и правилата за назначаването, набирането, условията и задълженията (и т.н.) на длъжностното лице по защита на данните (раздел 3.5), и обясняваме връзката между тези две неща.

2.2 Статут и подход на ОРЗД: пряка приложимост с "уточняващи разпоредби"

Регламент …

ОРЗД е **Регламент,**което означава правен акт на ЕС, който е ***пряко приложим*** в правния ред на държавите-членки на ЕС (и държавите от ЕИП извън ЕС) без да има нужда да бъде транспониран в националното законодателство, какъвто е случаят с директивите като Директивата за защита на данните от 1995 г.

Европейският законодател е избрал този начин, именно защото имплементирането на директивата от 1995 г. беше неравномерно: тя беше транспонирана различно в различните държави членки, което доведе до липсата на хармонизация.[226]

[227] През годините Европейската Комисия оценява транспонирането на Директивата от 1995г. противоречиво в различните държави членки. На теория, регламентът, бидейки пряко приложим, следва да води до **пълна хармонизация** на правото в областта, която попада в приложното му поле. В случая на ОРЗД, това е подкрепено от много по-засилените договорености за **споделяне на информация и сътрудничество** между регулаторите (националните надзорни органи или органи по защита на данните, ОЗД) и специален **механизъм за „съгласуваност"**, който е разгледан по-долу в тази точка.

Както обаче е показано в следващата подточка, в същото време ОРЗД все пак оставя много въпроси за доуреждане в националните закони на държавите членки на ЕС според тяхната нормативна или институционална система. Това би могло, , да възпрепятства пълната хармонизация, която ще обсъдим в точките „*Изисквания на уточняващите разпоредби*" и „*Сътрудничество и съгласуваност*". Има и граници на свободата на държавите членки в това отношение, и нови начини за надзор на ниво ЕС, за упражняване на тази „гъвкавост" (поне на теория).

… но с „уточняващи разпоредби"

Макар Регламентът да се стреми към по- голяма хармонизация, той все пак съдържа редица „гъвкави" разпоредби, наричани от Комисията „уточняващи разпоредби", които отстъпват пред националното законодателство на държавите членки особено в публичниясектор, но засягащи и задължения, наложени от националното законодателство на дружествата, попадащи в юрисдикцията на съответната държава членка (напр., съгласно трудовото право, или правилата за правоприлагане /) и по отношение на създаването на орган по защита на данните.

Типове „уточняващи разпоредби"

Италианският орган по защита на данните, *Garante della Privacy*, е установил четири различни (макар и донякъде припокриващи се) видове клаузи, които оставят място за по-нататъшно регулиране чрез законодателството на държавите членки:[228]

- **Допълнителни уточнения**

  Това са разпоредби, съгласно които държавата членка може да подържа или да въведе „по-конкретни *разпоредби, за да адаптира прилагането*" на съответната разпоредба в Регламента (за целта се използват различни фрази).

Примери:

[226] Това е заключението, направено в изследване, възложено от ЕС, от Дау Корф за Университета на Есекс, Report on an EU study on the implementation of the [1995] data protection directive (Доклад от изследване на ЕС за имплементирането на директивата за защита на данните [от 1995 г.]), 2002, което може да бъде намерено на:
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1287667 –
но ЕС се нуждаеше от още 10 години, за да се обърне внимание на това, предлагайки регламент.

[227] Вж.

[228] Антонио Касели, презентация пред първата обучителна сесия по „T4DATA", юни 2018 г., относно „*ОРЗД и националните правила*". Същината на тази презентация е описана и подробно разгледана в Приложение 4 към наръчника (в том Втори), където са дадени и още примери.

Държавите членки могат да уточнят кои дейности по обработване изискват ***предварително разрешение***, или да регулират използването на ***национални идентификационни номера***, или обработването на ***лични данни на служители***.

Държавите членки могат да *„запазят или да въведат **допълнителни условия, включително и ограничения**, по отношение на обработването на **генетични данни**, **биометрични данни** или **данни за здравословното състояние***", над условията и ограниченията, наложени от самия ОРЗД в член 9, параграфи 1 – 3 (членът, уреждащ „специални категории лични данни", обичайно наричани „чувствителни данни") (чл. 9, пар. 4). По този начин те могат, например, да предвидят, че винаги се изисква ***предварително съгласие*** за обработването на **генетични данни**.

- **Възможности и избори**

В някои отношения, ОРЗД позволява на държавите членки, чрез тяхното национално законодателство, да **изберат** определени възможности , които са конкретно посочени в него, или да разширят приложението на задължение или забрана, които съгласно Регламента се прилагат само в определени случаи, спрямо други случаи.

Например, държавите членки може да позволяват на ***деца*** на възраст над 13, 14 или 15 г. да се ***съгласят с определени информационни услуги***, вместо едва от 16-годишна възраст, както е предвидено в ОРЗД; или може да изискват ***назначаването на длъжностно лице по защита на данните***, когато Регламентът не предвижда такова изискване.

- **Ограничения и дерогации**

При спазването на определени доста широкообхватни **условия** (разгледани по-долу, под точките *„Изисквания на „уточняващите разпоредби"" и „Проблеми, свързани с* тях), чл. 23 от ОРЗД позволява радикални **ограничения** на всички права на субектите на данни във връзка с определени **важни цели от обществен интерес**: като ***национална сигурност***, ***отбрана***, ***обществена сигурност***, ***правоприлагане*** и ***съдебна независимост*** – но също така ***защита на икономическите или финансовите интереси на държавата***, прилагането на ***професионална етика***, както и всеки вид *„**функция по наблюдението, проверката или регламентирането***, свързана, дори само понякога, с упражняването на официални правомощия" в някакъв аспект на основния защитен интерес, в това число и "***защитата на субекта на данните или на правата и свободите на други лица***", както и ***принудителното изпълнение по граждански искове***.

Членове 85, 86 и 89 от ОРЗД съдържат разпоредби, които , от една страна, позволяват (а в някои отношения, изискват) **дерогации** от определени правила в Регламента, за да се защити **свободата на изразяване**, като позволяват **свобода на информацията** (достъп до документи и информация, съхранявани от публични органи) и **архивиране**, и улесняват **проучванията** (в обществена полза), докато от друга страна, налагат определени **условия** за тези дерогации (както е

и по-нататък разгледано в точки „*Изисквания на „уточняващите разпоредби“*“ и „*Проблеми, свързани с „уточняващите разпоредби“*“, по-долу).

Бележка: Някои от тези специални правила служат за защита на интересите на „другите”, докато други могат да се разглеждат като съществуващи в общ или обществен интерес, а някои, като свободата на информация, могат да служат и за двете. Това са въпроси, в областта на които правилата досега не са били хармонизирани, макар че в някои държави членки на ЕС и защитата на данните, и свободата на информацията са предоставени на едни и същи органи. Като се има предвид, че тези въпроси се превръщат във все по-транснационални – напр., трансграничните искания за достъп до публични данни; въпросите относно свобода на изразяване в опозицияс въпросите за защита на данните и неприкосновеността на личния живот, свързани с онлайн публикации; и международни медицински изследвания –очаква се, че Европейският комитет по защита на данните ще издаде допълнителни насоки по тези въпроси, по-специално във връзка с транснационалните дейности. Комисията също може да изготвя нови предложения по тези въпроси.

Регулаторни задължения

В някои отношения, различни от отбелязаните по-горе – по-специално, във връзка със създаването на независими надзорни органи (органи по защита на данните, ОЗД), и създаването на системи за сертифициране – ОРЗД **изисква** държавите членки да приемат подробни правила и уредби, прилагащи съответните изисквания за органите по защита на данните в тяхното национално законодателство. Това са до голяма степен технически въпроси (макар че, освен това, изискват спазването на важни стандарти, напр., за независимост и предоставяне на достатъчни ресурси).

Изисквания на „уточняващите разпоредби”

В много отношения, включително посочените в точките „*допълнителни уточнения*” и „*възможности и избори*” по-горе, но по-специално отбелязаните в точка „*ограничения и дерогации*”, ОРЗД **изисква** от държавите членки да приемат правни норми за уреждане на съответните въпроси, ***които отговарят на определени демократични, свързани с правата на човека, стандарти***.

Други разпоредби (които не са включени в тези точки) също **посочват необходимостта от регулиране** , изисквайки от държавите членки да приемат „***подходящи гаранции***” („***appropriate safeguards***”, “***suitable safeguards***”) или „***адекватни мерки***”. Тъй като самият ОРЗД често не пояснява какви могат да бъдат тези гаранции или мерки, държавите членки ще трябва да изяснят това в своите национални законодателства, които отново ще трябва да отговарят на определени ***демократични стандарти*** или върховенство на закона.

Важно е да се отбележи, че **освен това, на държавите членки не просто се дава пълно право на преценка** – както става ясно от изискванията, определени мерки или гаранции трябва да бъдат **„подходящи”**. В други отношения, определени **общо-приложими стандарти** и условия на върховенството на закона са изрично формулирани в ОРЗД , но всъщност, подобни стандарти и условия се прилагат спрямо всички съответни разпоредби..

По този начин, ОРЗД изрично предвижда, че по принцип широките дерогации, позволени по чл. 23 (обобщени по-горе в точка „*Ограничения и дерогации*”) трябва да

бъдат изложени в конкретен **закон** („***законодателна мярка***"), който трябва да „***е съобразен със същността на основните права и свободи*** *и [да] представлява* ***необходима и пропорционална*** *мярка в едно демократично общество с цел да се гарантира*" съответния интерес. Тези изисквания са преки отражения на изискванията, на които трябва да отговаря което и да е ограничение на някое от основните права, защитени от Европейската конвенция за правата на човека (ЕКПЧ) и Хартата на основните права на ЕС (Хартата). По-долу предлагаме цитат от последната:

> Всяко ограничаване на упражняването на правата и свободите, признати от настоящата Харта, трябва да бъде предвидено в закон и **да зачита** основното съдържание на същите права и свободи. При спазване на принципа на **пропорционалност,** ограничения могат да бъдат налагани, само ако са **необходими** и ако **действително отговарят на** признати от Съюза **цели от общ интерес** или **на необходимостта да се защитят правата и свободите на други хора**.
>
> (член 52, параграф 1, добавено удебеляване)

Тъй като всеки закон на държава членка, който ограничава които и да е права на субект на данни, по която и да е от „ уточняващите разпоредби" в ОРЗД, трябва да се разглежда като представляващ ограничение на правото на защита на данните, гарантирано от Хартата на основните права (чл. 8), всеки от тях трябва да покрива горепосочените критерии .

По-специално, съгласно Европейската конвенция за правата на човека и Хартата на основните права, и – по този начин – съгласно ОРЗД, съответният закон трябва да отговаря на определени съществени **изисквания за „качество"**: нормите в закона трябва да бъдат „**съвместими с върховенството на закона**" (което означава по-специално, че те не могат да бъдат ***дискриминационни*** или ***произволни***, и трябва да ***могат да бъдат оспорвани*** и да са предмет на ***ефективни правни средства за защита***) и, по-специално, **достъпни** (т.е., ***публикувани***) и достатъчно **ясни** и **точни**, за да бъдат „***предвидими***" при неговото (и тяхното) приложение.[229]

Позоваването към „зачитане [на] същността " на въпросните права и свободи трябва да се чете като **забраняващо всяка правна норма, която така дълбоко засяга дадено право, че го лишава от стойност**. Например, Съдът на ЕС е постановил, че:[230]

> правна уредба, осигуряваща общ достъп на публичните органи до съдържанието на електронни съобщения, трябва да се счита за засягаща съществената съдържание на основното право на зачитане на личния живот, гарантирано с чл. 7 от Хартата …

Поради това дерогациите на държавите членки по-специално по член 23 от ОРЗД– включително дерогации от правилата за защита на данните, за да се защитят

---

[229] Вж.: Harris, O'Boyle & Warbrick, Law of the European Convention on Human Rights, 2nd ed. (Харис, О'Бойл и Уорбрик, Право на европейската конвенция за правата на човека, 2ро издание), 2009 г., Глава 8, раздел 3, *Limitations (Ограничения)*. За обикновен обзор на съответните изисквания на ЕКПЧ, вж.: Douwe Korff, The standard approach under articles 8 – 11 ECHR and article 2 ECHR (Дау Корф, Стандартният подход по членове 8 – 11 от ЕКПЧ и член 2 от ЕКПЧ) (обучителен материал), може да се намери на: https://www.pravo.unizg.hr/_download/repository/KORFF_-_STANDARD_APPROACH_ARTS_8-11_ART2.pdf Вж. по-специално текста под въпроси 3 (Право) и 5 (Необходими и пропорционални) в този материал.

[230] Съд на ЕС, решение по *Schrems* (бележка под линия/под черта/ 70, по-горе), парагрф 94.

националната сигурност и отбраната –никога не са равнозначни на такива неоправдани и неприемливи прекомерни дерогации от основните правила.

По-специално, всякакви дерогации по чл. 23 и всякакви други отклонения, от което и да е от нормалните правила в ОРЗД, по която и да е от „ уточняващите разпоредби“, трябва да отговарят на изискването да са „**необходим[и] пропорционалн[и] в едно демократично общество**”. Това означава, че всяко отклонение от нормалните правила или ограничение, на което и да е неабсолютно право на субектите на данни, базирано на „уточняваща разпоредба“, трябва да бъде реално в изпълнение на изискваната „***легитимна цел***”/“***важна цел от обществен интерес***”, да отговаря на „***належаща обществена необходимост***”, и да е „***разумно пропорционална***” на тази нужда. Съдейки какво точно е необходимо в това отношение, държавите могат да получат определена „***свобода на преценка***”[231] – но тази свобода е ограничена от изискването мярката (дерогацията или ограничението) да е необходима „***в едно демократично общество*** ”.

Най-общо казано , ако има **ясна насока** по даден въпрос – каквато е предоставена в Директивата за защита на данните от 1995 г. от Работната група по член 29 и Европейският надзорен орган по защита на данните, а сега се предоставя и по ОРЗД от Европейския комитет по защита на данните (който включва Европейския надзорен орган по защита на данните) – и/или ако има **забележимо доближаване на мненията** по въпроса между държавите членки (или органите по защита на данните на държавите членки), тогава всяко отклонение от тази насока или консенсус от страна на една държава членка е вероятно да покаже че отклоняващите се мерки (дерогации или ограничения, които превишават онова, което се счита за необходимо или пропорционално в други държави членки) не е „необходимо” или „пропорционално” „в едно демократично общество”.

Както обаче е отбелязано в следващата точка, тези въпроси не могат да бъдат разрешени чрез „механизми за сътрудничество и съгласуваност” (разгледано отделно, по-късно).

Проблеми, свързани с „уточняващите разпоредби“

Спряхме се на „ уточняващитеразпоредби“ по-задълбочено, тъй като предизвикат проблеми при ефективното приложение на ОРЗД. Тези проблеми се проявяват в две форми.

Преди всичко, „уточняващитеразпоредби“ ще доведат, с оглед на своя характер, до **различни (или в по-голяма или по-малка степен подробни) правила, отразяващи националните особености, по отношение на идентични въпроси в различните**

[231] Доктрината за „свобода на преценка” (margin of appreciation), която е силно застъпена в съдебната практика на Европейския съд по правата на човека, е по-неяно изразена от Съда на ЕС, който, може да се каже, че предпочита да говори за „преценка” (discretion) или „свобода на преценка” (margin of discretion), предоставена на държавите членки по определени въпроси. За целите на настоящия наръчник обаче, доктрината може да бъде наричана по начините, по които е отразена в практиката и на съда в Страсбург и на съда в Люксембург, дори ако има някаква различна степен от контекста. Вж.: Francisco Javier Mena Parras, From Strasbourg to Luxembourg? Transposing the свобода на преценка concept into EU law (Франсиско Хавиер Мена Парас, От Страсбург до Люксмебург? Транспониране на концепцията за свобода на преценката в правото на ЕС), Брюксел, 2008 г., може да се намери на: http://www.philodroit.be/IMG/pdf/fm_transposing_the_margin_of_appreciation_concept_into_eu_law_-_2015-7.pdf

държави членки. Това не представлява такъв проблем във връзка с обработването, което се случва изцяло в рамките на една държава членка, и което е свързано само със субекти на данни в тази държава членка. Въпреки това, както беше отбелязано по-рано, в 21 век все повече държавни дейности имат международно отражение и включват трансгранични дейности по обработване на лични данни, както и в публичния сектор, и не само във връзка с правоприлагане или граници. Това важи в особена степен за ЕС заради „четирите свободи", които са основни за европейския проект: свободата на движение на стоки, услуги, хора и капитали .

Когато стоките или услугите се предлагат и закупуват зад граница, в рамките на ЕС или извън него, личните данни следват (и са от съществено значение за) сделките. Както хората се придвижват, така и техните данни се движат свободно: данните им за данъци, социални и пенсионни плащания, техните медицински данни, семеен статут , раждания, развод, смърт и местопребиваване. Когато се извършват плащания (между физически лица, или между физически лица и частни лица, или между физически лица и държавни агенции, независимо дали е данъчната служба, службата по местопребиваване или пенсионната служба), това води до потоци от техни финансови задължения и други данни. Такъв е случаят *a fortiori* (на по-силно основание), когато обработването или част от обработването се случва онлайн.

Когато, при такива обстоятелства, има различни правила в различните държави членки по отношение на въпросното обработване на данните, това поражда потенциални (и потенциално сериозни)правни проблеми, които ще трабва да бъдат решавани конкретно случай по случай (което често няма да е лесно). Следните примери илюстрират това във връзка с някои от специфичните дерогации и ограничения, които може да бъдат въведени съгласно „ уточняващите разпоредби", посочени по-рано:

Примери:

- Ако една държава членка наложи ограничения върху използването на националния идентификационен номер, които не са наложени в друга държава членка, трябва ли тези ограничения да се спазват от получател във втората държава членка (включително получател от обществения сектор),ако данните са прехвърлени за този получател ?

- Ако една държава членка наложи „допълнителни условия" или допълнителни „ограничения" на обработването на всички или някои видове чувствителни данни (напр., при използването на биометрични или генетични данни), които не са наложени в друга държава членка, дали тези условия или ограничения все пак трябва да бъдат спазвани от получателя във втората държава членка (включително получател от публичния сектор), ако данните бъдат прехвърлени на същия ?
- Ако една държава членка определи възраст за съгласие с използването на информационни услуги за деца, да кажем, над 14 години, а друга държава членка я остави на предложената от ОРЗД - 16-годишна възраст, може ли доставчик на информационни услуги в първата държава членка да предоставя своята услуга на дете на възраст над 14 години във втората държава членка, на база на съгласието на 14-годишното лице? Следва ли доставчикът да направи

разграничение на база IP адрес на детето (въпреки че той може да бъде лесно „подменен ” с VPN дори от 14-годишни)?

- Ако една държава членка изисква получаването на предварително разрешение от органа по защита на данните за обработване във връзка със социална закрила и обществено здраве, но друга държава членка не предвижда такова изискване, може ли публичен орган във втората държава членка да обработва лични данни във връзка със субекти на данни в първата държава членка за тези цели без такова предварително разрешение – както лесно би се случило във връзка с деца на мигранти, които напускат своя партньор и деца в родната си държава докато работят в друга държава членка, като обаче на родителят в родината се плащат помощи за деца и т.н.? (БЕЛЕЖКА: В контекста на предоставянето на такова предварително разрешение, съответният орган по защита на данните вероятно ще наложи или ще изиска налагането на определени гаранции и ограничения. Трябва ли държавната агенция в другата държава членка също да ги спазва? Ще бъде ли наясно изобщо агенцията за тях?)

Горепосочените проблеми са сериозно утежнени от **липсата в ОРЗД на разпоредба за „приложимото право”** по модела на съдържащата се в Директивата за защита на данните от 1995 г. (въпреки че тази разпоредба, в чл. 4, повдигна въпроси по отношение на езиковия превод и ефективността).[232] Може да се предположи, че такава разпоредба е оставена извън ОРЗД, тъй като е прието, че, като Регламент, той би бил прилаган по един напълно хармонизиран начин – но както е посочено по-горе, в (многобройните) области, обхванати от „уточняващитеразпоредби“ (които ще бъдат разгледани на национално равнище в конкретни закони), това е малко вероятно .

Вторият проблем е свързан със **спазването на изискванията на върховенството на закона**, изложени в предишната подточка. Има вероятност да възникнат въпроси дали определени закони в определени държави членки, които ограничават някои права или облекчават определени правила, отговарят на този критерий, т.е. дали те са достатъчно достъпни, конкретнии предвидими при тяхното прилагане, необходими или пропорционални за съответната (легитимна/важна) цел.

Тези проблеми често не могат да бъдат разрешени или дори да им бъде обърнато внимание според „механизмите за сътрудничество и съгласуваност”, обсъдени по-късно, тъй като тези механизми са ограничени до сътрудничество във връзка с мерки, които са взети или предприети или предложени за предприемане от органите по защита на данните: те не могат да бъдат използвани за отстраняване на недостатъци в законите на държавите членки. Това може да създаде сериозни проблеми, по-специално във връзка с прехвърлянето на лични данни от държавна агенция в една държава членка на ЕС на държавна агенция в друга държава членка, ако във втората държава данните ще бъдат обработвани съгласно закони, за които с основание може да се каже, че не отговарят на изискванията на върховенството на закона. Въпреки това, опитът в други области (като правилата в областта на правосъдието и вътрешните работи, необсъждани в това първо издание на наръчника) показва, че когато е необходимо,

[232] Вж. Douwe Korff, *The question of “applicable law”*, in: Compliance Guide 3 – Interim report, Privacy Laws & Business (Дау Корф, *Въпросът за „приложимото право”*, в: Ръководство за съответствие 3 – Междинен доклад, Прайваси Лоус & Бизнес), ноември 1999 г.

може да бъде предприето действие за справяне с тези проблеми, особено на база на предложенията на Комисията или на Европейския комитет по защита на данните.

Отражение върху длъжностните лица по защита на данните

От горепосоченото следва да стане ясно , че длъжностните лица по защита на данните би следвало да са запознати с, и да **разглеждат, не само правилата в ОРЗД, но и които и да е относими национални правила, стъпващи на „уточняващите правила в Регламента** – и до известна степен съответните закони и правила в други държави членки и в трети държави, ако организация, в която работят, разкрива лични данни на тези други държави.

Това може да се отнася до различни ситуации . В някои случаи, държавите членки могат просто да са запазили правила, съществували вече преди влизането в сила на ОРЗД, включително специални дерогации, за да защитят важни публични интереси, или за да улеснят изследване, макар че **те може не винаги да отговарят на изискванията на върховенството на закона над съответните „уточняващиразпоредби" или да са „подходящи („appropriate" или „suitable") от гледна точка на ОРЗД** (както е обсъдено по-горе). В други случаи, тяхната държава членка може да е приела конкретни закони или нормативни правила за „доуреждане" на въпроси, които са оставени на държавата членка съгласно ОРЗД, или с цел разяснение на това кои възможности са използвани и т.н. А в други случаи, държавата членка може все още да не е изяснила националното приложениена релевантните правила изобщо.

Разбира се, длъжностните лица по защита на данните не могат сами да отстраняват каквито и да е било недостатъци или проблеми в тези аспекти. В рамките обаче на техните собствени мрежи от длъжностни лица по защита на данните и в техните взаимодействия с националните им органи по защита на данните,[233] те могат да **привличат внимание към такива проблеми и да насърчават предприемането на подходящо действие**. Също така те следва – отново, за предпочитане, заедно с други длъжностни лица по защита на данните, работещи в подобни организации – **да подават сигнали до ръководството на собствените си организации** (в публичния сектор, например, съответния(те) правителствен(и) министър(и)) за установени такива недостатъци. В такива ситуации длъжностните лица по защита на данните трябва да разработят стратегически ефективни подходи за справяне със ситуацията.

2.3 Преглед на ОРЗД

По-долу се съдържа обширен преглед на ОРЗД, глава по глава и раздел по раздел.*

*

2018 ОБЩ РЕГЛАМЕНТ ОТНОСНО ЗАЩИТАТА НА ДАННИТЕ:
Глава I: **Общи разпоредби (Членове 1 – 4):** - Предмет и цели на Регламентът; - Материален обхват;

[233] Вж. „Extranet" на **Френския** ОЗД, което може да бъде полезно в такива контексти. Вж. бележка под линия 228, по-долу.

- Териториален обхват; - Определения.
<u>Глава II</u>: **Принципи (членове 5 – 11):** - Принципи, свързани с обработването на лични данни; - Законосъобразност на обработването [законни основания]; - Условия за даване на съгласие; - Условия, приложими за съгласието на дете във връзка с услугите на информационното общество; - Обработване на специални категории лични данни [чувствителни данни]; - Обработване на лични данни, свързани с присъди и нарушения; - Обработване, за което не се изисква идентифициране.
<u>Глава III</u>: **Права на субекта на данни**
Раздел 1 (член 12): **Прозрачност и условия:** - Прозрачна информация, комуникация и условия за упражняването на правата на субекта на данни.
Раздел 2 (членове 13 – 15): **Информация и достъп до лични данни:** - Информация, предоставяна при събиране на лични данни от субекта на данните; - Информация, предоставяна, когато личните данни не идват от субекта на данните; - Право на достъп на субекта на данните.
Раздел 3 (членове 16 – 20): **Коригиране и изтриване:** - Право на коригиране - Право на изтриване (Право на ограничаване на обработването „право да бъдеш забравен”) - Право на ограничаване на обработването [„блокиране”] - Задължение за уведомяване при коригиране или изтриване на лични данни или ограничаване на обработването - Право на преносимост на данните
Раздел 4 (членове 21 – 22): **Право на възражение и автоматизирано вземане на индивидуални решения:** - Право на възражение; - Автоматизирано вземане на индивидуални решения, включително профилиране.
Раздел 5 (Член 23): **Ограничения**
<u>ГЛАВА IV</u>:

Администратор и обработващ лични данни

Раздел 1 (членове 24 – 31):

Общи задължения:

- Отговорност на администратора;
- Защита на данните на етапа на проектирането и по подразбиране;
- Съвместни администратори;
- Представители на администратори и обработващи лични данни, които не са установени в Съюза;
- Обработващ лични данни;
- Обработване под ръководството на администратора или обработващия лични данни;
- Регистри на дейностите по обработване;
- Сътрудничество с надзорния орган.

Раздел 2 (членове 32 – 34):

Сигурност на личните данни:

- Сигурност на обработването;
- Уведомяване на надзорния орган за нарушение на сигурността на личните данни;
- Съобщаване на субекта на данните за нарушение на сигурността на личните данни.

Раздел 3 (членове 35 – 36):

Оценка на въздействието върху защитата на данните и предварителни консултации:

- Оценка на въздействието върху защитата на данните;
- Предварителна консултация.

Раздел 4 (членове 37 – 39):

Длъжностно лице по защита на данните:

- Определяне на длъжностното лице по защита на данните;
- Длъжност на длъжностното лице по защита на данните;
- Задачи на длъжностното лице по защита на данните.

Раздел 5 (членове 40 – 43):

Кодекси за поведение и сертифициране:

- Кодекси за поведение;
- Наблюдение на одобрените кодекси за поведение;
- Сертифициране;
- Сертифициращи органи.

ГЛАВА V (членове 44 – 50):

Предаване на лични данни на трети държави или международни организации:

- Общ принцип на предаването на данни;
- Предаване на данни въз основа на решение относно адекватното ниво на защита;
- Предаване на данни с подходящи гаранции;
- Задължителни фирмени правила;
- Предаване или разкриване на данни, което не е разрешено от правото на Съюза;
- Дерогации в особени случаи;
- Международно сътрудничество за защита на личните данни.

ГЛАВА VI: **Независими надзорни органи:**
Раздел 1 (членове 51 – 54): **Независим статут:** - Надзорен орган; - Независимост; - Общи условия за членовете на надзорния орган; - Правила за създаването на надзорния орган.

Раздел 2 (членове 55 – 59):

Компетентност, задачи и правомощия:

- Компетентност;
- Компетентност на водещия надзорен орган;
- Задачи;
- Правомощия;
- Доклади за дейността.

ГЛАВА VII:

Сътрудничество и съгласуваност

Раздел 1 (членове 60 – 62):

Сътрудничество:

- Сътрудничество между водещия надзорен орган и другите засегнати надзорни органи;
- Взаимопомощ;
- Съвместни дейности на надзорни органи.

Раздел 2 (членове 63 – 67):

Съгласуваност:

- Механизъм за съгласуваност;
- Становище на Комитета;
- Разрешаване на спорове от Комитета;
- Процедура по спешност;
- Обмен на информация.

Раздел 3 (членове 68 – 76):

Европейски комитет по защита на данните:

- Европейски комитет по защита на данните;
- Независимост;
- Задачи на Комитета;
- Доклади;
- Процедура;
- Председател;
- Задачи на председателя;
- Секретариат;
- Поверителност.

ГЛАВА VIII (членове 77 – 84):

Средства за правна защита, отговорност за причинени вреди и санкции:

- Право на подаване на жалба до надзорен орган;
- Право на ефективна съдебна защита срещу надзорен орган;
- Право на ефективна съдебна защита срещу администратор или обработващ лични данни;
- Представителство на субекти на данни;
- Прекратяване на производството;
- Право на обезщетение и отговорност за причинени вреди;
- Общи условия за налагане на административни наказания „глоба“ или „имуществена санкция“;

- Санкции.
ГЛАВА IX (членове 85 – 91): **Разпоредби, свързани с особени ситуации на обработване:** - Обработване и свобода на изразяване и информация; - Обработване и публичен достъп до официални документи; - Обработване на националния идентификационен номер; - Обработване в контекста на трудово или служебно правоотношение; - Гаранции и дерогации, свързани с обработването за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели; - Задължения за опазване на тайна; - Съществуващи правила на църкви и религиозни сдружения за защита на данните.
ГЛАВА X (членове 92 – 93): **Делегирани актове и актове за изпълнение:** - Упражняване на делегирането; - Процедура на комитет.
ГЛАВА XI (членове 94 – 99): **Заключителни разпоредби:** - Отмяна на Директива 95/46/ЕО; - Връзка с Директива 2002/58/ЕО; - Връзка с по-рано сключени споразумения; - Доклади на Комисията; - Преглед на други правни актове на Съюза за защита на данните; - Влизане в сила и прилагане.

2.4 Принципът на отчетност[234]

2.4.1 Новото задължение да бъде в състояние да докаже съответствие

Макар и да изглежда, че не е нещо ново (и да може да се каже , че е вдъхновено от американския правен подход, който е отразен в Насоките на ОИСР от 1980 г.), всъщност една от основните характеристики на новия Общ регламент относно защитата на данните (ОРЗД) на ЕС – вероятно дори *основната* характеристика – е че той силно акцентира върху факта, че:

> **Администраторът носи отговорност и е в състояние да докаже спазването на [принципите във връзка с обработването на лични данни] („отчетност”)”** (чл. 5, пар. 2).

[234] Този раздел се базира на и на места повтаря или обобщава Douwe Korff, The Practical Implications of the new EU General Data Protection Regulation for EU- and non-EU Companies (Практическото отражение на новия Общ регламент относно защитата на данните на ЕС за дружествата от и извън ЕС), август 2016 г., документ, представен в CMS Cameron McKenna LLP, Лондон, през февруари 2017 г., може да бъде намерен на:
http://ssrn.com/abstract=3165515

Както посочва италианският орган за защита на данните, *Garante della Privacy*: [235]

> Да бъде направено едно лице отговорно означава да се възложат действия и решения на това лице **и да се очаква то да носи отговорност за тези действия и решения**. Поради това, отчетността е **състоянието на отговорност** за действията и решенията, които са били възложени.

Новото не е в това че органът, отговорен за обработването - отговаря за спазването – това, разбира се, вече беше така съгласно Директивата за защита на данните от 1995 г. (въпреки че тази Директива не използва термина „отчетност"). Новото всъщност е фокусът върху администратора (а в някои случаи обработващият лични данни), който се изисква да докаже това съответствие : терминът се повтаря не по-малко от 33 пъти в Регламента.

Това контрастира с Директивата от 1995 г., която никъде не изисква изрично администратор или обработващ лични данни да докаже спазване на каквото и да е (освен ако, разбира се, те не са били задължени да направят това от ОЗД или съдилище). По-специално, различните системи за „уведомяване" или „регистрация", създадени съгласно Директивата в поне някои държави не са довели до такова съответствие ,[236] докато в други бяха полезни само с това, че бяха много подробни и представени по такъв начин, че да стимулират администраторите да прилагат всички законови изисквания спрямо всяка нова операция по обработване на данни. Съответният орган по защита на данните (ОЗД) предупреждаваше администраторът и предлагаше изменения или даваше съвет, когато това беше необходимо или се изискваше. В контекста на бързо разширяващи се и развиващи се практики за обработване на данни, и в държави (като държавите членки от ЕС), където има вече някакви значителни познания и опит с прилагането на правилата за защита на данните и нейните принципи, също в контекста на насърчаване на „социална отговорност" на организации, беше потърсен нов подход, подчертаващ основната отговорност и отчетност на обработващите лични данни (независимо дали като администратор или обработващ лични данни). Това е, което отстояват принципът на отчетност и задължението за доказване.

Раздел 2.3 отбелязва, по-долу, че Регламентът изисква назначаването на Длъжностни лица по защита на данните (ДЛЗД) за всички администратори от публичния сектор и много администратори от частния сектор, като основното институционално средства за прилагане на принципа на отчетност.

Както ясно показва разпоредбата за принципа за отчетност в чл. 5, пар. 2, който е цитиран по-горе, задължението да се докаже спазване, се прилага преди всичко спрямо основните принципи, на които е базиран Регламентът, изложени в чл. 5, пар. 1, т.е., спрямо законосъобразност, добросъвестност и прозрачност; конкретни, изрично указани и легитимни цели, както и ограничение на целта; свеждане на данните до

---

235 Луиджи Кароци, презентация на първата обучителна сесия за „T4DATA", юни 2018 г., слайд за „*Опис на активите и принципа за отчетност*" (оригинални подчертавания).

236 Вж. съображение 89 от ОРЗД, отразяващо Оценката на въздействието на ОРЗД на Комисията (Работен документ на службите на Комисията SEC (2012) 72 final), на стр.99. Той, на свой ред, препраща към „Консултативен документ на Работната група по член 29 по уведомленията", стр.6. Вж. бележка под линия 262 от работния документ на службите.

минимум (включващо адекватност, относимост и необходимост на данните); точност (включително актуалност); ограничение на съхранението (запазването); цялостност, поверителност и сигурност. То се прилага, разбира се, (изобщо се прилага *a fortiori*) особено стриктното към прилагането на тези принципи спрямо обработване, включващо специални категории данни (т.нар. чувствителни данни – чл. 9) или които в противен случай представляват висок риск за правата и свободите на физически лица (и , поради тази причина изисква специална оценка на въздействието върху защитата на данните – чл. 35).Освен това, Регламентът изрично или по подразбиране налага задължение да се докаже спазването в много по-специфични контексти, включително във връзка с:

- Получаването на съгласие (когато се изисква) (вж. чл. 7, пар. 1);
- Отказ по искане от субект на данни за достъп до данни или коригиране на данни (вж. чл. 11, пар. 2 и чл. 12, пар. 5);
- Несъобразяване с възражения на субектите на данни срещу обработване (вж. чл. 21, пар. 1);
- Разпоредбата за „достатъчни гаранции" за компетентност и вземането на „подходящи технически и организационни мерки", за да осигури сигурност на обработването на данни, от обработващи лични данни и подизпълнители на обработващи лични данни (вж. чл. 28 и 32);
- Разпоредбата за „подходящи гаранции" за прехвърляне на лични данни към трети държави без адекватна защита на данните (чл. 46);
- И други

Тясно свързани с това задължение за доказване на съответствие са новите общи и специфични задължения, които ОРЗД налага от гледна точка на:

- **създаване на регистър на дейностите по обработване на лични данни**;
  - провеждане на общ преглед на тези дейности ;
  - **оценка на рисковете** за правата и свободите на физическите лице, създадени от тези дейности;
- извършване на задълбочена **оценка на въздействието върху защитата на данните** във връзка с дейности, които се оценяват като вероятно водещи до „***висок риск***";
  - използване на **защита на данните на етапа на разработването и по подразбиране във връзка с всички дейности по обработка на лични данни;**
  - изисквания за уведомление при **нарушение на сигурността на данните**.

Ще разгледаме всичко това,и, по-специално, ролята на длъжностните лица по защита на данните във връзка с тях, по-подробно в част три.

На първо място, Регламентът налага **общо изискване да се водят подробни регистри на всички дейности на администратора по обработването на лични данни**, съдържащи конкретни данни за всяка отделна операция (чл. 30); тези регистри следва да бъдат водени в **регистър на дейностите по обработване на лични данни** и трябва да показват,

че – и как – се спазват горепосочените общи задължения и които и да е по-специфични такива (съображение 82). Вж. обсъждането на Задача 1 в Част три от този наръчник.

На второ място, Регламентът изисква администраторите, с помощта на техните длъжностни лица по защита на данните, да **преглеждат своите вътрешни дейности** и, когато е необходимо, да ги приведат в съответствие с Регламента и да отбележат прегледа и всяко корективно действие, предприето в горепосочения регистър. Вж. обсъждането на Задача 2 в част три от този наръчник.

На трето място, Регламентът налага общо задължение на администраторите „да обърнат внимание“ на **рисковете**, създадени от предложената операция по обработване на администратора, **съчетано със** задължението за прилагане на ***„подходящи технически и организационни мерки”*** за борба с тези рискове и задължения „*да се докаже, че обработването се извършва в съответствие с този Регламент*” – т.е., Регламентът изисква тези рискове наистина да бъдат оценени, както и мерките, взети предвид тази оценка,да са подходящи за тези рискове (чл. 24, пар. 1; също чл. 32). Тези въпроси също следва да бъдат надлежно вписани. Вж обсъждането на Задача 3 в част три от този наръчник.

На четвърто място, ако общата оценка на риска (отбелязана по-горе) показва, че съществува вероятност за **висок риск** за правата и свободите на физически лица, администраторът трябва, преди обработването, да извърши **оценка на въздействието върху защитата на данните (ОВЗД)** по отношение на предвидените дейности по обработване спрямо защитата на личните данни и да документира тази оценка. Документът от ОВЗД трябва да съдържа: системен опис на предвидените дейности по обработване и целите на обработването; оценка на необходимостта и пропорционалността на дейностите по обработване и на данните във връзка с тези цели; оценка на рисковете за правата и свободите на субектите на данни, които се предизвикват от обработването; и описание на мерките, предвидени за справяне с тези рискове, включително „*гаранциите, мерките за сигурност и механизмите за осигуряване на защитата на личните данни и за демонстриране на спазването на настоящия Регламент, като се вземат предвид правата и законните интереси на субектите на данни и на други заинтересовани лица*” (чл. 35). Виж обсъждането на Задача 4 в Част три от този наръчник.

На пето място, Регламентът налага задължение на администраторите да следват принципа за„**Защита на личните данни на етапа на проектирането и по подразбиране**”, както при подготовката, така и при изпълнението на всички дейности по обработване на администратора (чл. 25) – и администраторът трябва да е в състояние да докаже , че това е спазено. В това отношение, Регламентът споменава, че могат да се използва сертификация (печати за защита на данните) като „елемент”, който да демонстрира спазване (чл. 25, пар. 3, допълнително обсъден по-долу). Виж обсъждането на Задача 9 в част три от този наръчник.

И на шесто място, администраторите трябва да **документират подробно информацията за всички нарушения на сигурността на личните данни** (нарушения на сигурността на личните данни) и предприетите коригиращи действия, и да **уведомят** съответния (компетентен) надзорен орган за тези данни в срок от 72 часа (чл. 33). Субектите на данни, засегнати от нарушението, трябва също да бъдат осведомени, но само, ако „има вероятност нарушението на сигурността на личните данни да породи висок риск за

[техните] права и свободи", и с по-малко конкретика (чл. 34). Виж обсъждането на Задача 6 в Част три от този наръчник.

Освен това, Регламентът съдържа и някои по-специфични задължения за водене на регистри, включително разпоредбата, че ако двама или повече администратори съвместно определят целите и начините на обработване, те са съвместни администратори. Като такива, трябва да „определят по прозрачен начин съответните си отговорности за изпълнение на задълженията по настоящия регламент" под формата на „**договореност помежду си**"; и тази „договореност" „надлежно отразява съответните роли и връзки на съвместните администратори спрямо субектите на данни". На практика, тъй като администраторите могат да бъдат приканени от надзорните органи да докажат спазване на тези задължения, договорността ще трябва да бъде **в писмена форма или в сравнително надежден електронен формат** (чл. 26).

И, разбира се, различните разпоредби в Регламента, изискващи администраторите, съвместните администратори, обработващите лични данни и подизпълнителите на обработващите лични данни да уточняват договореностите помежду си и/или във връзка с предаване на данни в **договори или подобни правно-обвързващи инструменти** също изискват документиране.

2.4.2 Средства за доказване на съответствие

Общото задължение да се водят подробни **регистри и документация**, и по-специфичните задължения за водене на документация, наложени във връзка със съвместните администратори, нарушенията на сигурността на данните и оценки на въздействието върху защитата на данните, посочени по-горе, представляват основното, общо средство за доказване на спазване, предвидено в Регламента.

Тази документация следва да спазва една обща култура и подход за насърчаване на защитата на данните, отразени в тези **практики** като:

- съставяне и официално приемане на вътрешни политики за защита на данните (и предприемане на свързани действия, като обучение);
- внедряване на принципите за защита на данните на етапа на проектирането и по подразбиране във всички дейности по обработване на данни, продукти и услуги на администратора, на всяка стъпка, от самото им начало до реалното им прилагане ;
- свеждане до минимум на използването на запазването на лични данни, и, по-специално, използването на данни, които все още позволяват идентифициране (използване на псевдонимизация или анонимизация на данни, които преди са позволявали идентифициране, винаги когато това е възможно);
- осигуряване на възможно най-пълна прозрачност относно дейностите осъществени от администратор спрямо субектите на данни и обществото като цяло, на хартия, в онлайн формат и в ясни и много по-диференцирани декларации за защита на данните/ поверителност на уебсайтовете (напр., ясно разграничаване, директно на страницата, от която се събират личните данни, между задължителни и избираеми полета/цели и данни, и позволяване на много по-голям легитимен избор от ползвателите на сайта, чрез кликване в кутия), и

чрез въвеждане на ефективни и ефикасни средства за работа с молби от субекти на данни за обща или специфична информация; и

- гарантиране, че администраторът лично може да продължи ефективно да наблюдава дейностите, по-специално по отношение на сигурността (чрез достъп и изменение на дневници и т.н.; и е способен да повиши степента на сигурност, когато това е необходимо (напр., като използва „пачове").

(Вж. . Съображение 78)

В Част 3, ние ще разгледаме тези въпроси допълнително и по-подробно , с конкретни примери и практически насоки как да се изпълняват горепосочените задачи.

В допълнение обаче, предходното съображение (77) изброява редица **специални начини** да се докаже спазване, т.е.:

- извършване на действия в съответствие с одобрени кодекси на поведение;
- извършване на действия в съответствие с одобрени механизми за сертифициране в областта на защитата на данните;
- извършване на действия в съответствие с насоките, предоставени от Европейския комитет по защита на данните;

и, разбира се:

- извършване на действия в съответствие с указания, предоставени от длъжностно лице по защита на данните.

Към тях могат да бъдат добавени, по-специално във връзка с трансгранично прехвърляне и споделяне на лични данни:

- Обвързващи корпоративни правила (ОКП);
- административни споразумения („договорености") между публични органи; и
- стандартни или индивидуално одобрени договори за предаване на данни.

Във връзка с нарушения на сигурността на данните, уведомленията (и подробностите, посочени в уведомлението) също може да се разглеждат като специално средство за доказване на изпълнение на съответните изисквания.

Въпреки това е важно да се подчертае, че всички тези практики и методи за доказване на спазване съставляват „елементи" от цялостните усилия за отразяване на спазването, но не винаги представляват правно доказателствено средство на спазване.

2.4.3 Доказателствена стойност на различните средства за доказване на съответсвието

В повечето случаи придържането към някое от горепосочените средства за съответствие или „елемент, чрез който се демонстрира съответствие", т.е. създава презумпция за съответствие, но тази презумпция е оборима. Ако орган по защита на данните разглежда допълнително въпроса, той би могъл да установи, че, независимо от формалното придържане към тези насоки, кодекси, механизми за сертифициране, споразумения, договори или правила, в конкретния случай Регламентът все пак не е бил спазен (въпреки че, което и да е добросъвестно усилие за спазване, разбира се, би имало значително влияние върху нивото на която и да е санкция, ако действително такава бъде наложена – вж.. чл. 83).

2.5 Длъжностното лице по защита на данните (ДЛЗД)

2.5.1 Обща информация

Концепцията за ДЛЗД, назначени от администратори в публичния и частния сектор идва от немското право в сферата на защитата на данните, което дълго време ги е изисквало.[237] Дори в държави, които съгласно Директивата за защита на данните от 1995 г. не са изискали назначаването на ДЛЗД по закон (като например Австрия, която в други отношения, често следва немския пример) или са го предвидили като незадължителна по закон възможност (като във Франция), идеята се популяризира и е широко приета . В няколко държави има национални сдружения на длъжностните лица по защита на данните, а има и Конфедерация на европейските организации за защита на данните: CEDPO, която е издала „практически насоки за организации" относно „избора на най-подходящия кандидат" за длъжностно лице по защита на данните.[238] На глобално ниво, съществува Международната асоциация на професионалистите в сферата на неприкосновеността (International Association of Privacy Professionals (IAPP)) със седалище в САЩ, която, предлага сертифициране в областта на защитата на данните за „професионалисти в областта на неприкосновеността на информацията" (въпреки това, като редица други схеми за сертифициране на професионалисти в областта на неприкосновеността на иформацията, сертифицирането от асоциацията не се основава на ОРЗД: виж под-раздел 2.5.3 „Обучение и сертифициране").

(Вж. списъка на асоциациите на длъжностните лице по защита на данните в края на този под-раздел, с връзки към техните уебсайтове.)

Директивата за защита на данните от 1995 г. не изискваше назначаването на длъжностни лица по защита на данните от администратори, попадащи в нейното приложно поле. Вместо това, тя признаваше съществуването на длъжностни лица по защита на данните в правото и практиката на държавата членка, като им позволяваше да освобождават администраторите от задължението да съобщават за дейности по обработване на съответния държавен орган по защита на данните (ОЗД), ако правото на държавата членка изисква от съответния администратор да назначи длъжностно лице по защита на данните, „*което отговаря, в частност, за гарантиране по независим начин на вътрешното прилагане на националните разпоредби, приети съгласно настоящата Директива [и] за водене на регистър за извършваните от администратора дейности по обработката, който съдържа [същата информация каквато би трябвало принципно да бъде съобщена на органа по защита на данните]*" (член 18, параграф 2).

---

237 Германските термини са, съответно: *behördliche-* и *betriebliche Datenschutzbeauftragter*. За кратно резюме на ролята и функциите им по германското право, вж., напр.: https://www.wbs-law.de/eng/practice-areas/internet-law/it-law/data-protection-officer/
За по-подробно експозе на немски, вж., напр., Däubler/Klebe/Wedde/Weichert, Kompaktkommentar zum BDSG (Кратък коментар по германския Федерален закон за защита на данните), 3то издание. (2010 г.), коментари по §4f BDSG, включващи 85 бележки в полето, стр. 187 – 213.

238 CEDPO, Choosing the best candidate as your Data Protection Officer (DPO) – Practical guidelines for organisations (Как да изберете най-добрия кандидат за длъжностно лице по защита на данните (ДЛЗД) – Практически насоки за организации), 30 май 2016 г., които могат да бъдат намерени на: http://businessdocbox.com/Human_Resources/77901620-Choosing-the-best-candidate-as-your-data-protection-officer-dpo-practical-guidelines-for-organisations.html

Регламентът на ЕС от 2001 г., който определя правилата за защита на данните за самите институции на ЕС (Регламент (ЕО) 45/2001)[239] изисква от всяка институция или орган на ЕС да назначи поне едно длъжностно лице по защита на данните (чл. 24). Правилата за длъжностните лица по защита на данните на институциите на ЕС, установени в този регламент, са много подобни на тези в ОРЗД.

Т.нар. Директива за защита на данните във връзка с правоприлагането (Директива 2016/680),[240] приета едновременно с ОРЗД, изисква „компетентните органи", попадащи в приложното поле на този инструмент, също да назначат длъжностно лице по защита на данните; Насоките на Работната група по член 29 относно длъжностните лица по защита на данните (които, както допълнително е отбелязано по-долу, съдържат основните насоки за ДЛЗД, назначени съгласно ОРЗД). Те подчертават, че „[м]акар тези насоки да се фокусират върху длъжностните лица по защита на данните по ОРЗД, насоките имат отношение и към ДЛЗД по Директива 2016/680, по отношение на сходните им разпоредби".[241]

Вътрешните за ЕС длъжностни лица по защита на данните работят в тясно сътрудничество с Европейския надзорен орган по защита на данните (ЕНОЗД) и са създали мрежа от Длъжностни лица по защита на данните на институциите и структурите на ЕС. ЕНОЗД е създал уебсайт, („DPO Corner") в тяхна подкрепа. След позицията от 2005 г. на Европейския надзорен орган по защита на данните,[242] през 2010 г. мрежата от ДЛЗД издаде набор от Професионални стандарти за Длъжностни лица по защита на данните на институциите на ЕС и органи, работещи по Регламент (ЕС) 45/2001.[243] През 2012 г. ЕНОЗД издаде доклад относно статута на длъжностните лица по защита на данните, като част от своето наблюдение относно спазването на Регламент (ЕС) 45/2001 от институциите.[244] Този доклад „потвърждава, че функцията на

---

239 Пълно наименование: Регламент (ЕО) № 45/2001 на Европейския парламент и на Съвета от 18 декември 2000 година относно защитата на лицата по отношение на обработката на лични данни от институции и органи на Общността и за свободното движение на такива данни, О.В. L 8 от 12.1.2001 г., стр.1 и с.., намиращ се на:
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32001R0045&from=EN

240 Пълно наименование: Директива (ЕС) 2016/680 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни от компетентните органи за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания и относно свободното движение на такива данни, и за отмяна на Рамково решение 2008/977/ПВР на Съвета, ОВ L 119, 4.5.2016 г., стр.89 и сл., намираща се на:
http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680&from=EN

241 Насоки за длъжностните лица по защита на данните („ДЛЗД") на Работната група по член 29, първоначално приети на 13 декември 2016 г., в последната им редакция, приета на 5 април 2017 г. (WP243 rev.01), стр.4, бележка под линия 2., намиращи се на:
http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048
Оттук нататък са наричани „**Насоки на Работната група по член 29 за ДЛЗД**"

242 Европейски надзорен орган по защита на данните, Position paper on the role of Data Protection Officers in ensuring effective compliance with Regulation (EC) 45/2001 (Становище относно ролята на Длъжностните лица по защита на данните при осигуряването на ефективно спазване на Регламент (ЕО) 45/2001), намиращо се на:
https://edps.europa.eu/sites/edp/files/publication/05-11-28_dpo_paper_en.pdf

243 https://edps.europa.eu/sites/edp/files/publication/10-10-14_dpo_standards_en.pdf

244 ЕНОЗД, Monitoring compliance of EU institutions and bodies with Article 24 of Regulation (EC) 45/2001 – Report on the Status of Data Protection Officers (Наблюдение на спазването от институциите и структурите

длъжностното лице по защита на данните сега е ясно установена в рамките на институциите и структурите на ЕС и че те спазват чл. 24 от Регламента, но също така отбелязва „някои притеснителни сфери", които подлежат на допълнително наблюдение от Европейския надзорен орган по защита на данните.[245] В тези документи се съдържат доста обширни насоки по въпроси, имащи отношение към назначаването, позицията и задачите на длъжностните лица по защита на данните.

В по-ново време, и по-пряко във връзка с този Наръчник, Работната група по член 29 предоставя насоки относно длъжностните лица по защита на данните при подготовката за влизането в сила на ОРЗД.[246] Европейският комитет по защита на данните (ЕКЗД), който поема щафетата от Работната група по член 29 при влизането в пълна сила на ОРЗД, официално одобри тези насоки (както и другите документи по въпроси, възникващи по Регламента , приети от Работната група по член 29 преди тази дата).[247]

В резултат на това, няколко национални органа по защита на данните издадоха насоки относно длъжностните лица по защита на данните, някои от тях дори преди ОРЗД.[248]

на ЕС на член 24 от Регламент (ЕО) 45/2001 – Доклад за състоянието на Длъжностни лица по защита на данните), 17 декември 2012 г., наличен на: https://edps.europa.eu/sites/edp/files/publication/2012-12-17_dpo_status_web_en.pdf

245 *Вж.*, стр.3.

246 Вж. бележка под линия 209, по-горе.

247 Европейски комитет по защита на данните, Endorsement 1/2018 (Одобрения 1/2018), с които се одобряват, наред с другото, Насоките за ДЛЗД на Работната група по член 29 (посочен като седмия одобрен документ), приети на 25 май 2018 г., които могат да бъдат намерени на: https://edpb.europa.eu/sites/edpb/files/files/news/endorsement_of_wp29_documents_en_0.pdf

248 Вж., напр.:
Guide de Correspondant Informatique et Libertés (CIL) (*Guide Pratique Correspondant*), издадени от **френския** Орган по защита на данните, CNIL, през 2011 г., намиращи се на: https://www.cnil.fr/sites/default/files/typo/document/CNIL_Guide_correspondants.pdf
В **Италия**, националният орган по защита на данните, *Garante del Privacy*, издаде комплект от Често задавани въпроси (FAQs) за длъжностните лица по защита на данните (ДЛЗД), намиращ се на: https://www.garanteprivacy.it/garante/doc.jsp?ID=8036793 (Често задавани въпроси за длъжностните лица по защита на данните в частния сектор)
https://www.garanteprivacy.it/garante/doc.jsp?ID=7322110 (Често задавани въпроси за длъжностните лица по защита на данните в публичния сектор)
В **Полша**, националният орган по защита на данните, *Urząd Ochrony Danych Osobowych* (UODO), предоставя полезни съвети и препоръки относно прилагането на ОРЗД на своя уебсайт в специална секция , посветена на длъжностните лица по защита на данните: https://uodo.gov.pl/p/najwazniejsze-tematy/inspektor-ochrony-danych.
Преди влизането в сила на ОРЗД, полският орган поддържаше уебсайтът ABI за лицата, наричани по това време *Администратори на информационната сигурност*. Той съдържаше информация, която е полезна и при подготовката на бъдещи длъжностни лица по защита на данните да изпълнява тази функция, вж.: https://abi.giodo.gov.pl/. Чрез тази услуга, бъдещите длъжностни лица по защита на данните биха могли да зададат своите въпроси и предложения относно приложението и тълкуването на правните разпоредби в сферата на защита на личните данни.
В **Обединеното кралство** националният орган по защита на данните, *Information Commissioner (Комисар по информацията)* (обичайно наричан ICO (Служба на комисаря по информацията)), предоставя насоки на своя уебсайт, които по същество отразяват (и препращат към) насоките на Работната група по член 29, вж.:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-ОРЗД/отчетност-and-governance/data-protection-officers/

Настоящият раздел от Наръчника набляга на насоките на Работната група по член 29, но препраща и към останалите насоки, отбелязани по-горе, когато това е необходимо, за да се запознае по-обстойно читателя.

Основното, което трябва да бъде отбелязано в това въведение за ДЛЗД е, че от гледна точка на ОРЗД, тази длъжност е нова институция с огромно значение, която следва да се разглежда като съществен способ за практическата реализация на принципа на „отчетност" (задължение за доказване на съответствие), който беше разгледан по-рано: когато бъде назначено едно ДЛЗД и то добросъвестно изпълнява своите задачи (разгледани в част 3 от този наръчник), това следва да доведе до по-добро, по-пълно и сериозно спазване на ОРЗД от постигнатото основно чрез външен надзор от органите по защита на данните във връзка с Директивата за защита на данните от 1995 г. Сега, съгласно ОРЗД, органите по защита на данните имат както пряко, притежаващо широки познания, лице за контакт в организацията на всички съответни администратори, така и съюзник в рамките на организацията на администратора. Не е изненадващо, че няколко органа по защита на данните са определили като един от приоритетите си, сега, когато ОРЗД е в сила – да проверяват дали организациите, които трябва да назначат длъжностно лице по защита на данните (разгледано, в подраздел 2.5.2) реално са направили това.[249]

[249] Например, **Шведският** орган по защита на данните обяви, че ще извършва проверки дали организациите в банковия сектор, сектора на здравеопазването и застрахователния сектор са назначили длъжностни лица по защита на данните: Вж. https://www.datainspektionen.se/nyheter/datainspektionen-inleder-forsta-granskningarna-enligt-OPЗД/
Холандският орган по защита на данните подчертава по сходен начин в своя план за 2018 – 2019 г., че, *по-специално във връзка с публичните органи*, той ще проверява: „*изпълнението на задължението да се поддържа дейностирегистър на дейностите по обработване, задължението за назначаване на длъжностно лице по защита на данните, и начина, по който организацията разполага длъжностното лице по защита на данните и му дава възможност да изпълнява задачите, които трябва да изпълнява съгласно ОРЗД*", вж.: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/toezichtkader_autoriteit_persoonsgegevens_2018-2019.pdf (стр.7, в точката „*Overheid*" (публичен орган) (наш превод).

МЕЖДУНАРОДНИ И НАЦИОНАЛНИ АСОЦИАЦИИ НА ДЛЪЖНОСТНИТЕ ЛИЦА ПО ЗАЩИТА НА ДАННИТЕ:

Международни асоциации:

Глобални:

Международната асоциация на професионалистите в сферата на неприкосновеността (IAPP):
https://iapp.org/certify/cipp/

Европейски:

Мрежа на длъжностните лица по защита на данните на институциите и структурите на ЕС:
https://edps.europa.eu/данни-protection/eu-институция-dpo_en

Конфедерация на европейските организации за защита на данните, CEDPO
http://www.cedpo.eu/

Национални асоциации:

(Отбелязаните с * са членовете на CEDPO)

Франция:

Association Française des Correspondants à la Protection des Données à Caractère Personnel, AFCDP:*
https://www.afcdp.net/

Ирландия:

Association of Data Protection Officers (Асоциация на длъжностните лица по защита на данните), ADPO:*
https://www.dpo.ie/

Италия:

Associazone Data Protection Officer, ASSO DPO:*
http://www.assodpo.it/en/home_en/

Нидерландия:

Nederlands Genootschap voor Functionarissen Gegevensbescherming, NGFG:*
https://www.ngfg.nl/

Полша:

Stowarzyszenie Administratorów Bezpieczeństwa Informacji, SABI:*
http://www.sabi.org.pl/

Испания:

Asociación Profesional Española de Privacidad, APEP:*
http://www.apep.es/

Обединено крлатство:

National Association of Data Protection & Freedom of Information Officers (Национална асоциацият на длъжностните лица по защита на данните и свобода на информацията, NADPO:
https://nadpo.co.uk/

Германските и **австрийските** членове на CEDPO, съответно *Gesellschaft für Datenschutz und Datensicherheit e.V.*, DGG* (създадено през 1977 г.) и *Arge Daten**, не ограничават членството само до длъжностни лица по защита на данните, но са членове и двете на CEDPO:

https://www.gdd.de/ueber-uns
http://www.argedaten.at/php/cms_monitor.php?q=PUB-TEXT-ARGEDATEN&s=15904tpb

2.5.2 Задължението за назначаване на Длъжностно лице по защита на данните за публични органи[250]

Назначението на длъжностно лице по защита на данните е задължително за всички публични органи или органи, обработващи лични данни, които са в приложното поле на ОРЗД (чл. 37, пар. 1, б. „а")).[251] Макар да го оставя на държавите членки, Работната група по член 29 правилно взема предвид това изискване:[252]

„Публичен орган или структура"

ОРЗД не определя кое е „публичен орган или структура". Работната група по член 29 счита, че такова понятие следва да бъде определено съгласно националното право. Съответно, публичните органи и структури включват национални, регионални и местни органи, но съгласно приложимите национални законодателства, обичайно това понятие включва и редица други органи, управлявани от публичното право.[253] В такива случаи, е задължително определянето на длъжностно лице по защита на данните.

---

250 Освен във връзка с частни субекти, които изпълняват „обществени задачи" или „упражняват публична власт" – както е разгледано в текста – задължението да се назначи длъжностно лице по защита на данните за „изцяло" частни (търговски) дружества не се разглежда в този Наръчник. Достатъчно е да се отбележи, че за тези субекти Регламентът принципно предвижда, че длъжностното лице по защита на данните е задължително само в следните случаи:

- когато основните дейности на администратора или обработващия лични данни се състоят в дейности по обработване, които поради своето естество, обхват и/или цели изискват редовно и систематично мащабно наблюдение на субектите на данни; или
- когато основните дейности на администратора или обработващия лични данни се състоят в мащабно обработване на специалните категории данни съгласно чл. 9 [т.е., на т.нар. „чувствителни данни"] и на лични данни, свързани с присъди и нарушения, по чл. 10.

(чл. 37, пар. 1, б. б) и в) от ОРЗД)

Тези условия са разгледани по-подробно в Насоките за длъжностни лица по защита на данните на Работната група по член 29. Тук, може да бъде достатъчно да се отбележи, че на практика повечето дружества – независимо от своя мащаб – ще счетат за полезно да назначат длъжностно лице по защита на данните, което да изпълнява техните изисквания за „отчетност"/ „задължение да се докаже спазване", разгледани по-горе, в 2.2.

251 Единственото изключение в това отношение е свързано със „съдилищата, действащи в тяхното съдебно качество" (чл. 37, пар. 1, б. „а") от ОРЗД). Както обаче Работната група по член 29 подчертава в своите Насоки за длъжностните лица по защита на данните (бележка под линия 209, по-горе), това не означава, че те не трябва да спазват Регламента – обратното: те също трябва да го спазват. А по отношение на обработването на съдилищата, когато не действат в качеството си на съдебни органи, те трябва да спазват изискването за назначаване на длъжностно лице по защита на данните.

Този Наръчник не разглежда длъжностни лица по защита на данните за органи, осъществяващи обработване, което е изцяло извън обхвата на правото на ЕС, като национални агенции за сигурност.

252 Насоки на Работната група по член 29 относно ДЛЗД, (бележка под линия 209, по-горе) стр.6.

253 Вж., напр. определението за „орган от обществения сектор" и „орган, управляван от публичното прав" в член 2, параграфи 1 и 2 от Директива 2003/98/ЕО на Европейския парламент и на Съвета от 17 ноември 2003 г. относно повторната употреба на информацията в обществения сектор, ОВ L 345, 31.12.2003 г., стр.90 и сл. [оригинална бележка под линия]

Английският текст на тази директива може да бъде намерен тук:
http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32003L0098&from=EN

Задължението за назначаване на длъжностно лице по защита на данните всъщност се простира и отвъд тази чисто формална категория.

Субекти от частния сектор, които изпълняват „задачи в обществен интерес" или които „упражняват официални правомощия"

Работната група по член 29 подчертава, във връзка със специалното правно основание за обработване в чл. 6, пар. 1, б. „д") от ОРЗД, че (независимо от ограниченията върху задължението за назначаване на ДЛЗД за лица, принадлежащи „изцяло" към частния сектор)[254] ДЛЗД следва винаги да бъде назначавано от администратори от частния сектор, които изпълняват „задачи… в обществен интерес" или които „упражняват официални правомощия", дори ако те формално не са „публични органи" от гледна точка на националното право, тъй като в тези дейности тяхната роля ще бъде подобна на ролята на публичните органи:[255]

> Обществена задача може да бъде изпълнявана, както и публични правомощия могат да бъдат упражнявани не само от публични органи или структури, но и от други физически или юридически лица, управлявани от публичното или частното право, в сектори като, съобразно националната правна рамка на всяка държава членка, обществени транспортни услуги, водоснабдяване и електроснабдяване, пътна инфраструктура, обществени медии, социално жилищно настаняване или дисциплинарни органи за регулираните професии.
>
> В тези случаи субектите на данни могат да се намират в подобна ситуация, както когато данните им се обработват от публичен орган или структура. По-специално, данните могат да бъдат обработвани за подобни цели и субектите на данни често имат малък или никакъв избор за това дали и как данните им да бъдат обработвани и поради това може да изискат допълнителна защита, която едно длъжностно лице по защита на данните може да осигури .
>
> **Макар да няма задължение в тези случаи, Работната група по член 29 препоръчва, като добра практика, частните организации, осъществяващи публични задачи или упражняващи публични правомощия, да определят длъжностно лице по защита на данните.** Дейността на това длъжностно лице по защита на данните обхваща всички осъществявани дейности по обработване, включително тези, които не са свързани с изпълнението на обществена задача или упражняването на официално задължение (напр. управлението на база данни на служители).

Към примерите, посочени от Работната група по член 29, някой би могъл да добави ръководенето на затвори и други държавни институции или услуги (като депортиране на имигранти, за които е постановено, че се намират незаконно в страната) от частни лица. Във всички тези случаи частните лица успешно действат като държавни клонове – и във всички тези случаи въпросните дружества следва да назначат длъжностно лице по защита на данните. Държавите членки могат освен това да доразяснят това в своето национално законодателство и да наложат задължение за назначаване на ДЛЗД на

---

254 Вж. бележка под линия 218, по-горе.

255 Насоки за длъжностните лица по защита на данните на Работна група по член 29 (бележка под линия 209, по-горе), стр.6, с добавено удебеляване. Работната група по член 29 използва термините „обществена задача" и „публичен орган" чисто лингвистично: в насоките, тези термини се отнасят до „задачи от обществен интерес" и „упражняване на официалните правомощия", посочени в Чл.н 6, пар. 1, б. „д") от ОРЗД.

конкретни администратори или видове администратори, различни от формалните публични органи или структури (вж. чл. 37(4)).

ПРИМЕР:

В **Италия**, националният орган по защита на данните, *Garante* счита, че всички субекти, които преди това са попаднали в приложното поле на членове 18 до 22 от италианския Кодекс за защита на данните, трябва да се счита, че са задължени да определят длъжностно лице по защита на данните. Членове 18 до 22 от Кодекса за защита на данните предвижда общите правила, приложими спрямо обработването, осъществявано от публични субекти – като държавни административни органи, нетърговски публични структури на национално, регионално и местно ниво, области, местни органи, университети, Търговски палати, агенции в областта на здравеопазването, независими надзорни органи и т.н.

Освен това *Garante* твърди, че когато частен субект изпълнява публични функции – напр. на база на лиценз или концесия – определянето на ДЛЗД е силно препоръчително, въпреки че не е задължително. Той добавя, във връзка с Насоките за длъжностните лица по защита на данните на Работната група по член 29, че ако едно длъжностно лице по защита на данните бъде определено доброволно, се прилагат същите изисквания и условия както в случая на задължително определено длъжностно лице по защита на данните – от гледна точка на критериите за определянето на ДЛЗД , неговата позиция и отговорности.

Длъжностни лица по защита на данните за обработващи лични данни

Както посочва Работната група по член 29, членът в ОРЗД, който налага задължението да се назначи длъжностно лице по защита на данните в определени случаи (чл. 37), както е очертано за публичния сектор по-горе, се прилага, спрямо администратори и спрямо обработващи лични данни.[256] Тя добавя:[257]

> В зависимост от това кой изпълнява критериите за задължително определяне, в някои случаи само администраторът или само обработващият лични данни, в други случаи и двамата трябва да назначат длъжностно лице по защита на данните (които след това следва да си сътрудничат помежду си).
>
> Важно е да се подчертае, че дори ако администраторът изпълни критериите за задължително определяне, от неговия обработващ лични данни не се изисква задължително да назначи длъжностно лице по защита на данните. Това обаче може да се окаже добра практика.

За публичния сектор, в който всички съответни органи трябва да назначат длъжностно лице по защита на данните (както е разгледано по-горе), това може да изглежда, че не е важен въпрос. С оглед обаче на последния коментар на Работната група по член 29, ако даден публичен орган трябва да възложи някаква дейност по обработване на подизпълнител – частен субект (напр., счетоводство или извършването на проучвания),

---

256 Насоки за длъжностните лица по защита на данните на Работната група по член 29 (бележка под линия 209, по-горе), раздел 2.2, *Длъжностно лице по защита на данните на обработващия лични данни*, на стр.9.

257 *Пак там*. Работната група по член 29 дава някои примери, взети от частния сектор, които се фокусират върху ограниченията на задължението за назначаване на длъжностно лице по защита на данните за този сектор; поради това, те не са особено полезни в настоящия Наръчник.

би било най-малкото препоръчително да се избере обработващ лични данни, който също има длъжностно лице по защита на данните, или да се изиска от обработващия лични данни, който все още няма длъжностно лице по защита на данните, да назначи такова.

Доколкото работещи заедно публични органи могат в определени моменти да действат и като обработващи лични данни едини за други, това следва, още повече, да бъде отразено в писмената документация за техните договорености, както е отбелязано в следващата подточка и допълнително разгледано в Част 3, подраздел 3.1.

Длъжностни лица по защита на данните за големи публични органи или групи от органи

В следствие на „дигиталния преход“, личните данни все повече се обработват в изключително сложни среди и технически структури, в които различните участници работят в тясно сътрудничество и са свързани помежду си или чрез различни дейности по обработване включително на данни на граждани. Така стоят нещата и в публичния сектор, в който се срещат различни трудности от гледна точка на автономията, която различните агенции може да имат в рамките на една по-широка конституционна или административна правна рамка. Както е допълнително разгледано в Част 3, раздел 3.1, една от първите задачи, на което и да е новоназначено ДЛЗД, е да „определи обхвата” на контекста за обработването на лични данни, за надзора на който и/или консултирането, по който ще отговаря то. Част от тази работа ще бъде да се разясни, по отношение на тези сложни контексти, какъв статут точно имат различните субекти, които са част от организацията , и да се изготвят и документират подходящи договорености.

В това отношение, следва да бъде отбелязано, че ОРЗД изрично предвижда (както предвиждаше Директивата за защита на данните от 1995 г.), че “когато целите и средствата за ... обработване се определят от правото на Съюза или правото на държава членка” (какъвто ще е обичайно случаят при публичните органи), „администраторът или специалните критерии за неговото определяне могат да бъдат установени в правото на Съюза или в правото на държавата членка” (чл. 4, пар. 7). Често в такива случаи, е удачно да бъде назначено длъжностното лице по защита на данните за цялото обработване, обхванато от това определение в офисите на субекта, който е определен като администратор на обработването. Действително, може самият закон, определящ администратора, да разяснява това.

Ако това не е определено със закон, въпросът може да се наложи да бъде разрешен от съответния министър от правителството, висше длъжностно лице или между самите публични органи. Това следва да доведе до ясни договорености за съответните отговорности и компетентности на различните длъжностни лица по защита на данните в различните органи, формиращи част от организацията . Част от това включва решението дали да се назначи ДЛЗД или няколко длъжностни лица по защита на данните. Споразуменията следва също така да обхващат връзките и договореностите между различните длъжностни лица по защита на данните в оперативно свързанисубекти.

Някои много големи публични структури (или министри от правителството или висши длъжностни лица на тези структури) може да решат да назначат няколко длъжностни лица по защита на данните за всяка от своите съставни части – при условие че това отрязва действителното разпределение на правомощията за вземане на решения

между отделните отдели или звена на тези големи публични органи. Или те може да решат да назначат едно ДЛЗД за цялата структура, което да работи с определени лица в нея. В коментарите, направени от Работната група по член 29 в контекста на назначаването на длъжностни лица по защита на данните въз основа на договор за предоставяне на услуги (обсъден в следващата подточка) следва, че тези определени лица в отдели или обособени части на голямата организация следва, от една страна, да отговарят на изискванията за длъжностни лица по защита на данните, по-специално да не са в какъвто и да е конфликт на интереси, и – от друга страна – следва да се ползват с подобна защита, като самото ДЛЗД и да не бъдат подлагани под отговорност за упражняването на техните задължения. [258]

От друга страна , ОРЗД позволява на **групи от (официално обособени) по-малки публични структури** – като местни власти (на френски език: *communes*) – да решават (или да бъдат инструктирани) съвместно да назначат длъжностно лице по защита на данните:

> Когато администраторът или обработващият лични данни е публичен орган или структура, може да бъде определено едно длъжностно лице по защита на данните за няколко такива органа или структури, като се отчита тяхната организационна структура и мащаб. (чл. 37(3))

Това длъжностно лице по защита на данните би могло да бъде длъжностно лице на един от органите или съвместно да изпълнява задълженията си на повече от една структура , въз основа на договор за предоставяне на услуги (както е обсъдено в следващата подточка). Ако бъде назначено едно (вътрешно или външно) ДЛЗД, всеки от другите (малки) субекти следва все пак да определи служител, отговорен за поддържането на контакт с централното (съвместно) длъжностно лице по защита на данните – и в този случай същото се прилага спрямо по-големите органи: определените лица следва да отговарят на изискванията за длъжностно лице по защита на данните и да имат сходна защита, както самото длъжностно лице по защита на данните.

Външни длъжностни лица по защита на данните

Както вече бе отбелязано, публичните органи (и частните дружества) не трябва да създават вътрешна позиция за длъжностно лице по защита на данните, нито такова на пълен работен ден (макар че може би е предпочитано от повечето по-големи структури). По-скоро:

> [д]лъжностното лице по защита на данните може да бъде член на персонала на администратора или на обработващия лични данни, или да изпълнява задачите въз основа на договор за услуги" (чл. 37, пар. 6).

В Германия, откъдето произхожда идеята за длъжностни лица по защита на данните,[259] адвокатските кантори или други независими експерти предлагат ДЛЗД да функционира по този начин. Освен това, „асоциациите и другите органи, представляващи категории администратори или обработващи лични данни" могат, , също да изпълняват функциите на длъжностно лице по защита на данните за своите служители и в този смисъл да действат от името на всички тях (ср. чл. 37, пар. 4). Това би било полезно, по-специално,

---

[258] Ср. Насоки за длъжностните лица по защита на данните на Работната група по член 29 (бележка под линия 209, по-горе), раздел 2.4, последно тире, на стр.12.

[259] Вж. под-раздел 2.5.1, по-горе.

за малките предприятия. Редица големи консултантски фирми и адвокатски кантори също предлагат услуги, покриващи функциите на ДЛЗД „въз основа на договор за услуги". Ще възникнат и по-малки фирми, по-специално специализираните в работа с ИКТ, които ще предлагат същите услуги на подобна база.

Тези външни длъжностни лица по защита на данните не следва да бъдат дистанцирани от органите, на които предоставят услугите си: както става ясно в следващата част от Наръчника, длъжностните лица по защита на данните трябва да имат пълно и вътрешно разбиране за тези органи и техните дейности по обработване. Освен това трябва да бъдат напълно и лесно достъпни – за персонала на въпросните структури, както и за субектите на данни и органи по защита на данните (надзорни органи). Техните данни за контакт следва да бъдат ясно посочени на уебсайтовете на съответните органи, както и в брошури и т.н.

Френският орган по защита на данните, CNIL, счита, че длъжностното лице по защита на данните следва „препоръчително" да е член на персонала на организацията на администратора, но приема, че за малките и средните предприятия това може не винаги да е възможно.[260]

В публичния сектор, е препоръчително да се разполага с длъжностно лице по защита на данните от конкретния засегнат сектор – напр., както е разгледано по-горе, за голяма публична структура- основно длъжностно лице по защита на данните, или едно за група от по-малки органи към един от тях – вместо фирма от частния сектор да действа като външно длъжностно лице по защита на данните, но това ще зависи от културата и практиките в съответната държава.

2.5.3 Квалификации, качества и позиция на длъжностното лице по защита на данните

Необходим опит

Регламентът предвижда, че:

> Длъжностното лице по защита на данните се определя въз основа на неговите професионални качества, и по-специално въз основа на **експертните му познания в областта на законодателството и практиките в областта на защитата на данните и способността му да изпълнява задачите**, посочени в чл. 39 [както е разгледано по-долу, в 2.5.4].
>
> (чл. 37, пар. 5, добавено подчертаване)

По първата точка – експертни познания – документът за „професионалните стандарти" на длъжностните лица по защита на данните на институциите на ЕС отбелязва необходимостта от следното:[261]

> (а) Експертен опит в правото на ЕС в областта на защитата на неприкосновеността на личния живот и на данните, по-специално чл. 16 от Договора за функционирането на Европейския съюз, чл. 8 от Хартата на основните права на Европейския съюз, Регламент (ЕО) 45/2001 и други

[260] CNIL, *Guide Pratique Correspondant* (бележка под линия 228, по-горе), стр.6.

[261] Мрежа на длъжностните лица по защита на данните на институциите и структурите на ЕС, Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001 (Професионални стандарти за длъжностни лица по защита на данните на институциите и структурите на ЕС, работещи по Регламент (ЕО) 45/2001) (вж. бележка под линия 212, по-горе), стр.3 – 4.

съответни нормативните актове в областта на защитата на данните, и експертиза в сферата на ИТ и ИТ сигурността; и

(b) Добро разбиране на начина, по който работи институцията [към която е назначено длъжностното лице по защита на данните] и за неговите дейности по обработването на лични данни, и способност да тълкува съответните правила за защита на данните в конкретния контекст.

Техническото познаване на ИТ системите е препоръчително. Както **френският** орган по защита на данните, CNIL, посочва:[262]

> Във връзка с информационните технологии , се изисква добро разбиране на терминологията, [ИТ] практиките и различни форми на обработване на данни. Длъжностното лице по защита на данните следва да има широки познания, например, относно системите за управление и използване на данни, видовете софтуер, файловете и системите за съхранение на данни, както и относно изискванията за поверителност и политиките за сигурност (криптиране на данни, електронни подписи, биометрия, …). Тези знания следва да позволят на [длъжностното лице по защита на данните] да наблюдава изпълнението на ИТ проекти и да предоставя полезни съвети на администратора, отговарящ за обработването.

Съображение 97 от ОРЗД също подчертава, че:

> Необходимото ниво на експертни познания следва да бъде определено по-специално съобразно извършваните дейности по обработване на данни и защитата, която се изисква за личните данни, обработвани от администратора или обработващия лични данни.

С други думи, естеството на изискуемите „експертни познания" и „способност" може да бъде много различно в зависимост от дейностите на администратора: длъжностното лице по защита на данните за данъчен орган ще се нуждае от различна експертиза в сравнение с това, работещо за образователен или социален орган. Европейският надзорен орган по защита на данните посочва това като нужда от „**близост**" (на длъжностното лице по защита на данните до субекта, който обслужва):[263]

> Длъжностното лице по защита на данните играе основна роля в рамките на институцията/структурата: длъжностните лица по защита на данните са [т.е., следва да бъдат] запознати с проблемите на организацията, в която работят (*идея за близост*) и, с оглед на техния статут, имат съществена роля при даването на съвети и помощ при разрешаването на въпроси, свързани със защита на данните [да се чете: в зависимост от спецификите на въпросния орган].

Както се посочва в Насоките за длъжностните лица по защита на данните на Работната група по член 29:[264]

> Длъжностното лице по защита на данните следва да има нужното разбиране за дейностите по обработване, осъществявани [в съответния сектор и организация],

---

262 CNIL, *Guide Pratique Correspondant* (бележка под линия 208, по-горе), стр.8 (наш превод).

263 Европейски надзорен орган по защита на данните, Position paper on the role of Data Protection Officers in ensuring effective compliance with Regulation (EC) 45/2001 (Становище относно ролята на Длъжностните лица по защита на данните при осигуряването на ефективно спазване на Регламент (ЕО) 45/2001) (бележка под линия 210, по-горе), стр.5, добавено подчертаване.

264 Насоки за длъжностните лица по защита на данните на Работната група по член 29 (бележка под линия 209, по-горе), стр.11.

> както и да борави с информационните системи и да подпомага нуждите на администратора в областта на сигурността и защитата на данните.
>
> В случай когато става дума за публичен орган или структура, длъжностното лице по защита на данните следва да има и задълбочени познания за [вътрешните] административни правила и процедури на организацията.

Към което би могло да се добави: и за законите и правилата и процедурите, съгласно които работи съответният публичен орган (напр., данъчния закон или закона за образованието и т.н.), и като цяло за административното право и процес.

От друга страна, както е отбелязано по-долу, в точките „*Конфликт на интереси*" и „*Позиция в рамките на организацията*", назначаването на член на съществуващия персонал на публична структура може да създаде проблеми, по-специално, ако назначеното лице е назначено на непълно работно време и запазва други функции в рамите на въпросния орган.

Експертните познания в областта на законодателството и практиките в областта на защитата на данните могат принципно да бъдат доказани с обучение и офлайн и онлайн курсове, и т.н., преминати от въпросното лице – например такива като предлаганите в програмата „T4DATA", в контекста на която е написан този Наръчник. Но много други курсове, с различно ниво и качество, също са широко разпространени, както е посочено по-долу.

Обучение и сертифициране

Към момента на написване (декември 2018 г.) бяха предприети стъпки в, **Испания**, за създаването на програма за сертифициране за длъжностни лица по защита на данните, но тя все още не е стартирала.[265] Освен това, тази система за сертифициране на ДЛЗД (и някои други, които се разглеждат) са базирани на ISO 17024, т.е. на система за сертифициране на лица и професионалисти; като такива, те не отговарят на изискванията от ISO 17065, която е система по концепцията за сертифициране по ОРЗД (сертифициране на услуги, продукти, евентуално системи за управление). Така, системите за сертифициране, свързани с длъжностни лица по защита на данните, са различни от „сертификати" по смисъла на член 42 от ОРЗД. Те са обещаващи , но не са сертификати, съответстващи на изискванията на ОРЗД. .

Във Франция са издадени две „референции", свързани със системи за сертифициране на длъжностни лица по защита на данните, които са издадени от органа по защита на данните, CNIL, на 11 октомври 2018 г. и публикувани в национален Държавен вестник. Едната е за сертифицирането във връзка с компетентността на ДЛЗД, другата е относно

---

[265] Испанският национален орган по защита на данните, *Agencia Española de Protección de Dato* (AEPD) е създала Схема за сертифициране за длъжностни лица по защита на данните (*Esquema de Certificación de Delegados de Protección de Datos de la Agencia Española de Protección de Datos – Esquema AEPD-DPD*), съгласно която националната испанска агенция за акредитация (*la Entidad Nacional de Acreditación – ENAC*) може да акредитира Сертифициращи органи (*Entidades de Certificación*), които след това могат да издават съответните сертификати, въз основа на критерии, разработени от Органа за защита на данните (AEDP) и формален изпит, вж.:
https://www.aepd.es/reglamento/cumplimiento/common/esquema-aepd-dpd.pdf (версия 1.3, 13 юни 2018 г.)
Все още обаче не са акредитирани такива Сертифициращи органи и поради тази причина все още не са издадени сертификати за длъжностно лице по защита на данните.
Вж. също краткото, по-общо изложение на схемите за сертифициране в 2.1, по-горе.

предвиждането на компетентностите на длъжностните лица по защита на данните и за акредитиращите организации, оправомощени да сертифицират длъжностни лица по защита на данните.[266]

В **Германия** се предлагат различни курсове и семинари за обучение, някои от които водят до определена форма на сертифициране,[267] но въпреки че тази практика има дългогодишна история в страната, няма законово определена, официално призната система . Някои от международните и национални асоциации на ДЛЗД, изброени по-рано, също предлагат специализирани обучения – но, отново, без законова уредба.[268]

Много от тези обучителни курсове или семинари са насочени към това да предоставят на обучаващите се експертиза в областта на ОРЗД и насоки по отношение на задачите, възлагани на длъжностни лица по защита на данните по Регламента. ОРЗД обаче (подобно на германския и други национални закони) не предвижда изрично някакви по-подробни критерии или системи за сертифициране. Евентуално, в бъдеще, освен Испания, други държави членки също ще предвидят такива формални, официално признати системи и/или Европейският комитет по защита на данните би могъл (вероятно неформално) да одобри такива.[269] Докато това обаче се случи, параметрите остават по-скоро отворени. Както казва **италианският** орган по защита на данните, *Garante*:[270]

> Както при т.нар. „нерегулирани професии", са разработени собствена система за доброволно сертифициране на професионални умения и компетентности. Тези системи се управляват от няколко сертифициращи органа. Сертифицирания от този тип – които не попадат в приложното поле на чл. 42 от ОРЗД – понякога се издават след посещение на обучение и/или курсове за проверка на наученото.
>
> Макар и да представляват много ценен инструмент, който – подобно на други атестирания – може да предостави доказателства за това, че даден професионалист има поне основни познания за приложимите правила, тези системи за сертифициране не са равняват, сами по себе си, на „квалификации",

---

266 Вж.: https://www.cnil.fr/fr/certification-des-competences-du-dpo-la-cnil-adopte-deux-referentiels

267 Ср., напр.: https://www.datenschutzexperten.de/grundlagenseminar-ausbildung-betrieblicher-datenschutzbeauftragter-nach-bdsg-mit-dekra.html

268 Документът със Критерии за длъжностните лица по защита на данните в институциите на ЕС препоръчва система на Международната асоциация на професионалистите в сферата на неприкосновеността (IAPP). IAPP предлага специфични за регионите програми за сертифициране, включително такава, която е ориентирана към Европа, обхващаща и ОРЗД. Вж.: https://iapp.org/certify/cippe/

Мрежа на длъжностните лица по защита на данните на институциите и структурите на ЕС, Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001 (Професионални стандарти за длъжностни лица по защита на данните на институциите и структурите на ЕС, работещи по Регламент (ЕО) 45/2001) (вж. бележка под черта 212, по-горе), стр.5.

Документът за длъжностните лица по защита на данните в институциите на ЕС споменава и системи за сертифициране за управление на ИТ сигурността и за одити, но те са по-общи и не са специално насочени към защитата на данните.

269 В Насоките за длъжностните лица по защита на данните на Работната група по член 29 (бележка под черта 209, по-горе) просто се казва, че „от полза е и надзорните органи да насърчават адекватно и редовно обучение за длъжностните лица по защита на данните." (стр.11).

270 *Garante del Privacy*, Често задавани въпроси за длъжностните лица по защита на данните (бележка под черта 216, по-горе), раздел 3.

> даващи възможност за изпълнение на задачите, свързани с длъжностното лице по защита на данните и не могат да заменят задължението на публичните административни органи да оценят изискванията, на които едно длъжностно лице по защита на данните трябва да отговаря с оглед на задачите и задълженията, посочени в чл. 39 от Общия регламент относно защитата на данните.

Както посочва Конфедерацията на европейските организации за защита на данните (CEDPO):[271]

> Кандидатите вероятно ще Ви покажат много сертификати и дипломи, които са им издадени през годините, за да покажат колко са квалифицирани. Но как да прецените кои са съществени и кои не са? Първото нещо, което следва да проверите, е свидетелството за акредитация на страната, предоставяща обучението и сертифицирането. Ако тя е добре позната акредитирана страна, действаща в целия ЕС или национална организация (в някои държави сертифицират дори органи по защита на данните), можете да бъдете спокойни. Също така, е хубаво да се запознаете с програмата на обучителните курсове. Еднодневно обучение, или сертификати, получени главно в резултат на плащане и обикновен изпит, няма да подготвят едно надеждно ДЛЗД..

Всички различни документи с насоки също подчертават необходимостта организациите да гарантират, че тяхното длъжностно лице по защита на данните може да продължи да поддържа и подобрява своята експертиза, и след неговото назначаване, като взима участие в съответни курсове и семинари. Това всъщност се изисква и от ОРЗД (вж. последните думи в чл. 38, пар. 2). Както посочва Работната група по член 29:[272]

> Длъжностните лица по защита на данните следва да получат възможността да се осведомяват за развитието в областта на защитата на данните. Целта следва да бъде постоянно да се покачва нивото на експертиза на длъжностните лица по защита на данните и те следва да бъдат насърчавани да участват в обучителни курсове за защита на данните и други форми на професионално развитие, като участие във форуми, работни срещи и др., посветени на неприкосновеността на личния живот.

Френският орган за защита на данните, CNIL, предоставя полезна и специална „**extranet**" (база от данни) за регистрирани длъжностни лица по защита на данните, достъпна само за тях с потребителско име и парола, която им предоставя правни текстове (закони, постановления и т.н.) и обучение и информация, включително информация за нови доклади или насоки, издадени от CNIL, и за други юридически и практически новости, и им позволява да обменят възгледи и да провеждат обсъждания.[273]

Опит

Насоките за длъжностните лица по защита на данните на Работната група по член 29 не разглеждат въпроса какъв (колко продължителен) опит следва да има едно длъжностно лице по защита на данните. Мрежата от длъжностни лица по защита на данните на

---

271 CEDPO, Choosing the best candidate as your Data Protection Officer (DPO) – Practical guidelines for organisations (Как да изберете най-добрия кандидат за длъжностно лице по защита на данните (ДЛЗД) – Практически насоки за организации) (бележка под линия 239, по-горе), стр.2.

272 Насоки за длъжностните лица по защита на данните на Работната група по член 29 (бележка под линия 209, по-горе), стр.14.

273 CNIL, *Guide Pratique Correspondant* (бележка под линия 228, по-горе), section 4.

институциите на ЕС обаче препоръчва тези длъжностни лица по защита на данните да имат следния опит:[274]

> поне 3 години съответен опит [вж. по-долу], за да служат като длъжностно лице по защита на данните в структура, в която защитата на данните не е свързана с основната дейност [*пак там*] (и по този начин дейностите по обработване на лични данни са основно административни); и
>
> поне 7 години съответен опит, за да служи като длъжностно лице по защита на данните в институция на ЕС или в тези структури на ЕС, в които защитата на данните е свързана с основната дейност или които имат важен обем от дейности по обработване на лични данни.

Те добавят бележка под линия, че:

> Съответен опит включва опит при изпълнението на изискванията за защита на данните и опит в рамките на назначаващата институция/организация, в резултат от който са придобити познания как тя функционира. В отсъствието на посочените години опит (стаж), назначаващата институция/организация следва да бъде подготвена да предостави повече време на длъжностното лице по защита на данните за обучение и за работа по задължения в сферата на защитата на данните.

По въпроса дали обработването на лични данни „е свързан[о] с основната дейност" на съответната организация, насоката на Работната група по член 29 относно значението на сходния израз в ОРЗД („основните дейности на администратора или обработващия лични данни") е относима:[275]

> „Основни дейности" може да се счита, че са основните дейности, необходими за постигане на целите на администратора или обработващия лични данни.

Фразата „съответен опит" не следва да се чете и разбира изрично като опит, като длъжностно лице по защита на данните – това би могъл да е опит в изготвянето и прилагането на политики в съответната организация (или подобна организация), или съответните област като ИТ, разработване на продукти и т.н. Достатъчно е да се спомене, че позицията не следва да бъде възлагана на сравнително млад, неопитен човек или на лице, което не е запознато с конкретния (тип) организация, за която става въпрос.

Личностни характеристики и качества

И Европейският надзорен орган по защита на данните, и институционалните длъжностни лица по защита на данните в ЕС, и CEDPO отбелязват, че длъжностното лице по защита на данните трябва да притежава специални личностни качества. То е в деликатна позиция: трябва да е готово да каже „не" на своите началници в редки случаи, но по-често да бъде в състояние да помага за намирането на решение на въпроси, което трябва както да бъде приемливо за организацията, така и изцяло да бъде в съответсвие

---

274 Мрежа на длъжностните лица по защита на данните на институциите и структурите на ЕС, Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001 (Професионални стандарти за длъжностни лица по защита на данните на институциите и структурите на ЕС, работещи по Регламент (ЕО) 45/2001) (вж. бележка под линия 212, по-горе), стр.4.

275 Насоки за длъжностните лица по защита на данните на Работната група по член 29 (бележка под линия 209, по-горе), стр.6.

със закона (и, ако не друго, да следи и защитава неприкосновеността). Както се посочва в Насоките на Работната група по член 29:[276]

> Личностните качества следва да включват, например почтеност и висока професионална етика; основната грижа на длъжностното лице по защита на данните следва да бъде съответствието с ОРЗД. Длъжностното лице по защита на данните играе ключова роля при насърчаването на култура на защита на данните в рамките на организацията и помага да се реализират съществени елементи от ОРЗД …

Институционалните длъжностни лица по защита на данните от ЕС подчертават необходимостта от следните „личностни" и „междуличностни" умения:[277]

> Личностни умения: почтеност, инициативност, организираност, упоритост, дискретност, умения за себеотстояване при трудни обстоятелства, интерес от защитата на данните и мотивация да бъде длъжностно лице по защита на данните.
>
> Междуличностни умения: общуване, преговори, разрешаване на конфликти, способност за изграждане на работни взаимоотношения.

На друго място те отбелязват:[278]

> Надлежното изпълнение на задачите на длъжностното лице по защита на данните често изисква то да заеме твърда позиция и спрямо администратори, които заемат висока позиция в организацията, която може да бъде възприета, в най-добрия случай, като бюрократична или, в най-лошия случай – като неприятна и „създаваща проблеми". По този начин, длъжностното лице по защита на данните трябва да бъде в състояние да издържа на напрежението и трудностите, съпътстващи тази важна позиция.

CEDPO добавя:[279]

> Длъжностното лице по защита на данните трябва да се изправи пред редица предизвикателства, засягащи различни интереси. Ето защо длъжностното лице по защита на данните следва да покаже и силни комуникативни умения, съчетани с умела дипломация. Длъжностното лице по защита на данните не е (и не следва да бъде) „активист в областта на личния живот": с подкрепата на другите лидери на организацията, то трябва да играе роля на отговорно лице, което улеснява дейността и помага на организацията да включи неприкосновеност на личния живот в процесите по вземане на бизнес решения, както и не само да открива и предотвратява рискове, но и помага за по доброто разбиране на правилата и процесите за защита на личните данни. В допълнение към това, ОРЗД изисква той

---

[276] Насоки за длъжностните лица по защита на данните на Работната група по член 29 (бележка под линия 209, по-горе), стр.11.

[277] Мрежа на длъжностните лица по защита на данните на институциите и структурите на ЕС, Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001 (Професионални стандарти за длъжностни лица по защита на данните на институциите и структурите на ЕС, работещи по Регламент (ЕО) 45/2001) (вж. бележка под линия 212, по-горе), стр.4.

[278] *Пак там*, стр.6. Мрежата отправя препоръки за облекчаване на този натиск в контекста на обсъждането от нейна страна на позицията, която да бъде дадена на длъжностното лице по защита на данните в съответната организация, както е разгледано по-долу в точка „*Позиция на длъжностното лице по защита на данните в рамките на организацията*", по-долу.

[279] CEDPO, Choosing the best candidate as your Data Protection Officer (DPO) – Practical guidelines for organisations (Как да изберете най-добрия кандидат за длъжностно лице по защита на данните (ДЛЗД) – Практически насоки за организации) (бележка под линия 206, по-горе), стр.3.

да се отчита пред най-висшето ръководно ниво, като независимостта му да бъде гарантирана. Това изисква както „сериозност", така и лидерски умения.

Независимост

Вече отбелязахме, че "длъжностно лице по защита на данните може да бъде член на персонала на администратора или на обработващия лични данни или да изпълнява задачите въз основа на договор за услуги" (чл. 37, пар. 6). В нито един от случаите обаче това не е обикновена позиция на служител или изпълнител. По-специално, Регламентът подчертава, че:

> Тези служители по защита на данните, независимо от това дали са служители на администратора, следва да бъдат в състояние да изпълняват своите задължения и задачи **независимо**. (Съображение 97)

По-специално, Регламентът предвижда:

> Администраторът и обработващият лични данни правят необходимото **длъжностното лице по защита на данните да не получава никакви указания във връзка с изпълнението на тези задачи**. Длъжностното лице по защита на данните **не може да бъде освобождавано от длъжност, нито санкционирано от администратора или обработващия лични данни за изпълнението на своите задачи**. Длъжностното лице по защита на данните **се отчита пряко пред най-висшето ръководно ниво** на администратора или обработващия лични данни.
>
> (Чл. 38, пар. 3)

Работната група по член 29 разяснява това, както следва:[280]

> Горните разпоредби означават, че, при изпълнение на своите задачи по чл. 39, длъжностните лица по защита на данните не трябва да бъдат инструктирани как да процедират по даден въпрос, например, какъв резултат следва да бъде постигнат, как да разследват дадена жалба или дали да се консултират с надзорния орган. Освен това, те не трябва да бъдат инструктирани да възприемат определен възглед за въпрос, свързан с правото в областта на защитата на данните, например, конкретно тълкуване на правото.
>
> Независимостта на длъжностните лица по защита на данните обаче не означава, че те имат правомощия по вземане на решения, простиращи се отвъд техните задачи съгласно член 39.
>
> Администраторът или обработващият лични данни остава отговорен за спазването на законодателството в областта на защитата на данните и трябва да може да докаже спазване. Ако администраторът или обработващият лични данни вземе решения, които са несъвместими с ОРЗД и съвета на длъжностното лице по защита на данните, ДЛЗД следва да получи възможността да изрази своето особено мнение ясно за лицата, които вземат решенията.

Както е допълнително отбелязано в Част 3, съветът на длъжностното лице по защита на данните – и които и да е действия, предприети в разрез с този съвет – следва да бъдат записани и всяко пренебрегване на съвета може да бъде предявено срещу администратора или обработващия лични данни, във всяко последващо разследване от съответния орган по защита на данните. (Както е отбелязано по-рано, обратното –

---

280 Насоки за длъжностните лица по защита на данните на Работната група по член 29 (бележка под линия 209, по-горе), раздел 3.3, стр.14 – 15.

фактът, че даден администратор или обработващ лични данни е действал в съответствие с който и да е съвет или насока, издаден(а) от неговото длъжностно лице по защита на данните, може да представлява доказателство за спазването на ОРЗД (Съображение 77).[281]

Работната група по член 29 също пояснява обхвата на разпоредбата, че длъжностните лица по защита на данните „не може да бъдат освобождавани от длъжност, нито санкционирани от администратора или обработващия лични данни за изпълнението на своите задачи":[282]

> Това изискване затвърждава независимостта на ДЛЗД и спомага да се гарантира, че те действат независимо и се ползват с достатъчна подкрепа при изпълнението на техните задачи по защита на данните.
>
> Според ОРЗД санкционирането е забранено само ако се налага в резултат на изпълнението на задълженията на ДЛЗД в качеството му на ДЛЗД. Например ДЛЗД може да прецени, че дадено обработване би могло да доведе до голям риск и да посъветва администратора или обработващия лични данни да направи оценка на въздействието върху защитата на данните, но администраторът или обработващият лични данни да не е съгласен с оценката на ДЛЗД. В такъв случай ДЛЗД не може да бъде освободено от длъжност поради факта, че е дало този съвет.
>
> Санкционирането може да се извършва под най-различни форми и може да е пряко или непряко. То може да се състои например в отсъствието или забавянето на повишение; недопускането до кариерно развитие; лишаването от придобивки, каквито другите служители получават. Не е задължително тези санкции реално да бъдат наложени; само заплахата с такива е достатъчна, доколкото се използват за санкциониране на ДЛЗД на основания, свързани с неговите дейности като ДЛЗД.
>
> Като нормално управленско правило, какъвто би бил случаят с всеки друг служител или изпълнител съгласно приложимото национално договорно или трудово и наказателно право, ДЛЗД все пак може да бъде освободено от длъжност по законосъобразен начин по причини, различни от изпълнението на неговите задачи като ДЛЗД (например в случай на кражба, физически, психологически или сексуален тормоз или подобни груби прояви на лошо поведение).
>
> В този контекст следва да се отбележи, че в ОРЗД не е посочено как и кога ДЛЗД може да бъде освободено от длъжност или заменено с друго лице. Колкото по-стабилен е договорът на ДЛЗД обаче и колкото повече гаранции има срещу несправедливо освобождаване от длъжност, толкова е по-голяма вероятността да може да действа независимо. По тази причина Работната група по член 29 би приветствала полагането на усилия от организациите в тази насока.

Най-малкото, всеки договор или трудово правоотношение, предложен(о) на длъжностно лице по защита на данните, следва да включва клаузи, повтарящи разпоредбите за независимост в ОРЗД, или препращащи към тях. Трибуналите или съдилищата, произнасящи се по дела за уволнение, следва, разбира се, да вземат изцяло предвид разпоредбите на Регламента . При необходимост, е възможно да се измени трудовото законодателство. Държавите членки биха могли и да укрепят

---

281 Вж. раздел 2.4.2, по-горе.

282 Насоки за длъжностните лица по защита на данните на Работната група по член 29 (бележка под линия 209, по-горе), раздел 3.4, стр.15.

независимостта на длъжностни лица по защита на данните в други национални закони: примери за гаранции срещу уволнение на определени служители могат да бъдат намерени в закони, предоставящи специална защита, например за длъжностни лица в профсъюзи и/или изискващи одобрението на съветите на работниците и служителите за назначения и уволнение за определени длъжности.

БЕЛЕЖКА: Институционалните длъжностни лица по защита на данните на ЕС обсъждат въпросите на независимостта и конфликтите на интереси (следващият въпрос, разгледан в този Наръчник) основно от гледна точка на договорните, свързаните с продължителността на назначението и други гаранции, които са обсъдени по-късно в точка „*Позиция на длъжностното лице по защита на данните в рамките на организацията*" по-долу. CEDPO отбелязва, че организацията, която назначава длъжностното лице по защита на данните, следва да „обмисли … как да осигури независимостта на длъжностното лице по защита на данните".[283]

Конфликт на интереси

Както отбелязва Работната група по член 29:[284]

> Чл. 38, пар. 6 позволява на ДЛЗД да „изпълнява и други задачи и задължения". Той обаче изисква организацията да гарантира, че „тези задачи и задължения не водят до конфликт на интереси".
>
> Липсата на конфликт на интереси е тясно свързана с изискването да се действа по независим начин. Макар ДЛЗД да могат да имат други функции, също така може да им се възложат други задачи и задължения, само при условие, че същите не пораждат конфликт на интереси. Това води, по-специално до ситуация, при която ДЛЗД не може да заема позиция в рамките на организацията, в която то трябва да определи целите и начините на обработването на лични данни. Поради специфичната организационна структура във всяка организация, това трябва да се разглежда поотделно за всеки конкретен случай.
>
> Като по принцип, намиращите се в конфликт длъжности, могат да включват, длъжности във висшето ръководство (като главен изпълнителен директор, главен оперативен директор, главен финансов директор, главен медицински директор, началник на маркетингов отдел, началник на отдел Човешки ресурси и на отдел ИТ), както и други роли, разположени по-ниско в структурата на организацията, ако тези позиции или роли водят до определянето на целите и начините на обработване.
>
> В зависимост от дейностите, мащаба и структурата на организацията, може да е добра практика администраторите или обработващите лични данни:
>
> - да установят позициите, които биха били несъвместими с функцията на длъжностно лице по защита на данните
> - да съставят вътрешни правила в този смисъл, за да се избягват конфликти на интереси
> - да включат по-общо обяснение относно конфликта на интереси
> - да обявяват, че тяхното длъжностно лице по защита на данните няма конфликт на интереси във връзка със своята функция на длъжностно лице по

---

283 CEDPO, Choosing the best candidate as your Data Protection Officer (DPO) – Practical guidelines for organisations (Как да изберете най-добрия кандидат за длъжностно лице по защита на данните (ДЛЗД) – Практически насоки за организации) (бележка под линия 206, по-горе), стр.3.

284 Насоки за длъжностните лица по защита на данните на Работната група по член 29 (бележка под линия 209, по-горе), раздел 3.5, стр.15 – 16. Третият абзац („Като принципно правило …") се появява като бележка под линия в документа, а не в основния текст, както е тук.

защита на данните, като начин на повишаване на информираността за това изискване

- да включват гаранции във вътрешните правила на организацията и да гарантират, че уведомлението за вакантна позиция за ДЛЗД или договора за услуги е достатъчно точен и подробен, за да се избегне конфликт на интереси. В този контекст, следва да се има предвид и че конфликтът на интереси може да бъде в различни форми, в зависимост от това дали длъжностното лице по защита на данните е вътрешно или външно назначено.

Институционалните длъжностни лица по защита на данните на ЕС добавят:[285]

> Длъжностно лице по защита на данните следва да няма конфликт на интереси между задълженията си, като ДЛЗД и които и да е други официални задължения, по-специално във връзка с приложението на разпоредбите на Регламента (чл. 24, ал.3). Конфликт на интереси е налице, когато другите задължения, които едно ДЛЗД трябва да изпълнява, може да имат директно неблагоприятни последствия спрямо тези за защита на личните данни в рамките на същата институция. Ако е необходимо, длъжностното лице по защита на данните следва да отнесе този въпрос пред назначилия го орган.

Те обръщат по-подробно внимание на въпроса от гледна точка на договорни отношения, свързани с продължителността на назначението и други гаранции, както е отбелязано в следващата точка. CEDPO още веднъж отбелязва, че, ако назначението на длъжностното лице по защита на данните не е на пълен работен ден, организацията, която го назначава, следва да „обмисли … как да се справи [с] конфликта на интереси".[286]

Позиция на длъжностното лице по защита на данните в рамките на организацията

Йерархичната и договорна позиция на длъжностното лице по защита на данните в рамките на организацията е от решаващо значение във връзка с осигуряването на ефективност, независимост и избягването на конфликт на интереси на длъжностното лице по защита на данните.

От една страна, както е отбелязано по-рано, длъжностното лице по защита на данните следва да бъде „близко" до организацията, която обслужва (вж. по-горе, под точка „*Опит*"). Освен това, както посочва CEDPO:[287]

> За да бъде ефективно длъжностното лице по защита на данните, следва да бъде на място, което означава не само да е на разположение на различните заинтересовани лица в рамките на Вашата организация, но и активно да търси възможности за взаимодействие с различни отдели.

Това може да бъде проблемно в случай, когато е назначено външно длъжностно лице по защита на данните, действащо на основание на договор за услуги: по дефиниция то

---

285 Мрежа на длъжностните лица по защита на данните на институциите и структурите на ЕС, Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001 (Професионални стандарти за длъжностни лица по защита на данните на институциите и структурите на ЕС, работещи по Регламент (ЕО) 45/2001), (вж. бележка под линия 212, по-горе), стр.15.

286 CEDPO, Choosing the best candidate as your Data Protection Officer (DPO) – Practical guidelines for organisations (Как да изберете най-добрия кандидат за длъжностно лице по защита на данните (ДЛЗД) – Практически насоки за организации) (бележка под линия 206, по-горе), стр.3.

287 *Пак там*, стр.2.

няма да бъде част от структурата, която подпомага. В частния сектор е доста възможно да има – и в някои държави, като Германия, – външни длъжностни лица по защита на данните с обширни експертни познания и опит в частния сектор или под-сектор, в който работят. В публичния сектор, това може да е по-трудно, поради което в този сектор може да е по-препоръчително за по-малките структури да намерят ДЛЗД на друго място в същия сектор (както се предлага в раздел 2.3.2 по-горе, в точките „*Длъжностни лица по защита на данните за големи публични органи или групи от органи*" и „*Външни длъжностни лица по защита на данните*").

Винаги обаче има известно напрежение между необходимата „близост" на длъжностното лице по защита на данните до неговата организация, от една страна, и, от друга страна, необходимостта да се избягват конфликт на интереси и да се осигури на практика реалната независимост на ДЛЗД.

Както вече е отбелязано в становището на Работната група по член 29, това означава, че ДЛЗД не може да участва в определянето на целите и начините на обработването на лични данни и не може да заема висша ръководна длъжност, като главен изпълнителен директор или началник на главен отдел.[288]

Въпросът е разгледан много по-подробно от институционалните ДЛЗД на ЕС. Макар че техните възгледи трябва, разбира се, да се разглеждат в светлината на техния специфичен контекст, все пак е полезно да бъдат отбелязани. След като забелязват различни разпоредби в Регламента, които се отнасят до тях (Регламент (ЕО) 45/2001)[289] , и които са предназначени да гарантират тяхната независимост, те продължават, както следва:[290]

---

[288] Вж. по-горе, в точка „*Конфликт на интереси*", по-специално третия абзац в цитата от Насоките за длъжностни лица по защита на данните на Работната група по член 29. За разлика от тях, **италианският** орган по защита на данните, *Garante*, в своите Често задавани въпроси за длъжностните лица по защита на данните казва, че:

> … Чл. 38, пар. 3 предвижда, че длъжностното лице по защита на данните „се отчита пряко пред най-висшето ръководствона администратора или обработващия лични данни." Това изискване за пряко отчитане може да гарантира, по-специално, че висшето ръководство е информирано за насоките и препоръките, дадени от длъжностното лице по защита на данните, действащо в своето качество на консултант и лице, което повишава информираността спрямо администратора на данни или обработващия лични данни.
>
> Съответно, ако бъде определено вътрешно длъжностно лице по защита на данните, по принцип би било за предпочитане, да бъде избран ръководител на отдел или старши член на персонала, когато това е възможно, въз основа на организационната структура и като се взема предвид сложността на дейностите по обработване. По този начин, определеното длъжностно лице по защита на данните ще бъде в състояние да изпълнява своите задачи напълно автономно и независимо, както и като поддържа контакт директно с най-висшите ръководни нива.
>
> (*Garante*, Често задавани въпроси за длъжностните лица по защита на данните [бележка под линия 216, по-горе], раздел 2.)

Вероятно, най-добрият начин за съгласуване на възгледите на Работната група по член 29 и *Garante* в това отношение, би бил да се предложи длъжностното лице по защита на данните да бъде назначено *на нивото на* ръководител на отдел или старши ръководител, но без действително да е отговорен за дейностите по обработване на данни.

[289] Вж. бележка под линия 207, по-горе.

[290] Мрежа на длъжностните лица по защита на данните на институциите и структурите на ЕС, Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001 (Професионални стандарти за длъжностни лица по защита на данните на институциите и структурите на ЕС, работещи по Регламент (ЕО) 45/2001) (бележка под линия 13, по-горе), стр.6 – 7.

На практика обаче, може да е предизвикателство за длъжностното лице по защита на данните да изпълнява своите задължения при пълна независимост. Няма нужда да се отбелязва, че индивидуалното положение и личността на длъжностното лице по защита на данните ще имат значение, но може принципно да се допусне, че определени елементи може да отслабят позицията на длъжностното лице по защита на данните:

- Длъжностното лице по защита на данните на непълно работно време е изправено пред постоянен конфликт между разпределянето на времето си и усилията, които полага, за да изпълни своите задачи като ДЛЗД и други задачи. Що се отнася до напредването в кариерата и наблюдението върху изпълнението на задълженията, ръководството може да предвиди по-голяма тежест за дейностите, които не са свързани с функцията му на ДЛЗД. Това създава допълнително напрежение върху ДЛЗД да концентрира своите усилия върху задачите , които не са свързани с функцията му на ДЛЗД. Също така, длъжностното лице по защита на данните на непълно работно време е застрашено и от възникване на конфликт на интереси.

    - Длъжностното лице по защита на данните със срочен договор е по-вероятно да се окаже в по-слаба позиция да изпълнява своите задължения на ДЛЗД навременно в сравнение с ДЛЗД с постоянен договор (длъжностно лице или временен агент с безсрочен договор). Това е така, тъй като може да бъде притеснено за това как неговите действия биха могли да окажат отрицателно влияние върху подновяването на договора му. Ако ДЛЗД има кратък професионален опит, може да има затруднения да се изправи пред администраторите и може да бъде по-фокусирано върху собственото си кариерно развитие отколкото върху цялостното и навременно изпълнение на задълженията си.

    - Длъжностно лице по защита на данните, което се отчита пред и се контролира от непосредствения ръководител в йерархията (директор или началник на звено), може да усети натиск да сътрудничи и да се разбира с ръководството и другите колеги, като навременното изпълнение на задълженията му на ДЛЗД може да има отрицателно въздействие върху кариерата му. За да облекчи този натиск, ДЛЗД следва да се отчита на и да бъде контролирано от административния ръководител на институцията или структурата. Това е особено важно за длъжностни лица по защита на данните на непълно работно време, които следва да се отчитат директно пред и да се контролират от назначаващия орган за техните задължения като ДЛЗД, и съответно пред прекият началник в йерархията за другите задължения.

- Длъжностно лице по защита на данните, което трябва да поиска персонал и ресурси (ИТ ресурси, бюджет за командировки и обучение) от своя пряк началник може да срещне затруднения, ако последният не е напълно посветен на постигането на съответствие в сферата на защитата на данните. Това може да бъде избегнато, ако длъжностното лице по защита на данните носи отговорност за своя собствен бюджет и всякакви молби за допълнителни ресурси трябва да бъдат одобрявани от назначаващия орган.

Най-добрите практики, помагащи да се осигури независимостта на длъжностното лице по защита на данните, са:

- Институцията или структурата следва да установи позицията на длъжностното лице по защита на данните в рамките на организацията като

позиция на Консултант, Ръководител на звено или Директор и, във всеки случай, позицията на длъжностното лице по защита на данните следва да бъде официално призната като ръководно ниво в официалната органиграма на институцията/структурата;

- Институцията или структурата следва да назначи длъжностното лице по защита на данните за възможно най-дълъг срок, в светлината на договора на длъжностното лице по защита на данните. По този начин нормата би следвало да е назначение за петгодишен период, освен ако това е невъзможно при конкретните обстоятелства;
- Длъжностното лице по защита на данните следва да има постоянен договор/ договор с неопределен срок с институцията или структурата [и] следва да бъде достатъчно опитно (…);
- Длъжностното лице по защита на данните следва да бъде в състояние да посвети времето си изцяло на своите задължения като длъжностно лице по защита на данните, по-специално за големи институции и органи, и за по-малки такива в началната фаза на установяване на режим на защита на данните. Следва да бъде осигурена надлежна поддръжка от гледна точка на ресурси и инфраструктура. Задълженията, несвързани с функцията на длъжностно лице по защита на данните, на длъжностно лице по защита на данните на непълен работен ден следва да не представляват конфликт на интереси, или дори да приличат на конфликт, със задълженията на длъжностното лице по защита на данните като такова;
- Длъжностните лица по защита на данните в организации, в които дейностите по обработване на данни са основната дейност на организацията, обичайно ще изискват различни членове на персонала. Следва да се осигури такъв капацитет на персонала;
- Следва да има правила в рамките на организацията, които да гарантират задължението на всички членове на персонала да сътрудничат на ДЛЗД без да трябва да чакат нареждане или разрешение на техния ръководител;
- Длъжностното лице по защита на данните следва да се отчита през ръководителя на институцията или структурата, който следва да отговаря за контрола върху изпълнението от ДЛЗД на задълженията му, установени от Регламента. Лицето, отговарящо за контрола на изпълнението на ДЛЗД, следва да бъде внимателно към нуждата на ДЛЗД да заема силни позиции, които другите в организацията може и да не оценят. Длъжностното лице по защита на данните не следва да търпи неблагоприятни последствия заради изпълнението на задълженията си. Назначаващият орган следва да гарантира, че докато ДЛЗД заема тази длъжност, то се ползва от „нормално" кариерно развитие. При осъществяване на преглед на изпълнението на задълженията и задачите на ДЛЗД, оценяващото лице следва да внимава, както да не порицава длъжностното лице по защита на данните за заемането на непопулярни позиции, така и да не счита изискванията за защита на данните за административна тежест. За длъжностно лице по защита на данните на непълен работен ден, изпълнението на задълженията като такова следва да има същата тежест като изпълнението на задълженията, несвързани с изпълнението на функциятаму;
- Длъжностното лице по защита на данните следва да има своя собствена бюджетна линия, създадена в съответствие с правилата и процедурите на

съответната институция/орган; неговите молби за допълнителни ресурси следва да подлежат на одобрение от административния ръководител. Други договорености са приемливи, само ако предоставят на ДЛЗД ресурсите, от които се нуждае, за да изпълнява своите задължения по независим начин;

- Длъжностното лице по защита на данните следва да има право да полага подпис за кореспонденция във връзка със защитата на данните.

Органите по защита на данните може да счетат за подходящо и да издадат подробни насоки в този смисъл, по описаното в горните редове.

Ресурси и съоръжения

ОРЗД предвижда, че:

> Администраторът и обработващият лични данни подпомагат длъжностното лице по защита на данните при изпълнението на посочените в член 39 задачи [изброени в раздел 2.5.4, по-долу от тази точка], като осигуряват **ресурси, необходими за изпълнението на тези задачи**, и достъп до личните данни и дейностите по обработване, а така също поддържат неговите експертни знания.
>
> (Чл. 38, пар. 2)

В това отношение, Работната група по член 29 препоръчва, по-специално, следното:[291]

- Активно подпомагане на функцията на длъжностното лице по защита на данните от страна на висшето ръководство (като ниво съвет на директорите/управителен съвет).
- Достатъчно време на длъжностните лица по защита на данните, за да изпълняват своите задължения. Това е особено важно, когато ДЛЗД е назначено на непълно работно време или когато служителят изпълнява задължения по защита на данните в допълнение към други задължения. В противен случай, противоречащите си приоритети биха могли да доведат до пренебрегване на изпълнението на задълженията на длъжностното лице по защита на данните. Наличието на достатъчно време, което да бъде посветено на задачите на ДЛЗД е от първостепенна важност. Добра практика е да се установи процент от времето за функцията на ДЛЗД, когато тя не се изпълнява на пълен работен ден. Също така е добра практика да се определи времето, което е необходимо за изпълнението на функцията, подходящото ниво на приоритет за задълженията на длъжностното лице по защита на данните и за същото (или организацията) да състави работен план.
- Адекватна подкрепа от гледна точка на финансови ресурси, инфраструктура (помещения, съоръжения, оборудване) и персонал, където е подходящо.
- Официално съобщение за определянето на длъжностното лице по защита на данните до целия персонал, за да се гарантира, че в организацията знаят за съществуването и функцията му.
- Необходим достъп до други служби, като Човешки ресурси, правна, ИТ, сигурност и т.н., така че длъжностните лица по защита на данните да могат да получат съществена подкрепа, сътрудничество и информация от тези други отдели.
- Постоянно обучение. [Вж. по-горе, в точка „*Обучение и сертифициране*"]
- С оглед на размера и структурата на организацията, може да е необходимо да се създаде екип на длъжностното лице по защита на данните (ДЛЗД и негови

[291] Насоки за длъжностните лица по защита на данните на Работната група по член 29 (бележка под линия 13, по-горе), раздел 3.2, стр.13 – 14.

служители). В такива случаи, вътрешната структура на екипа и задачите на всеки от неговите членове следва да бъдат ясно посочени. Също така, когато функцията на длъжностното лице по защита на данните се упражнява от външен доставчик на услуги, екип от лица, работещи за този субект, може ефективно да изпълнява задачите на ДЛЗД-екипа, на отговорност на определено водещо лице за контакт за клиента.

Като цяло, колкото по-сложни и/или чувствителни са дейностите по обработване, толкова повече ресурси трябва да бъдат дадени на длъжностното лице по защита на данните. Функцията по защита на данните трябва да бъде ефективна и обезпечена с достатъчно ресурси във връзка с извършваното обработване на данни.

Както вече беше посочено, институционалните длъжностни лица по защита на данните на ЕС считат, че „длъжностно лице по защита на данните, което трябва да поиска персонал и ресурси (ИТ ресурси, бюджет за командировки и обучение) от своя пряк началник може да срещне затруднения, ако последният не е напълно посветен на постигането на съответствие в сферата на защитата на данните." Поради това, те препоръчват длъжностното лице по защита на данните да получи своя собствена бюджетна отговорност, като всички отправяни молби за допълнителни ресурси трябва да бъдат одобрени от назначаващия орган (а не от този пряк началник).[292]

CEDPO отбелязва:

[В] сложни организации, Вие ще трябва да мислите дали длъжностното лице по защита на данните ще получава или няма да получава помощ от други хора вътрешно, които ще допълват уменията му, постоянно (екипа на длъжностното лице по защита на данните) или според нуждите от време на време (външен консултант?).

В публичните органи създаване на екип би било наистина препоръчително. В малките публични органи, той би могъл да се състои просто от редовни срещи на съществуващия персонал с длъжностното лице по защита на данните за обсъждане на свързани въпроси и подготовка на вътрешни политики. В по-големите такива, на някои служители могат формално да им бъдат възложени функции по подпомагане на длъжностното лице по защита на данните на непълен работен ден. В определени органи, може да е необходимо да се назначат лица на пълен работен ден, които да подпомагат длъжностното лице по защита на данните. Както изясняват всички документи с насоки, решенията по тези въпроси следва да бъдат взети в светлината на (i) сложността на чувствителността на дейностите по обработване на лични данни, (ii) мащабите и ресурсите на въпросния субект. Но в крайна сметка ОРЗД съдържа законово изискване ресурсите, разпределени на длъжностното лице по защита на данните (и екипа му), да са достатъчни за поетите задачи.

Правомощия на длъжностното лице по защита на данните

Освен ресурсите и достатъчно силната, защитена и високо разположена позиция в рамките на организацията, длъжностното лице по защита на данните е необходимо да има и правомощието да изпълнява своите задачи. Чл. 38, пар. 2 (цитиран в предходната точка) ясно посочва, че заради това субектът, назначаващ длъжностното лице по защита

[292] Вж. по-горе, в точка *„Позиция на длъжностното лице по защита на данните в рамките на организацията*".

на данните, трябва да гарантира, то да има „достъп" до лични данни и дейности по обработването. Това следва да се разбира по същия начин, както съответстващата разпоредба в Регламента относно институционалните длъжностни лица по защита на данните на ЕС, чл. 24, пар. 6 от Регламент (ЕС) 45/2001, се разбира следното:[293]

> Регламентът изисква администраторите да съдействат на длъжностното лице по защита на данните при изпълнението на неговите задължения и да дават информация в отговор на въпроси, и посочва, че длъжностното лице по защита на данните трябва да има достъп във всеки един момент до данните, формиращи предмета на дейности по обработване, и до всички офиси, инсталации за обработване на данни и носители на данни.
>
> Въпреки че длъжностното лице по защита на данните няма право да пристъпва към изпълнение спрямо администратори, то има правомощие да наблюдава спазването, като събира всички относими данни, които назначаващата институция/ структура и нейните администратори са задължени да предоставят.

От значение са и други коментари от институционалните длъжностни лица по защита на данните на ЕС във връзка със задължението на ДЛЗД да осигури спазване на правилата в областта на защитата на данните:[294]

> Може да бъдат разработени ИТ инструменти, които да подпомагат длъжностното лице по защита на данните при изпълнението на редовно наблюдение. Могат да се сключат и административни договорености, като такива, които гарантират, че длъжностното лице по защита на данните получава копие от всички писма, сезиращи за проблеми във връзка със защитата на данните и изискващи консултиране с длъжностното лице по защита на данните по документи, в които се повдигат проблеми в областта на защитата на данните. Внимателното редовно наблюдение на спазването и отчитането на резултатите може да създаде силен натиск върху администраторите да осигурят съответствието на своите дейности по обработване. Поради това, редовното наблюдение и отчитане са най-силните инструменти на длъжностното лице по защита на данните за осигуряване на спазването. В този смисъл, е добра практика провеждането на годишно прочуване/доклад, отнесен до ръководството.

Специални въпроси възникват, когато администратор или обработващ лични данни откаже да следва съвета на своето длъжностно лице по защита на данните. Според думите на Работната група по член 29:[295]

---

[293] Мрежа на длъжностните лица по защита на данните на институциите и структурите на ЕС, Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001 (Професионални стандарти за длъжностни лица по защита на данните на институциите и структурите на ЕС, работещи по Регламент (ЕО) 45/2001) (бележка под линия 13, по-горе), стр.12. Отбележете, че, за разлика от чл, 38, пар. 2 от ОРЗД, чл. 24, пар. 6 от Регламент (ЕО) 45/2001 всъщност не споменава изрично достъпът до лични данни и дейности по обработване на лични данни. Ето защо, това се чете, в горния контекст, в по-общата разпоредба относно предоставянето на необходимите ресурси. Може да се предположи, че това е повлияно от по-специфичната, силна разпоредба за даване на достъп до такава информация (в рамките на институциите на ЕС) на Европейски надзорен орган по защита на данните.

[294] *Вж*.

[295] Насоки за длъжностните лица по защита на данните на Работната група по член 29 (бележка под линия 13, по-горе), стр.15. Същият подход е възприет от Мрежа на длъжностните лица по защита на данните на институциите на ЕС, вж. отново Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001 (Професионални стандарти за длъжностни

> Ако администраторът или обработващият лични данни взема решения, които са несъвместими с ОРЗД и съвета на длъжностното лице по защита на данните, ДЛЗД следва да има възможност да направи ясно своето мнение пред висшето ръководство и пред отговорните лица, които вземат решенията. В тази връзка, чл. 38, пар. 3 предвижда, че длъжностното лице по защита на данните „се отчита пряко пред най-висшето ръководно ниво на администратора или обработващия лични данни." Това пряко отчитане гарантира, че висшето ръководство (напр. съветът на директорите) е запознато със съвета и препоръките като част от задълженията на длъжностното лице по защита на данните да информира и съветва администратора или обработващия лични данни. Друг пример за пряко отчитане е изготвянето на годишен доклад за дейностите на длъжностното лице по защита на данните, предоставян на най-висшето ръководно ниво.

Макар да няма изрично задължение, предвидено в ОРЗД за длъжностното лице по защита на данните, да съобщава на органите за неспазване на закона, ОРЗД предвижда, че това е една от задачите на длъжностното лице по защита на данните:

> да действа като точка за контакт за надзорния орган по въпроси, свързани с обработването, … , и **по целесъобразност да се консултира** по всякакви други въпроси (чл. 39, пар. 1, б. „д"), добавено удебеляване)

Поради това, в случаи, в които длъжностно лице по защита на данните е почувствало, че служител е действал в нарушение на закона, то има правото – и всъщност – бихме казали – задължението – да повдигне въпроса пред националния орган по защита на данните, за да се разреши въпросът. Това демонстрира деликатността на позицията.

В същото време, както Работната група по член 29 правилно подчертава:[296]

> Автономията на длъжностните лица по защита на данните обаче не означава, че те имат правомощия за вземане на решения, простиращи се извън задачите им по член 39.
>
> Администраторът или обработващият лични данни остават отговорни за спазването на правото в областта на защитата на данните и трябва да може да докаже спазването на Регламента.

Формалности

Всички посочени по-горе изисквания и др. за длъжностното лице по защита на данните, следва да бъдат ясно отразени в правния акт, с който то се назначава. Както посочва италианският орган по защита на данните, *Garante della Privacy*, в своите Често задавани въпроси за длъжностните лица по защита на данните:[297]

> Чл. 37, пар. 1 от ОРЗД предвижда, че администраторът на данни или обработващият лични данни определят длъжностно лице по защита на данните. Съответно, съществуването на инструмент, определящ длъжностното лице по

лица по защита на данните на институциите и структурите на ЕС, работещи по Регламент (ЕО) 45/2001) (бележка под линия 13, по-горе), стр. 12 (вж. абзаца, следващ цитирания в текста по-горе).

[296] WP29 Насоки за длъжностните лица по защита на данните (бележка под линия 209, по-горе), стр.15, по отношение на принципа на „отчетност" в Чл. 5, пар. 2 от ОРЗД.

[297] *Garante*, Често задавани въпроси за длъжностните лица по защита на данните (бележка под линия 216, по-горе), раздел 1. *Garante* е приложило **формуляр образец за [назначаване на длъжностно лице по защита на данните]** към Често задаваните въпроси за улеснение. „**Образец на формуляр за изпращане на данните на длъжностното лице по защита на данните на Garante**" също е предоставен.

защита на данните е неразделна част от всяка договореност за изпълнение на съответното задължение.

Ако кандидатът за длъжностно лице по защита на данните е част от персонала, ще трябва да се състави ad-hoc инструмент, за определянето му като ДЛЗД. Обратното, ако бъде избран външен субект, формалното определяне на това лице за ДЛЗД ще бъде неразделна част от ad-hoc договор за услуги, който ще бъде изготвен съгласно чл. 37 от ОРЗД.

Независимо от естеството и вида на правния акт, последният трябва да посочва недвусмислено кое ще бъде длъжностното лице по защита на данните, като се запише името му, поетите задачи (които могат да се простират и извън предвидените в чл. 39 от ОРЗД) и задълженията, свързани с подпомагането, което длъжностното лице по защита на данните се очаква да предоставя на администратора на данни/обработващия лични данни съгласно приложимата законова и регулаторна рамка.

Ако са възложени допълнителни задачи на длъжностното лице по защита на данните освен тези, посочени първоначално в инструмента за назначаване, последният или договорът за услуги ще трябва да бъде съответно изменен и/или допълнен.

Инструментът за назначаване и/или договорът за услуги следва да посочват също така, накратко, причините даденото физическо лице да бъде назначено за длъжностно лице по защита на данните от публичната структура или орган, така че да може да се установи спазване на изискванията по чл. 37, пар. 5 от ОРЗД; в тази връзка, може да бъде направено препращане към резултата от процедурата по вътрешен или външен подбор. Посочване на критериите, приложени преди назначаването на определен кандидат не е просто индикация за прозрачност и добра администрация, но е и елемент, който се взема предвид при оценката на спазването на принципа за „отчетност".

След като е назначил длъжностното лице по защита на данните, администраторът на данни или обработващият лични данни трябва да включи данните за контакт на длъжностното лице по защита на данните в информацията, предоставяна на субектите на данни, и – също така – да публикува тези данни на съответния(те) уебсайт(ове); съобщаването на данните на Garante също се изисква съгласно чл. 37, пар. 7. Що се отнася до публикуването на уебсайта, може да е подходящо да се публикуват данните за контакт на длъжностното лице по защита на данните в секцията „прозрачност" или „откритост" на сайта, както и на страницата „неприкосновеност на личните данни" – където има такава.

Както е изяснено в Насоките [на Работната група по член 29], не е необходимо да се публикува името на длъжностното лице по защита на данните съгласно чл. 37, пар. 7; това обаче може да е добра практика в публичния сектор. Обратното, данните за контакт трябва да бъдат предоставени на Garante, за да се улесни взаимодействието. От друга страна, данните за контакт на длъжностното лице по защита на данните трябва да бъдат съобщени на субектите на данни в случай на нарушение на сигурността на личните данни (вж. чл. 33, пар. 3, б. „б")).

2.5.4 Функции и задачи на длъжностното лице по защита на данните (Обзор)

Във връзка с институционалните длъжностни лица по защита на данните на ЕС, Европейският надзорен орган по защита на данните е разграничил следните **седем функции на длъжностното лице по защита на данните**:[298]

- Функция повишаване на информираността и осведомеността;
- Консултативна функция;
- Организационна функция;
- Функция по сътрудничество;
- Функция по наблюдение на съответствието;
- Обработване на запитвания или жалби; и
- Функция по прилагане.

Длъжностните лица по защита на данните, назначени съгласно ОРЗД, изпълняват до голяма степен сходни функции. Те се свързват с редица по-специфични **задачи**, формулирани в чл. 39 от ОРЗД, както следва:

Член 39

Задачи на длъжностното лице по защита на данните

1. Длъжностното лице по защита на данните изпълнява най-малко следните задачи:

(а) да информира и съветва администратора или обработващия лични данни и служителите, които извършват обработване, за техните задължения по силата на настоящия регламент и на други разпоредби за защитата на данни на равнище Съюз или държава членка;

(б) да наблюдава спазването на настоящия регламент и на други разпоредби за защитата на данни на равнище Съюз или държава членка и на политиките на администратора или обработващия лични данни по отношение на защитата на личните данни, включително възлагането на отговорности, повишаването на осведомеността и обучението на персонала, участващ в дейностите по обработване, и съответните одити;

(в) при поискване да предоставя съвети по отношение на оценката на въздействието върху защитата на данните и да наблюдава извършването на оценката съгласно член 35;

(г) да си сътрудничи с надзорния орган;

(д) да действа като точка за контакт за надзорния орган по въпроси, свързани с обработването, включително предварителната консултация, посочена в член 36, и по целесъобразност да се консултира по всякакви други въпроси.

2. При изпълнението на своите задачи длъжностното лице по защита на данните надлежно отчита рисковете, свързани с дейностите по

[298] Европейски надзорен орган по защита на данните, Position paper on the role of Data Protection Officers in ensuring effective compliance with Regulation (EC) 45/2001 (Становище относно ролята на Длъжностните лица по защита на данните при осигуряването на ефективно спазване на Регламент (ЕО) 45/2001) (бележка под линия 210, по-горе), стр.6 – 7.

обработване, и се съобразява с естеството, обхвата, контекста и целите на обработката.

На практика, длъжностните лица по защита на данните по естествен път ще бъдат включени и в определени задачи, които се възлагат от техния администратор, тъй като повечето администратори (освен ако самите те нямат съответен, задълбочен експертен опит и умения извън позицията на тяхното длъжностно лице по защита на данните, напр., в техния правен отдел или отделът за осигуряване на съответствие) ще търсят помощта на своето ДЛЗД при изпълнението на тези задачи. Всъщност, това е смекчено представяне на нещата: в много случаи администратори, изправени пред своите нови, натоварващи отговорности по ОРЗД (по-специално по новите задължения за отчетност/доказване на спазване) ще се обърнат към своето длъжностно лице по защита на данните да извърши голяма част от съответната работа, дори ако, както ОРЗД изрично посочва в различни аспекти, по закон администраторът, а не длъжностното лице по защита на данните, е този, който ще носи отговорност за каквито и да е несъответсвия в това отношение.

По-специално, както изяснява чл. 5, пар. 2 от ОРЗД:

> *Администраторът* носи отговорност и е в състояние да докаже спазването на [различните изисквания на ОРЗД]

С други думи, тази отговорност не е прехвърлена на длъжностното лице по защита на данните – както става ясно и от чл. 39, цитиран по-рано, който подчертава консултативните и подпомагащи задачи на длъжностното лице по защита на данните.

Длъжностното лице по защита на данните обаче все пак има решаващо значение в това отношение, тъй като то трябва, чрез своя съвет, да даде възможност на висшето ръководство и на по-ниско разположените в йерархията служители да изпълняват своите съответни задължения. Обратното, ръководители на висши и по-ниски позиции имат задължение да се консултират с длъжностното лице по защита на данните, ако възникнат проблеми във връзка със спазването на ОРЗД.

Европейският надзорен орган по защита на данните е предоставил полезна, така наречена матрица RACI ("**R**esponsible, **A**ccountable, **C**onsulted, **I**nformed") в тази връзка, приложима по-специално във връзка с воденето на архивите/регистъра с дейности по обработване на лични данни:[299]

	Отговорен	Подотчетен	Съветващ	Информиран
Висше ръководство		**X**		

[299] Европейски надзорен орган по защита на данните, Accountability on the ground Part I: Records, Registers and when to do Data Protection Impact Assessments (Отчетност на основание на Част I: Документация, регистри и кога да се правят оценки на въздействието върху защитата на данни, февруари 2018 г., стр.4, може да се намери на: https://edps.europa.eu/sites/edp/files/publication/18-02-06_отчетност_on_the_ground_part_1_en_0.pdf
Би могло да се добави колона, „Субекти на данни" и „Орган по защита на данните", с „Xs" за тях в последната колона („Информиран"), но съответните задължения са всъщност по-сложни отколкото би могло да се отбележи по този начин: субектите на данни трябва да бъдат информирани за определени въпроси в много случаи (било то от администратора по негова собствена инициатива или при поискване), но не винаги за всичко, и в някои случаи трябва не просто да бъдат информирани органите по защита на данните, но действително да се извърши консултация с тях. Във всеки случай, матрицата има за цел да разясни въпроси в рамките на организацията на администратора, а не във връзка с външни субекти.

Отговорник за дейността	**X**			
Длъжностно лице по защита на данните			**X**	
ИТ отдел			**X**	
Обработващ лични данни, където е необходимо			**X**	

Той добавя следните разяснения на термините:[300]

> „**Отговорен”** означава имащ задължението да действа и да взема решения да постигне необходимите резултати; „**Подотчетен”** означава да бъде отговорен за действия, решения и изпълнение; „**Съветващ”** означава да се иска от от него съдействие и предоставяне на насоки ; „**информиран”** означава да бъде държан в течение за взети решения и за процесите

Европейският надзорен орган по защита на данните използва термина „**отговорник за дейността**” за лицето, отговарящо, на практика и ежедневно, за съответните дейности по обработване: или иначе казано, „отговорникът” за процеса. Както е разяснено допълнително по-долу, в точката „*Предварителна задача*”, част от първите задължения на ДЛЗД е да планира тези вътрешни разпределения на отговорностите.

В съответствие с посоченото по-горе, в обзора на задачите на длъжностните лица по защита на данните по-долу, тези задачи често ще бъдат описвани като „помагане на администратора да гарантира” различни въпроси или като „съветване на администратора” (или съответния „отговорник за дейността”/отговорен член на персонала) как да постигне определени цели, а не като „осигуряване” на тези въпроси или диктуване как следва да бъдат третирани те. На практика, особено в малки организации, е възможно самото длъжностно лице по защита на данните да носи голяма част от някои от тези тежести, но обичайно те остават отговорност на администратора (и вътрешно, на съответния „отговорник за дейността”/отговорен член на персонала).

От горното, и като се има предвид това *възражение* за неотговорността на ДЛЗД, ние извеждаме **петнадесет задачи на длъжностното лице по защита на данните, или които на практика пряко го засягат** (плюс *Предварителна задача*), които могат да бъдат групирани в седем функционални направления, установени от Европейския надзорен орган по защита на данните, както е посочено в началото на заключителната част на този наръчник, Част 3.

Достатъчно е да се отбележи тук, че тези функции и задачи, на свой ред, са явно и силно свързани с „**принципа на отчетност**” и посочените „**задължения да се докаже спазване**”, наложени на администратора, които са обсъдени, по-рано, в раздел 2.4 от този наръчник.

В следващата част от този наръчник (Част 3), ние предоставяме насоки как администратора и длъжностното лице по защита на данните следва да изпълняват тези задължения . На първо място, обаче, е важно да се повтори, че – макар че ДЛЗД да има

[300] *Вж.*, бележка под линия 7 (подчертаване с удебелен шрифт добавено).

голямо влияние и принос във връзка с горните задачи, то не носи никаква лична формална отговорност за спазване на ОРЗД.

Разбира се, длъжностното лице по защита на данните ще трябва да установи стратегия, за да бъде в състояние да изпълни всички задачи съгласно годишна или полугодишна програма с известна гъвкавост по отношение на възникването на евентуални неочаквани проблеми (както внезапен проблем със защитата на данните или нарушение на сигурността на личните данни, засягащо организацията, или решение на органа по защита на данните да разследва съответната организация).

- o – O – o –

ЧАСТ ТРИ

Практически насоки за задачите на длъжностното лице по защита на данните или които на практика ще изискват участие на длъжностното лице по защита на данните

(„Задачи на длъжностното лице по защита на данните")

Тази част от наръчника се стреми да предостави практически насоки относно **задачите на длъжностното лице по защита на данните, или които на практика ще изискват участието на длъжностното лице по защита на данните,** вече изброени в раздел 2.5.4, по-горе, и отново изложени по-долу. С цел краткост, ние ще ги наричаме „Задачи на длъжностното лице по защита на данните". Както е отбелязано в този раздел, изведени са петнадесет задачи от списъка със задачи, широко формулиран в чл. 39 от ОРЗД, които са групирани в **седемте функции на длъжностното лице по защита на данните**, установени от Европейският надзорен орган по защита на данните. В различните раздели, обсъждащи задачата, ние предоставяме илюстриращи ги **примери**, които са свързани с реалната практика.

Задачи на длъжностното лице по защита на данните:

Предварителна задача:

Определяне на обхвата на дейностите на администратора

Организационни функции:

Задача 1: Създаване на дейностирегистър на дейностите по обработване на лични данни

Задача 2: Преглед на дейностите по обработване на лични данни

Задача 3: Оценка на рисковете, предизвикани от дейностите по обработването на лични данни

Задача 4: Работа с дейности, които е вероятно да породят „висок риск": извършване на Оценка на въздействието върху защитата на данните (ОВЗД)

Функции по наблюдение на съответствието:

Задача 5: Повторение на задачи 1 – 3 (и 4) на текуща база

Задача 6: Справяне с нарушения на сигурността на личните данни

Задача 7: Задача за разследване (включително обработването на вътрешни и външни жалби)

Консултативни функции:

Задача 8: Консултативна задача – общи положения

Задача 9: Подпомагане и насърчаване на „Защита на данните на етапа на проектирането и по подразбиране"

Задача 10: Съветване и извършване на мониторинг на спазването на политиките за защита на данните, на договори между съвместни

администратори, между администратори и между администратор и обработващ лични данни, на Обвързващи корпоративни правила и клаузи за предаване на данни

Задача 11: Участие в кодекси за поведение и системи за сертифициране

Сътрудничество и консултиране с органа по защита на данните:

Задача 12: Сътрудничество с органа по защита на данните

Разглеждане на молби на субекти на данни:

Задача 13: Разглеждане на заявки и жалби на субекти на данни

Информация и повишаване на осведомеността:

Задача 14: Задачи за информиране и повишаване на осведомеността

Задача 15: Планиране и преглед на дейностите на длъжностното лице по защита на данните

Предварителна задача:

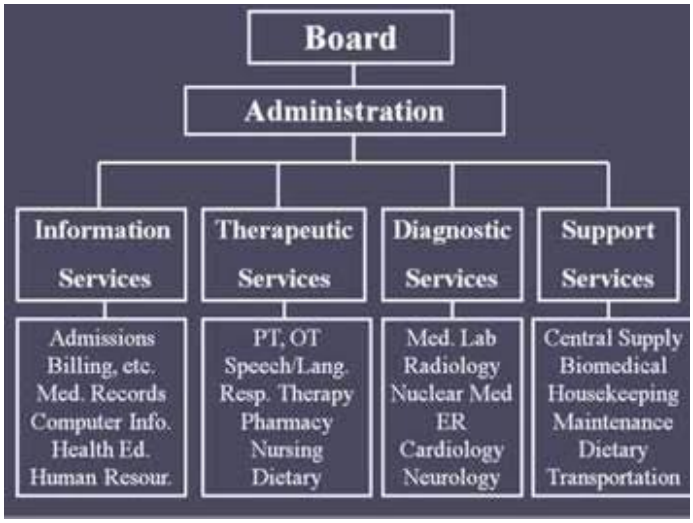
Предварителна задача на длъжностното лице по защита на данните: определяне на обхвата на средата на администратора и в общи линии очертаване на дейностите по обработване на организацията

Длъжностното лице по защита на данните може да изпълнява задачите си във връзка със своя работодател, само ако е напълно наясно с (i) **вътрешното** разпределение на задачите и отговорностите във връзка с (или които може да включват) каквото и да е обработване на лични данни; (ii) **външните** връзки и договорености на тази организация с други организации; и (iii) **правната(ите)** им рамка(и).

Преди да се заеме с основните си други задачи – с изключение на извършването на първоначалния опис (регистър) на дейности по обработване на лични данни, изброен на първо място в следващата точка (Задача 1), който може да бъде направен успоредно – длъжностното лице по защита на данните трябва да състави карта на вътрешните и външните връзки и линии на отговорност с всяка дейност по обработване на лични данни и да ги постави в по-широкия контекст на ролята и целите на организацията ,както и да се запознае задълбочено със съответните вътрешни правила.

За да изясни **вътрешните** структури и роли, длъжностното лице по защита на данните трябва, преди всичко, да получи и проучи **органиграмата** на неговата организация, която ръководството следва да му предостави.

ПРИМЕР: Органиграма на болница



Източник: *Principles of Health Science*, https://www.youtube.com/watch?v=FpQEwbAV3Qw

Органиграмите обичайно ще посочат само най-общо съответните звена и отдели: „човешки ресурси", „финанси и счетоводство", „правен отдел", „управление на клиенти" и т.н. (като много публични структури възприемат терминологията на частните субекти, напр. наричайки лицата, претендиращи за социални плащания „клиенти" на социалната служба). Те са полезна отправна точка, но не повече от това. В по-задълбочени обсъждания с висшето ръководство, включително директора(ите) по правните въпроси и по ИКТ на организацията и, когато е уместно, регионалните или националните офиси, длъжностното лице по защита на данните следва да изясни в повече подробности за какво точно отговарят различните звена и отдели, включително по-специално за какви цели всяко от звената и отделите се нуждае от, и реално обработва, лични данни; при какво устройство на вътрешните и външните технологии се извършва това; и дали то включва някакви външни технологични услуги или средства (включително облачно изчисление). Ето тук предварителното определяне на обхвата се припокрива с извършването на описа на дейности по обработване на лични данни в Задача 1 – но на предварителния етап, съответните дейности по обработване на лични данни трябва само да бъдат идентифицирани в по-широки граници, с оглед на целта за всяка такава операция и използваните технологии. Освен това, длъжностното лице по защита на данните следва в тази предварителна фаза да добие първоначална идея, какви точно **задачи** и **отговорности** има всяко звено или отдел по отношение на всяка операция с лични данни – т.е. то следва да установи кой е „**отговорникът за дейността**" за всяка операция (според терминологията на Европейския надзорен орган по защита на данните).

ПРИМЕРИ:[301]

Испанският орган по защита на данните, AEDP, изброява следното като **примери за официални (изискуеми по закон) регистри на лични данни, поддържани от местни органи**:

- Регистър на населението

[301] Базирани на: *Protección de Datos y Administración Local* (Защита на данните и местна администрация) секторен наръчник, издаден от испанския орган по защита на данните, AEPD, 2017 г., стр.8 (наш превод и редакция), наличен на: https://www.aepd.es/media/guias/guia-proteccion-datos-administracion-local.pdf

- Регистър на лицата, дължащи местни данъци
- Регистър на получателите на помощи (напр., помощ за настаняване или помощ за инвалидност)
- Регистър на клиентите на социалните служби (напр., закрила на детето)
- Регистри на налагането на глоби (напр., глоби за паркиране)
- Регистър на издадените разрешения и лицензи (напр., за бар)
- Регистър на местните полицейски звена и служители
- Регистър на хората, регистрирали се в местните бюра по труда;
- Регистър на децата в местната образователна система
- Регистър на лицата с издадени официални документи (напр., раждания, бракове, смърт)
- Регистър на лицата, погребани в местните гробища
- Регистър на ползвателите на библиотеки, водени от местните власти
- Регистър на лицата, регистрирали се да получават уведомления за културни събития

Както, разбира се:

- Счетоводство
- Човешки ресурси
- И други

Органът по защита на данните предоставя следните **примери за закони или регламенти, уреждащи обработването на лични данни във връзка с някои от регистрите на лични данни, водени от испанските местни органи**, посочени по-горе: [302]

Регистър:	Уреждащ закон/подзаконов акт:
• Регистър на населението	Закон за местните регистри на населението
• Регистър на лицата, дължащи местни данъци	Закон за местните заведения
• Данни за човешки ресурси	Подзаконови актове, уреждащи тази дейност

При някои обстоятелства, може да има други законови основания за обработването, напр.:

Регистър:	Други правни основания:
• Регистър на лицата, регистрирали се за културни събития	Съгласие и местен подзаконов акт
• Регистър на ползвателите на библиотеки на местните власти	Договор и местен подзаконов акт

В допълнение към това, е важно на всеки етап длъжностното лице по защита на данните (с помощта на ИТ специалистите и служителите по сигурността) също да се запознае задълбочено с **технически ИКТ системи, устройствени правилници и политики на неговата организация**: използваните компютри (или където те все още се използват – системите за ръчно подаване) и дали сред тях има портативни и/или мобилни

302 AEPD, Секторен наръчник за защита на данните и местна администрация (предходна бележка под линия), стр.11.

устройства (и/или лични „собствени устройства" на съответните служители – за които трябва да съществува [да бъде въведена] политика за носене на собствено устройство (Bring Your Own Device [BYOD]); дали компютри или устройства се използват онлайн или само офлайн, на място или/ и извън службата; какъв софтуер за сигурност и криптиране се използва, и дали той е напълно актуален; какви са външните връзки и съоръжения (включително използването на облачни сървъри, по-специално, ако същите са базирани извън ЕС/ЕИП, напр., в САЩ – в който случай трябва да бъдат проверени съответните мерки и договори за трансфер на данни); дали някаква част от обработването се извършва от обработващи лични данни (в който случай договорите с тях ще трябва да бъдат прегледани);[303] какви са мерките за физическа сигурност (врати, стаи, пароли за мрежи и компютри и т.н.); дали има политики и обучение за сигурност; и т.н. и т.н. На този предварителен етап тези многобройни въпроси не трябва да бъдат разглеждани и разрешавани – но те следва поне да бъдат **отбелязани, описани и записани**.

На следващо място, длъжностното лице по защита на данните следва да се опитва да изясни всички **външни** връзки, които организацията му има с други организации. Те принципно са **три типа**: (а) организации (дъщерна/главна/партньорска), с които организацията на длъжностното лице по защита на данните има формални връзки, в рамките на онова, което (в публичния сектор) обичайно ще бъде обща **йерархична рамка**. Местната власт може официално да бъде под непосредствената юрисдикция на регионален орган, който от своя страна е под контрола или надзора на провинциален или федерален държавен орган, който на най-високо ниво попада в по-широка публична агенция в цялата страна, в рамките на национална организация или министерство. Ще има обаче големи разлики в мерките между различните държави, или дори в рамките на една държава, включително що се отнася до относителната автономия, с която се ползват различните органи, и във връзка с установяването и управлението на техните дейности по обработване по лични данни – именно поради това длъжностното лице по защита на данните следва да се запознае задълбочено с конкретните мерки за конкретната организация, в която работи.

Рамката за всички съответни публични структури, принадлежащи към определена йерархия, ще бъде определена до голяма степен в **правото**, на редица нива: конституция, закони, подзаконови нормативни актове (вторично, обвързващо законодателство), министерски наредби и инструкции, както и в евентуални

---

[303] Испанският орган по защита на данните, AEPD, в дописка за този наръчник, дава **примери** за дейности по обработване, които често се възлагат от местните органи (т.е., при които, от гледна точка на защитата на данните, обработването се извършва от обработващ лични данни):
• Подготовката на платежните ведомости за персонала
• Унищожаването на документация или носители
• Контролът на камерите за видеонаблюдение
• Управлението на събирането на данъци
• Поддръжка на компютърно оборудване
• Обработване на данни на Общинския регистър на населението:
• Обработване на данни на общинските данъци:
• Обработване на данни за човешки ресурси: приложимо спрямо подзаконови нормативни актове в областта на обществените услуги.
• Абонамент чрез услуга, предлагана от Общинския съвет на неговия уебсайт, за получаване на съобщения, свързани с културни дейности.
• Записване в банка за работни места.
(AEDP отбелязва и облачното изчисляване, както вече е отбелязано в текста.)

необвързващи или законово неуредени **договорености**, споразумения,[304] насоки и изложения на политики и т.н. Обработването на лични данни от организацията на длъжностното лице по защита на данните може да попада и в приложното поле на **кодекси за поведение**, които могат да бъдат различни видове . Отново, длъжностното лице по защита на данните следва да придобие възможно най-пълно и подробно разбиране на тези правила, договори и кодекси – и на процесите, чрез които те са приети, прилагани и преглеждани и изменяни, отново, ако е необходимо с помощта на юриста(ите) на неговата организация (и/или като посещава курсов по съответните теми, ако не е напълно запознат с тях, когато заема позицията си).

Ще има и други длъжностни лица по защита на данните в останалите организации, принадлежащи към съответната йерархия – и ще бъде от решаващо за отговорното за дадено дружество ДЛЗД да бъде напълно ангажирано с тях, в **мрежа на длъжностните лица по защита на данните**. Когато все още няма такава мрежа, длъжностното лице по защита на данните следва да работи за нейното създаване. Всички ДЛЗД следва, разбира се, да създават **тесни и добри връзки с националния орган по защита на данните (ОЗД)**, включително и с който и да е от висшето ръководство в рамките на органа по защита на данните със специфични отговорности във връзка с публичните органи/вида публичен орган, към който принадлежи организацията на длъжностното лице по защита на данните.

Договореностите, сключени от френския орган по защита на данните, CNIL, за национална мрежа на длъжностните лица по защита на данните, със специална „extranet", са добър пример за орган по защита на данните, подкрепящ формирането на такава мрежа и взаимодействия.[305]

Има и връзки към **външни организации, които са извън организационната йерархия на длъжностното лице по защита на данните**. Сред тях могат да бъдат други **публични органи в различна йерархия** – например, може да има връзки между образователни институции и институции за закрила или полицията, или между образователни органи в една държава и подобни организации в друга. Още веднъж, ще има (или трябва да има) **закони**, уреждащи тези връзки с такива други органи, или други **формални, обвързващи договорености и споразумения** (като договорености за споделяне на данни и споразумения между образователни институции и организации за закрила). Длъжностното лице по защита на данните следва още веднъж да получи пълни подробности за всички тези договорености, когато същите включват или може да включват обработването на лични данни – и следва наистина да ги прегледа, за да види дали те адекватно отразяват, потвърждават и въвеждат изискванията на ОРЗД и на които и да е относими национални закони и правила в областта на защитата на данните – и на по-общото законодателство в областта на защитата на правата на човека.[306]

---

[304] Тези договорености биха могли да включват споразумения между публични структури, съгласно които една публична структура обработва лични данни от името на друга публична структура, т.е. действа като обработващ лични данни за втория орган. Вж. обсъждането в текста на договорите между администратори, между администратор и обработващ лични данни и договорите за предаване на данни.

[305] Вж. раздел 2.5.3, в точка „Формално обучение и сертифициране", по-горе и бележка под линия 228.

[306] Срв. Решението на Европейския съд по правата на човека по делото *Copland v. the UK* от 3 април 2007 г., в което Съдът предвижда, че една неясно формулирана разпоредба на закон, предоставяща на публичен орган широка компетентност в определена област (*в дадения случай*, предоставянето на висше

Длъжностното лице по защита на данните може да не е в състояние, като такова, да оспори закон или правна договореност, съдържащи недостатъци, но би могло – и би следвало – да уведоми работодателя си, и вероятно съответния орган по защита на данните за виждането си, че законът е с недостатъци.

Понякога, връзките между формално обособени субекти, и сътрудничеството между тях, са основани на **неформални, непублични механизми** . Това обаче може да бъде проблемно от гледна точка на защитата на данните.

Както отбелязва Работната група по член 29 в своето становище относно концепцията за администратор и обработващ лични данни:[307]

> Налице е нарастваща тенденция за организационна диференция в най-относимите сектори. В частния сектор разпределението на финансовите или други рискове е довело до текуща корпоративна диверсификация, която се подобрява единствено чрез сливания и придобивания. В публичния сектор, подобна диференциация се осъществява в контекста на децентрализация или отделяне на политически отдели и изпълнителни агенции. В двата сектора има нарастващ фокус върху развитието на вериги или при предоставянето на услуги между организации и при възлагане на подизпълнители, или когато е на лице аутсорсинг на услуги, за да се възползват от специализацията и възможностите за икономии от мащаба. В резултат от това, се наблюдава ръст на различните услуги, предлагани от доставчиците на услуги, които не винаги се считат за отговорни или подотчетни. Поради организационните избори на дружествата (и техни изпълнители или подизпълнители) съответни бази данни може да бъдат разположени в една или повече държави в рамките на Европейския съюз или извън него.

Това води до затруднения във връзка с разпределението на отговорностите и предоставянето на контрол. Работната група казва, че участващите субекти следва да предоставят „достатъчна яснота" относно това разделение на отговорностите и ефективно предоставяне на (различни форми и нива на) контрол, което на практика означава, че участниците следва да ***обсъдят*** тези въпроси, ***да се договорят*** по тези разпределения и отговорности , както и да ***запишат*** това под формата на **официално споразумение**, което може (и при поискване, разбира се, следва) да бъде предоставено на съответния орган по защита на данните или органи по защита на данните и (вероятно в опростена форма) на субекти на данни и на обществото като цяло.

Като част от задачата по предварително определяне на обхвата, длъжностното лице по защита на данните следва отново да **провери** дали има каквито и да е такива официални споразумения, и ако да, дали те реално отразяват практическите разделения и отчет на на отговорностите и (б) дали напълно отговарят на изискванията на ОРЗД. Ако няма действащо официално споразумение, длъжностното лице по защита на данните следва да **даде съвет** такова да бъде спешно съставено (и ДЛЗД следва да участва в

и последващо образование) не представлява „закон" от гледна точка на Европейската конвенция за правата на човека:
http://hudoc.echr.coe.int/eng?i=001-79996 (вж. по-специално параграф 47.)

307 Работна група по Член 29, Opinion 1/2010 on the concepts of "controller" and "processor" (Становище 1/2010 относно концепциите за „администратор" и „обработващ лични данни") (WP169, приет на 16 февруари 2010 г.), стр.6, може да се намери на:
http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf

обсъждането, споразумението и записването). Ако има само неформални договорености, ДЛЗД следва да **посъветва** те да бъдат заменени с официални такива.

Освен това, когато връзки и договорености с други субекти представляват или включват споразумение между администратори и/или между администратор и обработващ лични данни, те следва да бъдат подкрепени от съответни (отговарящи на ОРЗД) **договори между администратори и/или между администратор и обработващ лични данни**; и когато връзките и споразуменията с други субекти включват предаване на лични данни към държави извън ЕС/ЕИП (т.нар. „трети държави"), трансферът следва да бъде основан на съответни (отговарящи на ОРЗД) **клаузи за предаване на данни** (било то стандартни клаузи, одобрени от съответния орган по защита на данните или органи по защита на данните или от Европейския комитет по защита на данните, или *ad hoc* клаузи, които са в съответствие с ОРЗД).

Когато съществуват такива договори или клаузи, длъжностното лице по защита на данните следва да ги **прегледа**, за да види дали те са в съответствие с ОРЗД, а когато няма такива договори или клаузи, но би следвало да има, длъжностното лице по защита на данните , съответно **дава съвет** те да бъдат сключени спешно.

Тези задачи на длъжностното лице по защита на данните във връзка с официални споразумения, договори между администратори, както и договори между администратори и обработващи лични данни и клаузи за предаване на данни (и в други свързани отношения), са допълнително разгледани в 3.x, по-долу. Тук ще бъде достатъчно да се отбележи, че длъжностното лице по защита на данните следва да **установи** тези проблеми в задачата по предварително определяне на обхвата, за да им бъде обърнато внимание след това.

Накрая, организацията на длъжностното лице по защита на данните ще има **контакти с външни доставчици на стоки или услуги (от частния и публичния сектор)**, простиращи се от аутсорснато обработване на данни, счетоводство и управление на уебсайтове до доставката на храна за столове, поддръжка и ремонти, медицинска и социално осигуряване за персонала и т.н. . Работата, осъществена в тези отношения, ще бъде базирана на **договори** (обикновени граждански договори или специални публично-частни договори). Тези договори ще уреждат и ще бъдат базата за всякакво обработване на лични данни от страните по тези договори: за събирането на съответните лични данни от споделянето и използването на тези данни, до тяхното окончателно унищожаване или изтриване. Ако другият субект е администратор на свое собствено основание, тези договори (или поне елементите, относими към защитата на данните на тези договори) ще представляват, от гледна точка на защита на данните, **договори между администратор и администратор за обработване на лични данни**. Ако другият субект действа просто като обработващ лични данни за организацията на длъжностното лице по защита на данните, договорът ще бъде **договор между администратор и обработващ лични данни**. И ако съгласно договора се предават лични данни в място извън ЕС/ЕИП (обичайно на „облачен" сървър, поддържан от изпълнителя), те представляват **договори за прехвърляне на лични данни**.

В дейността по предварително определяне на обхвата, длъжностното лице по защита на данните следва още веднъж да **установи** дали има такива договори , след това, скоро след извършването на определянето на обхвата, да ги **прегледа** и, когато те липсват или

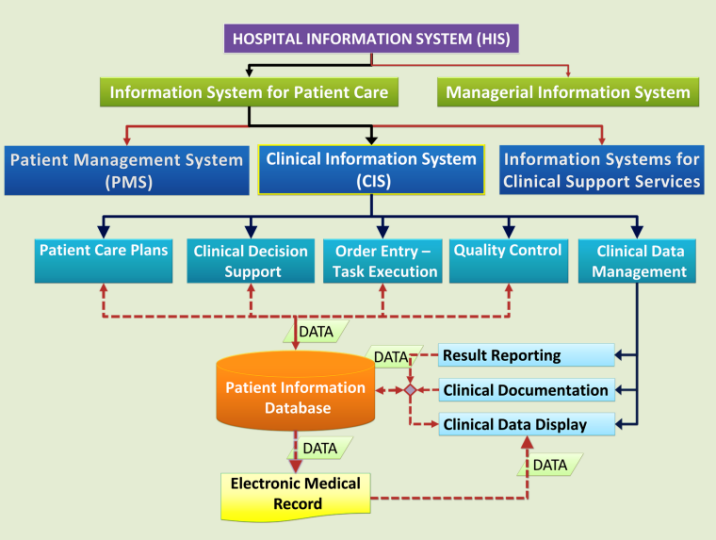
са с недостатъци от гледна точка на ОРЗД, **да даде съвет** те да бъдат съставени или редактирани.

Очертаване в общи линии на дейностите по обработване на лични данни на организацията

Извършването на общ преглед на дейностите на организация отДЛЗД (както е посочено по-горе), ще представлява решаваща стъпка към създаването на подробен регистър на всички тези дейности и всички индивидуални дейности по обработване на лични данни, извършвани в Задача 1 (разгледана по-нататък). Това следва да доведе до графика като представената по-долу от д-р Абдула Салех, посочваща *„Функционалните компоненти на една клинична информационна система ”* (използвана в първото обучение по T4DATA, в презентация от италианския орган по защита на данните, *Garante del Privacy*).[308]

ПРИМЕР:

Карта на дейностите по обработване на лични данни на организацията [тук: болница]



Източник: Д-р Абдула Салех, https://drdollah.com/hospital-информация-system-his/

Следва да се отбележи, че горепосочената карта е по-тясно свързана с дейности по обработване на лични данни от представената по-рано органиграма на болница.

308 Луиджи Кароци, Презентация на първата обучителна сесия за „T4DATA”, юни 2018 г., слайдове за *„Практически насоки за длъжностни лица по защита на данните – Регистърът с дейности по обработка на данни*”.

Организационни задачи:

ЗАДАЧА 1: Създаване на регистър на дейностите по обработване на лични данни

Съгласно чл. 30 от ОРЗД, всеки администратор трябва да „поддържа **регистър** на дейностите по обработване, за които отговоря", съдържащ подробности за всяка операция, като името на администратора (би могло да се добави, на „отговорника за дейността") надеждността, целта(целите) на дейността , категориите субекти на данни, лични данни и получатели и т.н. Това задължение за водене на регистър на дейностите по обработване е тясно свързано с принципа на отчетност, разгледан в 2.2 по-горе, улеснявайки ефективния надзор от съответния орган по защита на данните („надзорен орган") – както е подчертано от съображение 82 от ОРЗД:[309]

> ***За да докаже спазването*** на настоящия регламент, администраторът или обработващият данни ***следва да поддържа документация за дейностите по обработване***, за които той е отговорен.
>
> Всеки администратор и обработващ лични данни **следва да е длъжен да си сътрудничи с надзорния орган и да му осигури достъп до тази документация при поискване**, за да може да бъде използвана за наблюдение на тези дейности по обработване.

С други думи, както поставя нещата италианският орган по защита на данните, *Garante*,:[310]

> **Регистърът е мярка за доказване на спазване на ОРЗД**

Препращането към „дейности по обработване под отговорността на администратора" внушава, че документацията (често пъти, наричана регистър) трябва да обхваща **всички** такива дейности по обработване и това е изрично предвидено в немската версия на ОРЗД.[311] Това също има смисъл, защото, както отбелязва и *Garante*:[312]

> Общата картина на информационни активи „лични данни" и свързаната операция по обработване, предоставена от регистъра, е **първата стъпка към отчетност**, тъй като тя дава възможност за оценката на риска за правата и свободите на лицата и да се приложат подходящи технически и организационни мерки, за да се осигури ниво на сигурност, съответстващо на нивото на риска.

Макар че, както при повечето други изисквания на ОРЗД, това е формално задължение на администратора, а не на длъжностното лице по защита на данните, на практика длъжностното лице по защита на данните ще бъде лицето, което ще отговаря за тази работа (в тясно сътрудничество със съответния персонал на администратора), или което

---

309 Луиджи Кароци, презентация на първата обучителна сесия за „T4DATA", юни 2018 г., слайд за „*Опис на активите и принципа за отчетност*" (оригинални подчертавания)

310 *Пак там*.

311 "*Jeder Verantwortliche und gegebenenfalls sein Vertreter führen ein Verzeichnis* ***aller Verarbeitungstätigkeiten****, die ihrer Zuständigkeit unterliegen.*" (добавено подчертаване).

312 Луиджи Кароци (бележка под линия 202, по-горе) (оригинално подчертаване).

поне ще бъде тясно приобщено към нея и ще я контролира. Както посочва Работната група по член 29 (РГ по 29):[313]

> На практика, длъжностните лица по защита на данните често създават списъци и водят регистър на дейностите по обработване на база на информация, предоставена им от различните отдели в съответната организация, които отговарят за обработването на лични данни. Тази практика е установена по много текущи национални закони и съгласно правилата за защита на данните, приложими спрямо институциите и структурите на ЕС.[314]
>
> Чл. 39, пар. 1 предвижда списък със задачи, които длъжностното лице по защита на данните трябва да има като минимум. Поради това, нищо не пречи на администратора или на обработващия лични данни да възлага на длъжностното лице по защита на данните задачата да поддържа документирането на дейности по обработване под отговорността на администратора. Това документиране следва да се разглежда като един от инструментите, даващи възможност на длъжностното лице по защита на данните да изпълнява своите задачи за наблюдение на спазването, информиране и даване на съвети на администратора или обработващия лични данни.
>
> Във всеки случай, регистърът, който се изисква да бъде воден съгласно чл. 30, следва да се разглежда и като инструмент, позволяващ на администратора и на надзорния орган, при поискване, да имат обзор на дейностите по обработване на лични данни, изпълнявани от дадена организация. Така, това е предпоставка за съответствие и, като такава, ефективна мярка за отчетност.

За едно ново длъжностно лице по защита на данните, това изисква, на първо място описване на всички дейности на организацията, които могат да включват обработване на лични данни и на връзки с други организации. Това предполага преценка кои данни съставляват лични данни, което не винаги е лесно.[315] ***Първоначален, основен опис*** може да бъде полезно извършен успоредно с по-обширното определяне на обхвата на организацията и нейния оперативен контекст, в предварителната задача (Задача 0), описана по-горе. При условията на изключението, посочено по-долу, той би следвало след това да бъде последван от ***пълен опис***.

Пълният опис следва да доведе до създаването на **регистър** (събирането на „**регистри**") за всички дейности по обработване на лични данни на администратора, споменат в чл. 30 (както е разгледано малко по-късно в този раздел, в точка „*Съдържание и структура на позициите в регистъра*"), който следва след това (и след прегледа и оценката на, отбелязани на следващо място, в Задачи 2 и 3) да се поддържа актуален от длъжностното лице по защита на данните (или длъжностното лице по защита на данните следва поне да гарантира поддържането му в актуално състояние): вж. текста по-долу, в точка „*(текущо) Наблюдение на спазването*", след Задача 4.

Освобождаване:

---

313 Работна група по член 29, Насоки за длъжностните лица по защита на данните (бележка под линия 209, по-горе), раздел 4.4, *Роля на длъжностното лице по защита на данните в деловодството*, стр.18.

314 Чл. 24, пар. 1, б. „г" от Регламент (ЕО) 45/2001 [оригинална бележка под линия]

315 Виж Работна група по член 29, мнение 4/2007 относно определението на лични данни (WP136), прието на 20 Юни 2007, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136

Чл. 30, пар. 5 освобождава **предприятията и организациите, които наемат по-малко от 250 души, и които обработват „лични данни“** спорадично,[316] от задължението да водят регистър на техните дейности по обработване на лични данни. Това освобождаване обаче не се прилага, ако:

- Обработването, извършвано от предприятието или организацията, „*има вероятност [] да породи* ***риск за правата и свободите на субектите на данни***” (следва да се отбележи, че това не трябва да бъде „висок риск”, като такъв, който да създаде необходимост от провеждането на Оценка на въздействието върху защитата на данните (Задача 4): всеки риск за правата и свободите на субектите на данни, независимо колко е малък, би изисквал записването (и прегледа) на дейностите на администратора;
- обработването **не е спорадично**; или
- обработването включва **чувствителни данни или данни, свързани с присъди и нарушения**.

Що се отнася до първото от тези, в контекста на оценките на въздействието върху защитата на данните (които се изискват, когато има вероятност за „*висок риск* за правата и свободите на физическите лица”: вж. Задача 4, по-долу), Работната група по член 29 е описала термина „**риск**” като:[317]

> сценарий, описващ събитие и неговите [отрицателни] последици, прогнозиран като тежест и вероятност –

и обяснява, че:[318]

> препращането към „**правата и свободите**” на субекти на данни се отнася основно за правата на защита на данните и неприкосновеността на личния живот, но може да касае и други основни права, като свободата на словото, свободата на мисълта, свободата на движението, забрана на дискриминацията, правото на свобода, самоосъзнаване и изповядване на религия.

дейностидейностидейностидейностиПрез Април 2018, Работната група по член 29 публикува документ с позицията си относно чл. 30 (5) от ОРЗД.[319] В него тя подчертава, че:

чл. 30, пар. 5 е ясен и точно определя трите категории обработване, които са алтернативни, за които изключението не се прилага. Наличието само на една от тях води до възникването на задължение за поддържане на регистър на дейностите по обработване.Следователно, въпреки че администраторът или обработващия данни

---

316 Според нас, условието, че малката организация трябва да извършва обработване на лични данни само „спорадично” следва от разпоредбата (разгледана в текста), че освобождаването не се прилага, ако обработването от малката организация „не е спорадично”.

317 Работна група по член 29 Насоки за оценки на въздействието върху защитата на данните (бележка под линия 315, по-долу), стр.6.

318 *Вж.*, добавено подчертаване.

319 Работната група по член 29, Позиция относно изключенията от задължението за поддържане на регистри по дейностите по обработване, съгласно чл. 30, параграф 5 от Общия регламент за защита на данните, https://www.cpdp.bg/userfiles/file/WP29/20180419_Art29WP_PositionpaperArt30_publish_Bg.pdf Позицията не е официално одобрена от Европейския комитет по защита на данните в момента на одобрението на насоките на Работната група по член 29, но все пак може да се смята за референтен източник.

имат по-малко от 250 служители, ако същите извършват обработване на данните, което 1) има вероятност да породи риск (не само голям риск) за правата на субектите на данните; 2) не се извършва спорадично; 3) засяга специални категории данни, съгласно чл. 9, пар. 1 или данни, отнасящи се до присъди и нарушения, съгласно чл. 10, те трябва да поддържат регистър на дейностите по обработване. Тези организации трябва да поддържат регистри единствено за категориите обработване на данни, визирани в чл. 30, пар. 5 от Общия регламент.

Например, малка фирма редовно обработва данни на своите служители. В резултат, това обработване не би могло да бъде считано за „спорадично“ и следва да бъде включено в регистъра на дейностите по обработването.[320] Други дейности, които могат да се считат за „спорадични“ могат да не бъдат включени в регистър на дейностите по обработването само, ако не биха породили риск за правата и свободите на субектите на данните и само ако не засягат специални категории данни или данни, отнасящи се до присъди и нарушения.

Пример:

В **Хърватия**, подробна информация за всички държавни служители и служители на публични органи, трябва по закон да се качва в централизирана система, „*Регистър на служителите в публичния сектор“*. Това се прилага дори спрямо най-малките публични субекти, като малки местни общности, които могат да наемат само ограничен брой хора. Поради това обработването на данните за тези няколко служители от тази много малки общности не е „спорадично” и не се ползва от освобождаването от водене на регистри.

Ако се съмнява, администраторът следва да потърси съвета на длъжностното лице по защита на данните по тези въпроси – и длъжностното лице по защита на данните следва да бъде предразположено да даде съвет в полза на създаването на пълен регистър в крайни случаи, вместо да рискува да бъде постановено, че организацията е нарушила задълженията,посочени в чл. 30, пар. 1 – 4.

Бележки:

1. По въпроса дали регистъра на дейностите по обработване на лични данни трябва да бъде направен достъпен до някого (онлайн или по друг начин), или не, вж. Задача 12, „*Задачи по повишаване на информираността и осведомеността*”.
2. Създаването на регистъра като такъв все още не включва оценка на съответствието на регистрираните дейности в ОРЗД: това е направено в Задача 2 – но, разбира се, регистърът следва да бъде изменян и актуализиран, както и когато се извършват изменения в дейностите по обработване, записвани в него: вж. позицията „*Наблюдение на спазването: Повтаряне на задачи 1 – 3 (и 4) на текуща база*”, в края на Задача 4 (точно преди Задача 5).

Съдържание и структура на позициите в регистъра (записи):

ОРЗД прави разграничение между регистрите на администратори и обработващи лични данни.

[320] Работната група по член 29 счита, че процес по обработване на данни може да бъде определен като „спорадичен“ само ако не се извършва редовно и ако се извършва извън редовната нормална дейност на администратора или обработващия лични данни. Виж Работна група по член 29, Насоки относно член 49 от Регламент 2016/679 (WP262)

Съдържание и структура на позициите (записите) в регистъра на администратора

Съгласно чл. 30, пар. 1 от ОРЗД, **регистърът** на дейностите по обработване на лични данни на *администратор* трябва да се състои от съвкупност от **записи** на всяка такава операция; и **всеки такъв запис трябва да включва следните данни** (думите в квадратни скоби и курсив са добавени):

a. името и координатите за връзка на администратора и — когато това е приложимо — на всички съвместни администратори, на представителя на администратора и на длъжностното лице по защита на данните, ако има такива;

b. целите на обработването;

c. описание на категориите субекти на данни и на категориите лични данни

d. категориите получатели, пред които са или ще бъдат разкрити личните данни, включително получателите в трети държави или международни организации;

e. когато е приложимо, предаването на лични данни на трета държава или международна организация, включително идентификацията на тази трета държава или международна организация, а в случай на предаване на данни, посочено в чл. 49, пар. 1, втора алинея, документация за подходящите гаранции;

f. когато е възможно, предвидените срокове за изтриване на различните категории данни;

g. когато е възможно, общо описание на техническите и организационни мерки за сигурност, посочени в член 32, параграф 1.

Този списък не включва **правно основание** за обработването на съответните данни (чл. 6 във връзка с нечувствителни данни; чл. 9 във връзка с чувствителни данни) или правни инструменти, използвани при договорите с обработващи лични данни или при предаване на лични данни – но те са толкова важнивъв връзка с което и да е определяне на законността и съвместимостта с ОРЗД, на която и да е операция по обработването, че също трябва да бъдат въведени в регистъра, във връзка с всяка операция по обработване на лични данни (определенивъв връзка с целта на обработването), като валидността на твърдяното и записано правно основание трябва да бъде проверено в срок.

ПРИМЕРЕН ФОРМАТ НА ОСНОВЕН РЕГИСТЪР НА АДМИНИСТРАТОР ЗА ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ [321]

Следва да се отбележи, че трябва да бъде създаден отделен запис за всяка обособена операция

Част 1 – Информация относно администратора и т.н..

ДАННИ ЗА КОНТАКТ С **АДМИНИСТРАТОРА**:	Име, адрес, имейл, Телефон
ДАННИ ЗА КОНТАКТ СЪС **СЪВМЕСТНИЯ АДМИНИСТРАТОР**:*	Име, адрес, имейл, Телефон
ДАННИ ЗА КОНТАКТ С **ПРЕДСТАВИТЕЛЯ**:*	Име, адрес, имейл , Телефон

[321] Разширен от образеца на формуляра, представен от Кароци (бележка под линия 202, по-горе) с редакции (напр., портретен вместо пейзажен фромат) и записи за името на операцията, правните основания за обработването, подходящи гаранции за предаване на данни и добавени подробности във връзка с технологии и сигурност (в съответствие с последващи препоръки от Кароци).
БЕЛЕЖКА: Примерен формат на по-подробен (15-страничен) запис за обработване на лични данни е приложен в края на разглеждането на настоящата задача.

(*) ***ако е приложимо***
ДАННИ ЗА КОНТАКТ С **ДЛЗД**: Име, адрес, имейл , Телефон

Част 2 – Основна информация за операцията по обработване на лични данни (ООЛД)[322]

1. Име на ООЛД[323]	
2. Отговорно звено („отговорник за дейността")	
3. Цел на ООЛД	
4. Категории субекти на данни	
5. Категории лични данни	
6. Това включва ли чувствителни данни?	
7. Законово основание за обработването:* * Срв. чл. 6 от ОРЗД за нечувствителни данни, чл. 9 за чувствителни данни	
8. Данните предават ли се на 3-та държава или на международна организация?	
9. В случай на предаване по член 49, параграф 1, точка 2 от ОРЗД: какви подходящи гаранции са предоставени?	
10. Срокове за изтриване	
11. Данни за системите, приложенията и процесите (хартиени/електронни досиета; десктоп пакет/централно управлявано приложение / облачна услуга/ локална мрежа; пренос на данни; и т.н.) и свързаните технически и организационни мерки (за сигурност)	

[322] Примерната диаграма по-горе има за цел просто да илюстрира изискванията за записване в най-общи линии. **Примерният подробен протокол от обработка на данни**, споменат в предишната бележка под линия и приложен към тази Задача, изисква важни допълнителни данни, напр., за всяка категория лични данни: целта, относимостта и източника на данните и т.н.

[323] От гледна точка на защитата на данните в правен аспект, всяка операция по обработване на лични данни е операция, която най-добре се определя на база на целта, обслужвана от операцията (както е записана в 2.). В много организации обаче хората, изпълняващидейностите, често ще имат специфично функционално/вътрешно име за операцията – въпреки, че двете наименования, разбира се, често ще се припокриват и могат да бъдат идентични.

12. Обработването на данни включва ли намесата на обработващ/и лични данни? Ако това е така, предоставете детайлна информация и копие от съответните договори.	

Съдържание и структура на позициите (записите) в регистъра на обработващия лични данни[324]

Съгласно чл. 30, пар. 2 от ОРЗД, **регистърът** на дейностите по обработване на лични данни на *обработващия лични данни* следва да се състои от съвкупност от **записи** на всяка такава операция; и **всеки такъв запис трябва да включва следните подробности**:

a. името и координатите за връзка на обработващия или обработващите лични данни и на всеки администратор, от чието име действа обработващият лични данни и — когато това е приложимо —на представителя на администратора или обработващия лични данни и на длъжностното лице по защита на данните;

b. категориите обработване, извършвано от името на всеки администратор;

c. когато е приложимо, предаването на лични данни на трета държава или международна организация, включително идентификацията на тази трета държава или международна организация, а в случай на предаване на данни, посочено в член 49, параграф 1, втора алинея, документация за подходящите гаранции;

d. когато е възможно, общо описание на техническите и организационни мерки за сигурност, посочени в член 32, параграф 1.

По-долу, отново предоставяме примерен формуляр на вида протокол, който един обработващ лични данни следва да води, за да изпълни тези изисквания.

ПРИМЕРЕН ФОРМАТ НА ПРОТОКОЛ ЗА ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ НА ОБРАБОТВАЩ ЛИЧНИ ДАННИ [325]

Следва да се отбележи, че трябва да бъде създаден отделен протокол за всяка отделна операция по обработване на лични данни за всеки отделен администратор

Част 1 – Информация относно обработващия лични данни и който(които) и да е подизпълнител(и) на обработващия лични данни

ДАННИ ЗА КОНТАКТ С **ОБРАБОТВАЩИЯ ЛИЧНИ ДАННИ**: Име, адрес, имейл, Телефон

---

[324] Следва да се отбележи, че е все по-трудно напълно да бъдат разграничени обработващите лични данни от администраторите. Често пъти, субектите, които са предоставяли непосредствени услуги на обработващ лични данни (действайки просто както са били инструктирани от администратора, който е определил средствата и целите), сега поемат много повече отговорности и могат да станат „съвместни администратори". Това е особено валидно във връзка с доставчиците на облачни услуги – някои от които сега дори предлагат „*Изкуствен интелект и машинно учене (AI/ML) чрез машинно обучение като услуга (MLaaS)*", вж.:
http://www.techmarketview.com/research/archive/2018/04/30/machine-learning-as-a-service-market-overview-technology-prospects
Както е разгледано в *Предварителна задача*, договореностите между субектите, участващи в такива сложни договорености, следва да бъдат ясно и надлежно записани. Формулярите, в които се записват съответните дейности по обработване, следва да бъдат прегледани и поправени, а да отговарят на тези (договорени и записани) споразумения между субектите. Субектите, които са повече от непосредствени обработващи лични данни, следва да използват подробния формуляр, споменат в следващата бележка под линия.

[325] Относно разширен от образеца на формуляр, представен от Кароци (бележка под линия 202, по-горе) с редакции. Срв. бележка под линия 286, по-горе.

ДАННИ ЗА КОНТАКТ С **ДЛЗД**:	Име, адрес, имейл , Телефон
ДАННИ ЗА КОНТАКТ С **ПОДИЗПЪЛНИТЕЛЯ НА ОБРАБОТВАЩИЯ ЛИЧНИ ДАННИ**:*	Име, адрес, имейл , Телефон
ДАННИ ЗА КОНТАКТ С **ДЛЗД**:	Име, адрес, имейл , Телефон
ДАННИ ЗА КОНТАКТ С **ПОДИЗПЪЛНИТЕЛЯ НА ОБРАБОТВАЩИЯ ЛИЧНИ ДАННИ**:*	Име, адрес, имейл , Телефон
ДАННИ ЗА КОНТАКТ С **ДЛЗД**:	Име, адрес, имейл , Телефон

* *ако е приложимо*

Част 2 – Информация относно администратора на конкретната въпросна ООЛД

ДАННИ ЗА КОНТАКТ С **АДМИНИСТРАТОРА**:	Име, адрес, имейл , Телефон
ДАННИ ЗА КОНТАКТ СЪС **СЪВМЕСТНИЯ АДМИНИСТРАТОР**:*	Име, адрес, имейл , Телефон
ДАННИ ЗА КОНТАКТ С **ПРЕДСТАВИТЕЛЯ**:*	Име, адрес, имейл , Телефон
(*) ***ако е приложимо***	
ДАННИ ЗА КОНТАКТ С **ДЛЗД**:	Име, адрес, имейл , Телефон

БЕЛЕЖКА: Взаимоотношенията между администратора и обработващия лични данни, и между обработващия лични данни и който и да е подизпълнител на обработващия лични данни трябва да бъдат базирани на писмен договор, отговарящ на изискванията на чл. 28 от ОРЗД. Обработващите лични данни следва да съхраняват копия на съответните договори с попълнения формуляр.

Част 3 – Данни за операцията по обработване на лични данни (PDPO)

1. Категорията (видът) обработване, което се извършва за администратора във връзка с общата PDPO включително:	
- категориите субекти на данни;	
- категориите лични данни; и	
- дали то включва чувствителни данни.	
2. Предават ли се данните на 3-та държава или на	

	международна организация?	
3.	В случай на предаване по чл. 49, пар. 1, т. 2 от ОРЗД: какви подходящи гаранции са предоставени?	
4.	Данни за използваните системи, приложения и процеси (вид електронни досиета; десктоп пакет/централно управлявано приложение / облачна услуга/ локална мрежа; пренос на данни; и т.н.) и свързаните технически и организационни мерки (за сигурност)	
5.	Обработването на данни включва ли намесата на обработващ/и лични данни? Ако това е така, предоставете детайлна информация и копие от съответните договори.	

Съдържание и структура на регистъра:

Длъжностното лице по защита на данните следва да създаде **регистър** от **протоколите (записите)**, които получава за всяка отделна операция по обработване на лични данни. Те обичайно най-добре се подреждат по **организация** и в рамките на тази подредба – по **отговорник за дейността**. С всеки отделен протокол, длъжностното лице по защита на данните следва да води цялата съответна документация (както е указано в примерните формуляри по-горе).

Длъжностното лице по защита на данните следва да отбележи в регистъра кога е получен всеки протокол, кога е прегледана съответната операция по обработване (както е направено в Задача 2, описана на следващо място), с резултата от този преглед и предприети всякакви корективни мерки; и да посочи когато операцията следва да подлежи на редовен (напр., годишен) преглед.

- o – O – o –

Приложение: Примерен формат на подробен протокол за обработване на лични данни[326]

[326] По-подробен образец на проткол за лични данни е предоставен от полския орган по защита на данните, *Urząd Ochrony Danych Osobowych* (UODO) на неговия уебсайт, на полски език, на: https://uodo.gov.pl/pl/123/214 (последвайте първия линк в дъното на страницата.)

Приложение:

ПРИМЕРЕН ФОРМАТ НА ПОДРОБЕН ПРОТОКОЛ ЗА ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ

Моля, използвайте отделен формуляр за всяка отделна операция по обработване на лични данни

БЕЛЕЖКА: Ако смятате за необходимо да уточните или изясните даден въпрос, моля, добавете номер в съответното поле и приложете страница с тези уточнения или разяснения, с препратка към този номер.

I. ОБЩА ИНФОРМАЦИЯ: * означава задължително поле (ако е приложимо)

Администратор: (Основна организация на администратора)* (Име, място на установяване и адрес, регистрационен номер и т.н.)	
Свързани субекти (Всякакви субекти, с които е свързан администраторът във връзка с тази операция, напр., дъщерни фирми/дружества или свързани публични структури; обработващи лични данни, които участват в тази операция)	
Бизнес отдел: („Отговорник за дейността")* (Напр., Човешки ресурси, Счетоводство, Научно-развойна дейност, Продажби, Поддръжка на клиенти)	
Лица за контакт в рамките на отдела:	
ОСНОВНА ЦЕЛ НА ОПЕРАЦИЯТА ПО ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ:* ***Моля, посочете възможно най-точно***	
Използват ли се или разкриват ли се лични данни за някаква друга (второстепенна) цел или цели?* ***Моля, посочете възможно най-точно и добавете линк или препратка към свързания запис.***	
Изпълнява ли се тази операция за всички свързани субекти по същия начин? Или отделно и/или различни за различните субекти?* ***Моля, посочете.***	

Ако дейностите са различни за различните субекти, моля, използвайте отделни формуляри за всеки от тях.	
Приблизително, с колко лица (субекти на данни) е свързана тази операция (ако е известно)?*	[*Добавете брой или „неизвестен"*]
Дата на подаване на този формуляр до длъжностното лице по защита на данните:*	
Формуляр & операция по обработване, прегледани от длъжностно лице по защита на данните:	[*Да/Не и дата, да се въведе от длъжностното лице по защита на данните*]
Дата за извършване на преразглеждане/ актуализация на този формуляр:	[*Да се посочи от длъжностното лице по защита на данните*]

II. ПОДРОБНОСТИ ЗА ОПЕРАЦИЯТА ПО ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ:

II.1 Данните и източниците на данни

[БЕЛЕЖКА: Всички полета са задължителни, ако са приложими, освен ако не е посочено друго]

1. Какви лични данни или категории лични данни са събрани и използвани за тази операция?	*Поставете √ където е уместно :*	**Кога и от кого са получени данните?** **Напр.:** (субект на данни=СД) - подробен работен план/ПРП/ при наемане на лицето - СД, при записване в изследването
- Лично и фамилно име(на)		
- Дата на раждане		
- Домашен адрес		
- Служебен тел. номер		
- Личен тел. номер		
- Адрес на служебна електронна поща		
- Адрес на лична електронна поща		
И всякакви други данни по-долу, ако е приложимо:* ** Вж. също по-долу, в 2,* относно *чувствителни данни*		

Добавете допълнителни редове, ако е необходимо		
2. Дали данните, които събирате и записвате за операцията, <u>включват или непряко разкриват</u> някои от следните специални категории лични данни („чувствителни данни”)?	*Поставете √, ако данните са изрично събрани и използвани за операцията; Поставете √ и добавете („непряко”) ако данните са разкрити непряко (обяснете в бележка, ако е необходимо)*	**Кога и от кого са получени данните?** **Напр.:** (субект на данни=СД) - ПРП при наемане на лицето - СД, при записване в изследването
- Расов или етнически произход		
- Политически мнения или принадлежности		
- Религиозни или философски убеждения		
- Членство в профсъюзна организация		
- Генетични данни		
- Биометрични данни		
- Данни относно здравето на лицето		
- Данни относно сексуалната ориентация или половия живот на лицето		
- Информация относно присъди или нарушения		
- Национален идентификатор* * Напр., национален идентификационен номер (Единен Граждански Номер (ЕГН)), данъчен номер		
- Данни относно дългове/ кредитен рейтинг		
- Данни за непълнолетни		
3. Ако е известно или определено: Колко дълго се пазят (специалните и други) данни? Какво се случва след това?* * Посочен период или събитие, напр., „7 години” или „До 5 след прекратяване на		

трудовото правоотношение". Също така, обяснете какво се случва с данните, напр., изтриване/унищожаване или анонимизирането им. **БЕЛЕЖКА: Ако има различни периоди на запазване за различни данни, моля посочете това.**	

II.2 Разкриване на данни

4. Пред кои трети лица и кои от горепосочените данни се разкриват? И за какви цели? **БЕЛЕЖКА: Това се прилага и за данни, до които се осигурява достъп онлайн – особено ако се осигурява директно *Относно* разкривания, включващи предаване на трети държави, вж. по-долу, във II.5**	**Трето лице получател: място и държава на установяване:**	**Цел(и) на разкриването(ията):**
ВСИЧКИ ДАННИ, ИЗБРОЕНИ В II.1		
***ИЛИ:* Следните данни:** (Копирайте данните от 1 & 2 по-горе)		
-		
-		
-		
-		
-		
-		
-		
-		
-		
-		
-		
-		
-		
-		
-		
-		
-		
-		
-		
Добавете допълнителни редове, ако е необходимо		

II.3 Законово основание за обработването

5. **На какво законово основание се обработват данните?** **БЕЛЕЖКА: Ако има различни законни основания за различни данни или за различни (основния, второстепенниили нови, несвързани) цели, моля, посочете това (ако е необходимо, като копирате и поставите списъците с данни от по-горе по-долу, с различните законни основания, преместени във втората колона).**	*Поставете отметка за съответното законово основание и дайте пояснение в следващата колона, както е уместно.*	**Пояснение:**
- Субектът на данни се е съгласил с обработването **БЕЛЕЖКА: Вж. също Въпроси 6 – 9, по-долу.**		
- Обработването е необходимо за договора между Вашата организация и субекта на данни (Или за да се предприемат стъпки по искане на субекта на данни преди сключването на договор – напр., получаване на препоръки)		
- Обработването е необходимо за спазване на правно задължение на Вашата организация * Напр., по трудовото или данъчното право – *моля, посочете въпросното право*		
- Обработването е необходимо, за да се защитят жизнените интереси на субекта на данни или на друго лице		
- Обработването е необходимо за изпълнението на задача, изпълнявана в обществен интерес* * *Моля, посочете източника на задачата (обичайно, закон)*		
- Обработването се извършва в упражняване на официално правомощие * *Моля, посочете източника на задачата (обичайно, закон)*		

- Обработването е необходимо за законните интереси на Вашата организация (или друг субект) и този интерес не по-маловажен от интересите на субектите на данни Напр., маркетинг към Вашите собствени клиенти или предотвратяване на измама – моля, посочете ясно.		
СЪГЛАСИЕ – допълнителни данни:		
6. **Ако данните се обработват на база на съгласието на субектите на данни, как и кога е получено това съгласие?** **БЕЛЕЖКА: Ако съгласието е предоставено на хартия или в електронен формат, моля, представете копие от съответния текст/линк**		
7. Какво доказателство за даването на съгласието се пази? Напр., пазят ли се копия от хартиени формуляри или дневници за електронно съгласие?		
8. Какъв период от време се съхранява това доказателство?		
9. Ако в контекста на даден договор от Вашата организация бъдат поискани повече данни отколкото са необходими за договора, информиран ли е субекта на данни, че той не е длъжен да предостави допълнителните данни? **БЕЛЕЖКА: Или отговорете „N.A." (Неналично) или, ако е налично , представете копие от съответния текст/линк**		

II.4 Информиране на субектите на данни [БЕЛЕЖКА: Тази информация не е задължителна, но е полезна при оценка и преразглеждане на вътрешните политики за защита на данните]

10. **Информирани ли са субектите на данни за следното? И ако да, кога и как?**	*Посочете Да/Не (или „N.A." („Неприложимо"))* **БЕЛЕЖКА: Ако е относимо, можете да кажете „ очевидно в контекста" и/или „Субектът на данни вече има тази информация"**	Обяснете как и кога е направено това **Моля, представете копия от всякакви уведомления или линкове с информация**
- Че Вашата организация е администратора на операцията по обработване на лични данни?		
- Данни за Вашата организация (напр., име и регистрационен номер)?		
- Ако е приложимо, данни за Вашия представител в ЕС?		
- Данните за контакт на длъжностното лице по защита на данните?		
- Основната цел на обработването?		
- Всяка друга цел, за която Вашата организация иска (или може да иска) да обработва данните?		
- Ако данните не са били получени директно от субектите на данни, източникът или източниците на данните, и дали те включват публично достъпни източници (като публични регистри)?		
- Получателите или категориите получатели на данните? **Бележка: Срв. Въпрос 4, по-горе**		
- Дали данните ще бъдат предадени в държава извън ЕС/ЕИП (*напр., на облачен сървър в САЩ*)? **БЕЛЕЖКА: Това се прилага и за данните, до които се предоставя достъп (особен директно, онлайн) на субекти в държави извън ЕС/ЕИП.**		
- Ако данните се прехвърлят по този		

начин, какви гаранции са въведени и къде могат субектите на данни да получат копия на същите? **БЕЛЕЖКА: Могат да се предвидят гаранции в договори за предаване на данни или чрез кодове или печати за неприкосновеност на личния живот.**		
- За какъв период от време ще бъдат пазени данните?		
- За правото да искат достъп, коригиране на данните им; да поискат данните им да бъдат блокирани; да възразят срещу обработване?		
- За правото им да подадат жалба в съответния Орган по защита на данните?		
11. Ако всички или част от данните са обработвани на база на съгласие, информирани ли са субектите на данни за следното?		
- Че могат да оттеглят съгласието си по всяко време (и как да направят това) (без това да засяга законосъобразността на вече извършеното обработване)?		
12. Ако предоставянето на данните е законово или договорно задължение (или изискване за сключването на договор), субектите на данни информирани ли са за следното?	*Посочете Да/Не (или „N.A." („Неприложимо"))* **БЕЛЕЖКА: Ако е относимо, можете да кажете „ очевидно в контекста" и/или „Субектът на данни вече имаше тази информация"**	Обяснете как и кога е направено това **Моля, представете копия от всякакви уведомления или линкове с информация**
- Изисква ли се от тях да предоставят данните и		

какви са последиците, ако не ги предоставят?		
13. **Ако всички или част от данните се обработват на база на критерия „законни интереси”, субектите на данни информирани ли са какъв е законният интерес от въпроса?**		Моля, представете кратко резюме на критериите, приложени при проверката на баланса по отношение на основните права и свободи на субектите на данни съгласно чл. 6, пар. 1, б. „е“) от ОРЗД.
14. **Ако субектите на данни ще бъдат обект на автоматизирано вземане на решение или профилиране, информирани ли са те за следното?**		Моля, представете кратко резюме на логиката, използвана при автоматизираното вземане на решение или профилиране.
- Че ще бъде осъществено това вземане на решение или профилиране?		
- В общи линии (но ясно), каква е използваната „логика”?		
- Какво е значението на автоматизираното вземане на решение или профилиране и предвидените последствия от вземането на решение или профилирането?		

II.5 Потоци от трансгранични данни

[БЕЛЕЖКА: Попълването на поле 17 не е задължително, но пак е полезно за вътрешна оценка]

15. **Прехвърля ли се някаква част от личните данни на трета държава [т.е., извън ЕС/ЕИП] (или сектор в тази държава) или на международна организация, която *е* прието, че предоставя**	*Посочете Да/Не и въпросната държава/и. Ако предаването е само на част от данните, но не на всички данни, посочете за всяка категория данни.*	*Обяснете целта на предаването, напр.: като част от собствените дейности на Вашата организация (напр., при използване на базиран в облака софтуер), или като част от разкриване на данните на трето*

„адекватно" ниво на защита по чл. 45 от ОРЗД?		*лице (моля, посочете това лице/тези лица)*
ВСИЧКИ ДАННИ, ИЗБРОЕНИ В II.1		
***ИЛИ:* Следните данни:** (Копирайте данните от 1 & 2, по-горе)		
-		
-		
-		
-		
-		
-		
-		
-		
-		
-		
-		
-		
Добавете допълнителни редове, ако е необходимо		

16. **Прехвърлена ли е някаква част от данните на трета държава [т.е. извън ЕС/ЕИП] (или сектор в трета държава) или на международна организация, за която <u>не</u> е прието, че осигурява „адекватно" ниво на защита по член 45 от ОРЗД?**	*Посочете Да/Не и въпросната държава/и. Ако предаването е само на част от данните, но не на всички данни, посочете за всяка категория данни.*	*Обяснете целта на предаването, напр.: като част от собствените дейности на Вашата организация (напр., при използване на базиран в облака софтуер), или като част от разкриване на данните на трето лице (моля, посочете това лице/тези лица)*	*Каква гаранция или дерогация подкрепя предаването? Моля, посочете номер от списъка в ***Бележката** по-долу и представете копие на всеки относим документ*
БЕЛЕЖКА: *Ако данните се предават за различни цели на различни получатели в различни държави, моля, отговорете на въпросите отделно за всеки контекст на всяко предаване.*			
ВСИЧКИ ДАННИ, ИЗБРОЕНИ В II.1			
***ИЛИ:* Следните данни:** (Копирайте данните от 1 & 2 по-горе)			

-			
-			
-			
-			
-			
-			
-			
Добавете допълнителни редове, ако е необходимо			

*** БЕЛЕЖКА:** Съгласно ОРЗД, предаване на държави, за които не е прието, че предоставят „адекватна" защита, може да се извършва само ако са въведени „подходящи гаранции", както са изброени в лявата колона по-долу, или ако се прилага дерогация, както са изброени в дясната колона.

Гаранции съгласно чл. 46 от ОРЗД: 1. Международен инструмент между публичните органи; 2. Обвързващи корпоративни правила (ОКП); 3. Одобрени стандартни клаузи за предаване на данни; 4. Кодекс за поведение; 5. Механизъм за сертифициране; 6. Одобрени ad hoc клаузи	Дерогации съгласно чл. 49 от ОРЗД, ако няма гаранции съгласно чл. 46 (вж. Насоките на Европейския комитет по защита на данните в това отношение: преписано е ограничително приложение и тълкуване): 7. Съгласие; 8. Договор между администратора и субекта на данни 9. Договор между администратора и трето лице 10. Необходимо поради важни причини от обществен интерес 11. Необходимо за правни претенции; 12. Необходими, за да бъдат защитени жизненоважните интереси на субекта на данните или на други лица; 13. Предаването се извършва от регистър, достъпен за обществеността

17. **Има ли въведени правила за процедиране при каквото и да решение на съд или трибунал и каквото и да е решение на административен орган на трета държава, което може да бъде връчено на администратора или който и да е обработващ лични данни, изискващо администраторът или обработващият лични данни да предаде или разкрие лични данни?** (Срв. чл. 48 от ОРЗД)	*Посочете Да/Не и ако да, моля, представете копие от насоките.*

III. СИГУРНОСТ И ПОВЕРИТЕЛНОСТ

БЕЛЕЖКА: Ако отговорите на въпросите по-долу се различават за различните данни, моля, отговорете им поотделно за всеки отделен набор от данни.	*Моля, посочете допълнителни подробности:*

Личните данни, изброени в II.1 на хартиен носител ли се съхраняват или в електронен формат? Ако са на хартия, съхраняват ли се в структуриран ръчен сборник (досие с данни)?	
Къде (физически) се съхраняват данните? (Вашите офиси? На сървъри при основния администратор? На сървъри на свързана организация? На сървъри на трето лице (напр., Доставчик на облачни услуги)?	
Какви мерки са въведени за защита срещу неразрешен достъп до физическото(ите) място(места), където се съхраняват/са достъпни данните? Има ли въведена политика за сигурност на данните, която урежда това? (*Ако да, моля, представете копие*.)	
Какъв хардуер се използва при обработването на данните? Кой отговаря за управлението и сигурността на този хардуер?	
Съхраняват ли (някои от) данните на преносими носители/устройства? Какви са тези носители/устройства? Кой ги съхранява?	
Може ли някое от лицата с достъп до данните да използва лични устройства за достъп или обработване на данните? Ако да, има ли политика за Носене на собствено устройство (BYOD) по този въпрос? *Моля, представете копие от политиката.*	
Всички лица ли са с право на достъп до личните данни при спазване на задължение за поверителност (било то съгласно законов или професионален набор от норми или съгласно договор)? *Моля, представете подробности или копия, на които и да е относими норми или договорни клаузи.*	
Какъв софтуер/приложения се използва/т при обработването на данните? (Напр., десктоп MS Office пакет, централно	

управлявано приложение, облачна услуга и т.н.)	
- Този софтуер на местно или на централно ниво се управлява? Ако е на централно ниво, кой е централният орган? Ако това не сте Вие, има ли формална договореност между този субект и Вашата организация относно използването на софтуера? *Моля, представете копие на тази договореност.*	
- Софтуерът използва ли „облак”? Ако да, кой е Доставчикът на облачни услуги и къде е базиран този доставчик? И къде е/са разположен/и физически облачния/те сървър/и? Данните на облачния сървър напълно ли са криптирани? Как (т.е., с каква технология на криптиране)? *Моля, представете копие от договора, съгласно който се извършва това обработване.*	
- Кой отговаря (т.е., кой има „администраторски” правомощия) във връзка с този софтуер? (Вие? Някой друг в рамките на Вашата организация? Някой в централна организация, с която сте свързани? Някой друг?)	
Предават ли се данните в някакъв момент/ при някакви обстоятелства електронно на друг носител, система или устройство?	
Ако те са електронно предавани, прави ли се това: - по интернет? Ако е така, данните криптирани ли са? Как (т.е., с каква технология за криптиране)? - посредством FTP? Как се обезпечава сигурността на това? - посредством VPN? Как се обезпечава сигурността на това? - друго – *моля, посочете*	

- o – O – o -

ЗАДАЧА 2: Преглед на дейностите по обработване на лични данни

След като създаде регистър на дейностите по обработване на лични данни на организацията си , (Задача 1) следващата стъпка за длъжностното лице по защита на данните е извършването на задълбочен **преглед** на всички регистрирани дейности по обработване на лични данни, за да прецени дали отговарят на изискванията на ОРЗД във всички приложими аспекти, включително във връзка с:

- посочване и ограничаване на целите;
- действителност на което и да е съгласие (и съществуването на документирано доказателство за даденото съгласие) или приложимостта на каквито и да е други правни основания за обработването;
- обработените лични данни и тяхната относимост и необходимост във връзка с посочената цел(и));
- качество на данните (точност, актуалност, и т.н., на данните, както и свеждане на данните до минимум и псевдонизимизация);
- информация, предоставена на субекта на данни по инициатива на администратора (независимо дали данните са събрани от субекта на данни или по друг начин, или при искане – също във връзка с данни, събирани от посетители на уебсайта);
- периодът от време, за който данните се запазват във форма, която позволява идентифициране и всякаква информация относно де- идентификация;
- техническа, организационна и физическа сигурност на данните (включително ограничение на физическия достъп и ограничение на техническия достъп до данните[потребителско име, пароли, политики за ПИН, и т.н.], криптиране, и т.н.);
- трансгранични трансфери на данни (правните и други договорни, и други споразумения за тях);
- и други.

Въз основа на констатациите по по-горните точки, длъжностното лице по защита на данните следва да може да **оцени**:

- дали операцията по обработването ***като цяло*** може да бъде счетена за съответстваща на ползващия се с предимство принцип на законосъобразност и добросъвестност.

(Отбележете, че тази оценка на съответствието с ОРЗД е отделна и различна от оценката на риска, описана по-долу като Задача 3).

Записите по дейностите по обработване на лични данни на лицата, създадени в Задача 1 (по-специално, ако са създадени в по-подробния формат)[327] следва да формират основата на прегледа, като водят до задаването на съответните въпроси от длъжностното лице по защита на данните и даването на отговори по тях, включително, по-специално:

[327] Предоставени в примерния формат на подробен запис по обработване на лични данни, приложен в Задача 1.

- Дали е достатъчно ясно, кой бизнес отдел е "**отговорник за дейността**" по отношение на дейностите по обработване на лични данни (т.е., кой има ежедневната фактическа отговорност за обработването)? Това предвидено ли е е в **официален документ** (напр., специфични указания от администратора към отдела)?

- Дали **целта**, или **целите**, на операцията по обработване на личните данни е посочена достатъчно точно? Къде (т.е. в какъв вид **документ**)? Ако личните данни използвани в операцията по обработването са използвани за повече от една цел, каква е ***основната цел*** и каква е или са ***второстепенната цел(и)***? Дали тези второстепенни цели са ***съвместими*** с основната цел, или са отделни цели?

  БЕЛЕЖКА: При оценката на съвместимостта на всяко обработването на второстепенната цел с основната цел , длъжностното лице по защита на данните трябва да вземе предвид въпросите, посочени в чл. 6 пар. 4 от ОРЗД.

  Дали всички цели, за които се обработват личните данни са напълно обосновани и легитимни?

  - Дали обработваните лични данни са **адекватни**, **относими** и **необходими** за основната цел? Как се гарантира, че те са и продължават да бъдат **точни** и **актуални** за тази цел, и какви мерки са взети, за да се гарантира това и за ***коригиране*** или ***актуализиране*** или ***изтриване*** на неточна или неактуална информация?

    Дали предприетите мерки са подходящи и достатъчни? Възможно ли е същата цел да бъде постигната с по-малък риск за неприкосновеността и другите права на засегнатите физически лица?

  - Какви лични данни са използвани или разкрити за каквито и да е второстепенни цели или действително нови, несвързани цели (обикновено с трета страна)? Дали обработваните лични данни са **адекватни**, **относими** и **необходими** за тези второстепенни или нови, несвързани цели? (Ако всички данни, събрани за една [основна] цел, са разкрити прибързано за дадена/каквато и да е второстепенна цел или цели или нова, несвързана цел, те или някои от тях, биха могли да бъдат доста прекомерни за тази второстепенна или несвързана цел или тези вторични или несвързани цели. Дали това е било взето предвид?)

    БЕЛЕЖКА: Виж подробния формуляр за обработване на лични данни, в II.2.

    Дали всички второстепенни цели, за които се обработват личните данни, са напълно обосновани и легитимни?

- Как се гарантира, че данните, които са използвани или разкривани за второстепенни или нови, несвързани цели *са* **точни** и **актуални** за тези второстепенни или нови цели към момента на първото им използване или разкриване за тези цели, и какви мерки са предприети , за да се гарантира, че те *остават* **точни** и **актуални** след първото използване или разкриване, и че са ***коригирани*** или ***актуализирани*** или ***изтрити,*** както и когато станат неточни или неактуални? Адекватни и достатъчни ли са съответните мерки?

  NB: Ако данните са използвани или разкрити за повече от една второстепенна или нова цел, на тези въпроси следва да бъде даден отделен отговор, за всяко едно поотделно второстепенно или ново използване или разкриване.

- **Кога, как, от кого и в каква форма** са получени **съответните** лични данни? Напр.: субектът на данни, държавна институция, (бивш) работодател, и т.н.; напр. на хартиен носител, чрез електронен превод и т.н..

  Бележка: На този въпрос следва да бъде даден отговор, както за **нечувствителни,** така и за **чувствителни данни**, и в случай, че се получават различни данни от различни източници, това следва да бъде посочено. Виж подробен формуляр за обработване на лични данни, в II.1 и II.2.

  Подходящи ли са тези източници? Биха ли могли някои от данните, получени от трети страни, да бъдат получени чрез поискване от самите субекти на данни?

- **Колко дълго се пазят** личните (не-чувствителни и чувствителни) данни? **Какво се случва в края на този период**? (Напр.: ***изтриване***, ***унищожаване***, ***превръщане на данните в анонимна форма*** – или в ***псевдонимизирана*** форма – но имайте предвид, че последното означава, че данните все още се пазят във форма, която позволява идентифициране).[328] Ако данните се пазят в анонимна или псевдонимизирана форма, ***защо*** се прави това? (Напр., за изследователски или исторически цели? Ако е така, обработването за тази цел следва да бъде оценявано отделно за съвместимост с ОРЗД.)

  Бележка: Периодът на пазене може да бъде посочен, като конкретен период или събитие, напр. "7 години" или "До 5 години след прекратяване на трудовото правоотношение". Имайте предвид, че съществуват официални стандарти за препоръчаните методи за изтриване/унищожаване на данни за различните категории данни и носители на данни.[329] Длъжностното лице по защита на данните следва да

---

[328] Отбележете, че съгласно ОРЗД (както и съгласно Директивата за защита на данните от 1995 г.) за личните данни може да се каже, че са превърнати в анонимна форма само, ако те повече не могат да бъдат свързани с конкретно физическо лице от *никого* – т.е. не само от администратора (но и от колеги, близки и приятели, които могат да намерят данните в предполагаема неидентификационна форма в Интернет или на изхвърлена хартия). В това отношение, длъжностните лица по защита на данните следва да са наясно, че все повече данни, които може да изглежда, че са "не-лични", или за които се смята, че са "превърнати в анонимна форма" могат все по-лесно да бъдат (отново) свързани с конкретни физически лица. В частност, данните в предполагаеми "анонимни" "Големи масиви" набори от данни често неочаквано и притеснително дават възможност за повторна идентификация, особено, ако различни набори от данни бъдат свързани или "съпоставени". В допълнение, ако дори действително нелични набори от данни бъдат използвани за създаването на "профили" (независимо дали на типичните потребители на определен продукт, или на типични пациенти, или на типични престъпници или терористи), и тези профили след това бъда приложени към набори от данни, за да отделят физически лица, които отговарят на профила – тогава това обработване също може много сериозно да засегне тези физически лица, на които може да им бъде отказана застраховка, работа или достъп до полет или дори до държава (или по-лошо) въз основа на реално неоспорими алгоритми. Вж.: Дау Корф и Мари Жорж, Passenger Name Records, data mining & data protection: the need for strong safeguards (Записи на имената на пътници, добиване на данни и защита на данните: нуждата от силни мерки за защита), доклад за Консултативния комитет по защита на данните към Съвета на Европа, юни 2015 г., документ T-PD(2015)11, раздел I.iii, на Съвет на Европа, *The dangers inherent in data mining and profiling (Опасностите, присъщи на извличането на данни и профилирането),* достъпен на: https://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_документ/T-PD(2015)11_PNR%20draft%20report%20Douwe%20Korff%20&%20Marie%20Georges_15%2006%202015.pdf

[329] Вж. например:

- DIN Германския институт по стандартизация (German Institute for Standardization), Офис-машини – унищожаване на носители на данни (Office machines - Destruction of data carriers), DIN 66399, октомври 2012.

провери дали тези стандарти са спазени (специално по отношение на чувствителна информация или в правния смисъл на защита на данните или в по-широк социален или политически смисъл.

Подходящи ли са периодите на пазене на данни ? Или твърде дълги? Дали мерките за изтриване/унищожаване на данни са в съответствие с националните и международни стандарти? Ако данните се пазят извън обичайните срокове за съхранение в анонимизирана или псевдонимизирана форма: (i) дали това е подходящо с оглед на целта на удълженото съхранение? Дали данни, в псевдонимизирана форма, могат да бъдат пазени в изцяло анонимизирана форма и все още да бъдат достатъчни за специалната цел? Колко вярно е всяко твърдение, че дадени данни са „анонимизирани"? (Имайте предвид, че пълната анонимизация е все по-трудна за постигане, особено в големите масиви от данни и по-специално, ако е позволено набори от данни да бъдат съчетани или свързани с други набори от данни.)

- На кои трети страни се разкриват горепосочените данни? И **за какви цели**? Данните, които се разкриват са ***адекватни***, ***относими*** и ***необходими*** за тези цели, ***точни*** и ***актуални***, и ако е така, как се гарантира, че остават такива?

  Бележка: Отговорите на горепосочените въпроси могат отчасти да препращат към отговорите на въпроси, обсъдени по-горе.

- На какво **правно основание /правни основания** се обработват личните данни?

Бележка:

За нечувствителни данни, правното основание трябва да бъде едно от тези, посочени в Чл. 6 от ОРЗД, а за чувствителни данни, едно от тези, посочени в Чл. 9 от ОРЗД.

Обърнете внимание, че основанието за обработване "легитимен интерес" (чл. 6, пар. 1, б. „е") не се прилага за обработване на каквито и да е данни – включително нечувствителни данни – от публични органи, при изпълнението на техните задачи (чл. 6, пар. 1, последно изречение) и не може да се позовава на никой администратор, независимо дали в публичния или в частния сектор, за обработване на чувствителни данни (виж чл. 9).

Освен това, ако обработването се основава на чл. 6, пар. 1, б. „в" или „д" ("обработването е необходимо за спазване на законово задължение, което се прилага спрямо администратора", "обработването е необходимо за изпълнението на задача от обществен интерес или при упражняването на официални правомощия, които са предоставени на администратора"), това трябва да бъде основано на правото на Европейския съюз или на държава членка на ЕС (чл. 6, пар. 3). Ако посоченото правно основание е някое от гореизброените, длъжностното лице по защита на данните трябва

- NIST Специална публикация 800-88 Редакция 1, Насоки за изчистване на носители (Guidelines for Media Sanitization), декември 2014, на http://dx.doi.org/10.6028/NIST.SP.800-88r1
- Национална агенция по сигурността на САЩ/Централна служба по сигурността (US National Security Agency/Central Security Service), Наръчник за унищожаване на носители (Media Destruction Guidance), на https://www.nsa.gov/ia/mitigation_guidance/media_destruction_guidance/index.shtml

да провери дали съответният правен акт отговаря на изискванията, посочени в чл. 6, пар. 3 от ОРЗД.

Подходящо ли е правното основание за обработване на данните? Спазени ли са съответните условия за прилагане на правното основание (напр. по отношение на съгласието, което е разгледано по-долу)?

Имайте в предвид, че правното основание за обработване на основната цел, може да бъде различно от правното основание, за което и да е друго обработване (включително използване или разкриване), на които и да е данни, за каквато и да е второстепенна или нова, несвързана цел(и) – и валидността на правното основание трябва да бъде оценена, отделно за всяка от тях.

- Ако данните се обработват на основание **съгласие** на субектите на данни:
  - ***как и кога*** е получено съгласието (напр. в хартиена или електронна форма, чрез пряк въпрос или като се поиска от дадено лице да постави отметка в кутия)?[330]
  - какво ***доказателство*** се съхранява за това, че съгласието е било дадено (напр. хартиени копия, дневници)?
  - как и за какъв период от време се ***пази*** това доказателство?
  - ако в контекста на договор, Вашата организация иска повече данни от необходимите за договора, дали субектът на данни ***е уведомен, че не е необходимо той/тя да предоставя допълнителни данни***?
- Информирани ли са **субектите на данни** по всички въпроси, за които е необходимо да бъдат информирани (вж чл. 13 и чл. 14 от ОРЗД, както е предвидено във формуляра за подробно обработване на лични данни, в II.4), и ако е така, кога и как?

  Предоставена ли е цялата необходима информация? Направено ли е в най-добрият формат? В най-добрия момент? Задължителните за попълване полета отличават ли се ясно от незадължителните?
- Прехвърлят ли се някои от данните **към трета [т.е., извън ЕС/ЕИП] държава** (или сектор в трета държава) или към **международна организация,** за която *е* прието, че предоставя "адекватно" ниво на защита, съгласно чл. 45 от ОРЗД?

  Дали съответното решение за адекватност действително покрива обработването? Все още ли е валидно (виж заключението на Съда на Европейския съюз, а именно, че решението за адекватност на "Safe Harbor" е било недействително)?

[330] Следва да се отбележи, че просто изявление на уебсайт, което казва: „*Като продължавате да използвате този уебсайт, вие се съгласявате със събирането и използването на личните ви данни*" вече не е достатъчно да съставлява валидно съгласие съгласно ОРЗД. Не само, че това е недостатъчна информация за използването на данните – което прави „съгласието" недействително, тъй като но не е „информирано съгласие". Но също така, е съмнително дали продължаването към уебсайта може да се смята, че съставлява „*недвусмислен знак за желанията на субекта на данни*" за такова съгласие (срв. определянето на съгласието в Член 4, параграф 11 от ОРЗД).

- Прехвърлят ли се някои от данните **към трета [т.е., извън ЕС/ЕИП] държава** (или сектор в трета държава) или към **международна организация,** за която **не** е прието, че предоставя „адекватно" ниво на защита съгласно чл. 45 ОРЗД? Ако е така, каква гаранция или дерогация подкрепя прехвърлянето?

  Бележка: Съгласно Регламента, прехвърлянията към държави, за които не се счита, че предоставят "адекватна" защита може да се осъществи само, ако са налице „**подходящи гаранции**", както са изброени в чл.46 от ОРЗД, *или* ако се прилага **дерогация**, както е посочено в чл. 48 от ОРЗД (виж раздел II.5 във формуляра за подробно обработване на лични данни, въпрос 16).

  Споменати ли са защитните мерки или дерогацията(ите) правилно? Дали отговарят на всички изисквания, посочени в съответния член (чл. 46 или 48)?

- Дали има налични правила за процедиране в случай на решение на съд или трибунал и каквото и да е решение на административен орган на трета държава, което може да бъде връчено на администратора или на обработващия лични данни, като изисква от администратора или обработващия лични данни да прехвърли или разкрие лични данни?

  Бележка: Съгласно чл. 48 от ОРЗД, съдебни решения и решения на трети държави „могат да бъдат признати или да подлежат на изпълнение, по какъвто и да било начин, само ако се основават на международно споразумение, като договор за правна взаимопомощ, което е в сила между третата държава, отправила искането, и Съюза или негова държава членка, без да засягат другите основания за предаване на данни съгласно настоящата глава." Това е труден въпрос за преценка за собствениците на бизнес и много администратори и обработващи лични данни, и следва да са налице насоки за това как собствениците на бизнес и администраторите и обработващите лични данни следва да действат, ако се случи да им бъде представено такова съдебно решение или друго решение. Най-малко, обработващите лични данни и собствениците на бизнес следва, незабавно да отправят въпроса към най-високото управленско ниво на администратора, и длъжностното лице по защита на данните.

  Ако има съответни насоки, адекватни ли са (напр. дали са приети преди пълното прилагане на ОРЗД, може да не са споменали включването на длъжностното лице по защита на данните по тези въпроси, тъй като може да не е съществувало длъжностно лице по защита на данните към момента на изготвяне на насоките)? Ако все още няма насоки по това, следва да бъдат спешно изготвени такива, които да предвиждат длъжностно лице по защита на данните в съдържанието си.

- Какви формални, организационни, практически и технически мерки са налице за гарантиране сигурността и поверителността на данните?

  Бележка: Съгласно чл. 32 от ОРЗД, администраторите и обработващите лични данни трябва да приложат „подходящи технически и организационни мерки, за да гарантират ниво на сигурност, съответстващо на риска (рисковете)", което обработването оказва върху правата и свободите на физическите лица (включително по-специално субектите на данни). Този член изброява различни мерки като псевдонимизация и криптиране, клаузи за поверителност, технически мерки за осигуряване на цялостност, достъпност и устойчивост на използваните системи и възможностите за възстановяване.

  Въпросът ще бъде допълнително разгледан в Задача 3 (оценка на риска). **Първоначален преглед** на предприетите мерки (или непредприетите мерки) следва да бъде направен още в контекста на Задача 2, за да даде **предварителна**

индикация за това дали предприетите мерки са "подходящи" в светлината на „достиженията на техническия прогрес, разходите за прилагане и естеството, обхватът, контекстът и целите на обработването, както и рисковете с различна вероятност и тежест за правата и свободите на физическите лица" (както е посочено в чл. 32).

Много (макар и не всички) от мерките, са обхванати от признати международни стандарти, като тези, изброени по-долу. Следва обаче да се отбележи, че те не винаги покриват всички относими въпроси, напр. те по-скоро се фокусират върху сигурността, отколкото върху минимизирането на данните или ограниченото на целта.[331]

Дори така, **длъжностните лица по защита на данните следва да са наясно със стандарти** като тези – и да **проверят, дали техният орган по защита на данните или Европейският комитет по защита на данните е направил коментар** (положителен, отрицателен или в допълнение):[332]

- ISO/IEC 27001:2013 Практически кодекс за контрол на информацията
- ISO/IEC 29100 – Информационни технологии — Методи за сигурност — Рамка на неприкосновеност
- ISO/IEC 27018 - Кодекс за добра практика за защита на лични данни (PII) в обществени облаци, действащи като обработващи лични данни на PII
- ISO/IEC 29134 – Насоки за оценка на въздействието върху неприкосновеността на личните данни (PIA)
- ISO/IEC 29151 – Кодекс с добри практики за защитата на личната информация
- JIS 15001:2006 – Изисквания към системата за управление на защитата на лични данни
- BS 10012:2017 – Спецификация за система за управление на личната информация

Допълнителни стандарти в процес на изготвяне:

- ISO 20889 – Методи за де-идентификация на данни, подобряващи неприкосновеността
- ISO 29184 – Уведомления за неприкосновеност и съгласие онлайн
- ISO 27552 Подобрение към ISO/IEC 27001 за управление на неприкосновеността – Изисквания → Ново заглавие: Допълнение към ISO/IEC 27001 и ISO/IEC 27002 за управление на неприкосновеността на информацията – Изисквания и насоки

---

331 Преди няколко години, органи по защита на данните забелязват, че ISO документ за сигурността, който обхваща PIN кодове, не посочва броя и естеството на знаците, които следва да бъдат използвани. Оттогава, Органите по защита на данните имат политика да взаимодействат, колкото може повече с ISO стандарти, чиито дейности са свързани с какъвто и да е субект на защита на данните

332 Източник: Alessandra de Marco, презентация към първата обучителна сесия "T4DATA, юни 2018, слайдове за "*съществуващите стандарти (за сигурността и неприкосновеността)*" и "*Стандарти (за неприкосновеността), незавършени към момента*".

- UNI Референтна практика – Насоки за управление на личните данни в ИКТ среда съгласно ОРЗД

Ако при обработването е използван "облак", следва да бъде взето предвид и дали са обсъдени въпросите, изброени в "Доверен облак – Профил на защита на данните за облачни услуги (TCDP)", насоки, издадени от пилотен проект ,подкрепян от немското правителство "Сертифициране за Защита на данните за облачни услуги" (въпреки, че към момента те все още се позовават на Федералния закон за защита на данните от преди ОРЗД, вместо на ОРЗД).[333]

На този етап, длъжностното лице по защита на данните следва да провери дали администраторът и/или собствениците на бизнес са запознати с горепосочените стандарти и се стремят да ги прилагат, и ако е така, дали имат сертификати. Въпросът дали те са действително изпълнени, или следва да бъдат, може да бъде разгледано в Задача 3 (оценка на риска).

Този преглед е първият етап от функцията на длъжностното лице по защита на данните "*Текущ мониторинг на съответствието*" (отбелязано след Задача 4).

Ако в каквото и да е отношение, според длъжностното лице по защита на данните дадена операция по обработване на лични данни не отговаря, на които и да е от изискванията на ОРЗД, длъжностното лице по защита на данните трябва **да уведоми** съответното отговорно лице или лица, вътре в организацията за недостатъците, и да предложи действие за поправянето им (до и включително спирането на операцията като цяло, ако е необходимо). В случай, че това уведомление не бъде последвано от действие, длъжностното лице по защита на данните следва да отправи въпроса към най-висшето ръководство (вж. по-долу под "*Консултативни задачи*").

Имайте предвид, че този общ преглед на дейностите по обработване е отделен въпрос от случая на нарушение на личните данни, обсъден във връзка със Задача 6 ("*Процедиране при нарушения на лични данни*"): тези нарушения следва да бъдат *незабавно* докладвани на най-висшето ръководство.

Длъжностното лице по защита на данните, следва да пази пълни **записи** на всички негови прегледи и оценки, и на такива уведомления.

- o – O – o -

[333] Вж.: https://tcdp.de/data/pdf/14_TCDP_v1.0_EN.pdf (вж. в частност списъка със стандарти на стр. 14 – 16). Версията, достъпна към момента на писането (в.1.0) датира от септември 2016, но авторите се надяват, че – след създаването на подкрепени от ОРЗД стандарти за одит и процедури по сертифициране – "*TCDP схемите за сертифициране ще бъдат превърнати в схеми за сертифициране съгласно Общия регламент относно защитата на данните за облачни услуги.*" (стр. 7). Срв. също обсъждането на рисковите фактори, и т.н., идентифицирани от Европейския надзорен орган по защита на данните във връзка с облачни услуги, обсъдени в Задача 3, по-долу.

ЗАДАЧА 3: Оценка на рисковете, предизвикани от дейностите по обработване на лични данни

Както е отбелязано в точка 2.4.1 по-горе, Общият регламент относно защитата на данните налага общо задължение на *администраторите* да „[вземат] предвид естеството, обхвата, контекста и целите на обработването, както и **рисковете с различна вероятност и тежест за правата и свободите на физическите лица**", които се предизвикват от всяка операция по обработване на лични данни, и да „въвежда[т] подходящи технически и организационни мерки, за да гарантира[т] и да [са] в състояние да докаже[ат], че обработването се извършва в съответствие с настоящия регламент" (чл. 24, пар. 1); вж. също чл. 25, пар. 1)).

Длъжностното лице по защита на данните, също така:

> при изпълнението на своите задачи надлежно отчита рисковете, свързани с дейностите по обработване, и се съобразява с естеството, обхвата, контекста и целите на обработката.
>
> (чл. 39, пар. 2)

Спазването на тези изисквания, изисква да се установят съответните рискове. Това следва да се направи във връзка с извършването на опис на дейностите по обработване на лични данни и създаването на регистър на тези дейности (Задача 1) и по-специално с прегледа на тези дейности (Задача 2).

Общият регламент относно защитата на данните не изисква изрично участието на длъжностното лице по защита на данните във всички общи оценки на риска: той предвижда такова участие единствено във връзка с по-задълбочените Оценки на въздействието върху защитата на данните (чл. 35, пар. 2) – вж. Задача 4, по-долу). На практика обаче е силно препоръчително (най-малкото) да се включи длъжностното лице по защита на данните, както и в тези по-общи оценки на риска. Действително, оценката често ще зависи от мнението на длъжностно лице по защита на данните.

Следва да се отбележи, че рисковете, които трябва да бъдат оценени, са не само рисковете за сигурността в тесен смисъл, т.е. вероятността от възникване на **нарушението на сигурността на данните** и неговото въздействието[334] – а по-скоро рисковете за **правата и свободите на субектите на данни (и други лица)**, които могат да бъдат предизвикани от операцията по обработване. Това включва не само техните, общи права на неприкосновеност на личния живот и на личен живот, както и техните специфични права на субекти на данни, но също така, в зависимост от случая, техните права на свобода на изразяване, свобода на движение, свобода от дискриминация, свобода от авторитарна власт, правомощия и правото да останат в демократично общество без неправомерно наблюдение от техните собствени или от други държави, както и от правото на ефективно правно средство за защита. Концепцията е всеобхватна.[335]

---

[334] „**Нарушение на сигурността на лични данни**" е определено в Общия регламент относно защита на данните като: „нарушение на сигурността, което води до случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до лични данни, които се предават, съхраняват или обработват по друг начин." (Член 4, параграф 12). Вж. Задача 6, по-долу.

[335] Вж. разглеждането на значението на „риск" и „висок риск", съответно в Задача 1 (в точка „*Освобождаване*") и Задача 4.

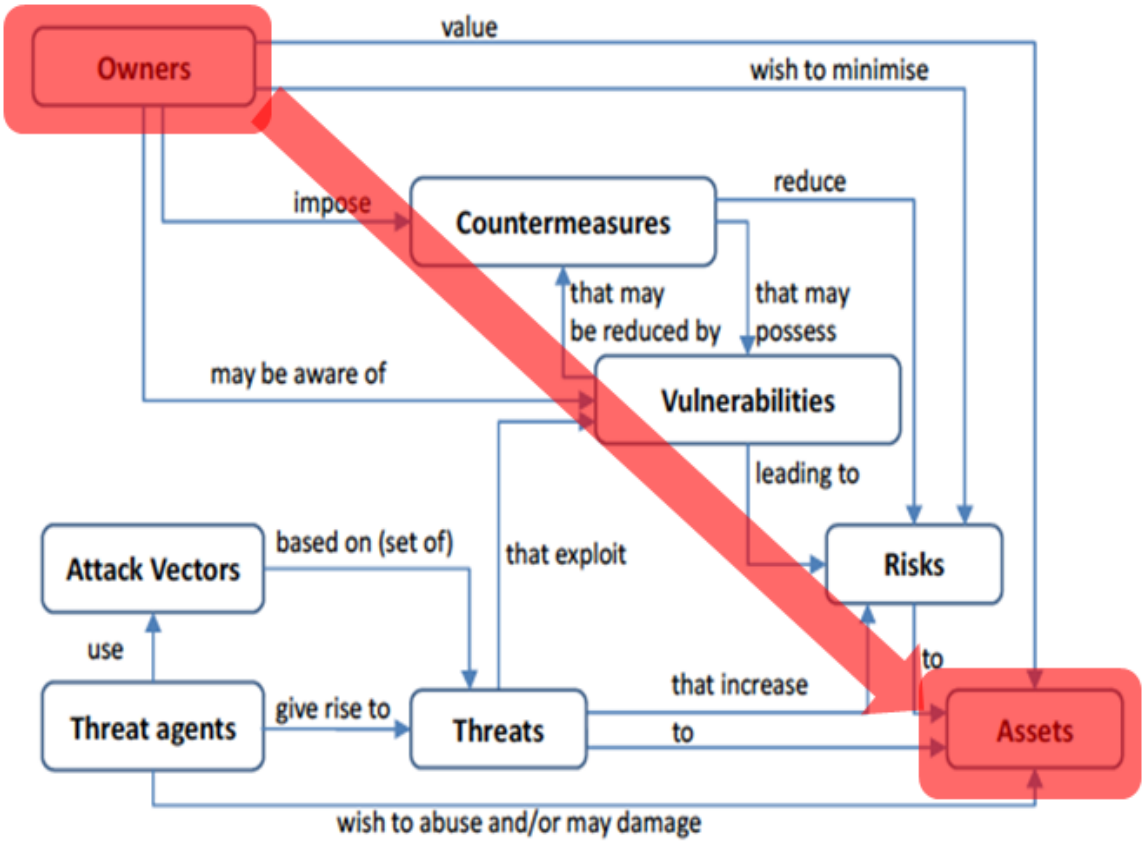
Общата оценка на риска следва, също така да вземе предвид, констатациите в Задача 2. Например, ако се установи, че въпреки че конкретна операция по обработване, като такава, е била законосъобразна (т.е. имала е подходящо законно основание и е обслужвала законен интерес), но че са били събрани и държани неотносими и прекомерни данни за съответната цел, противно на принципа на „свеждане на данните до минимум" – тогава може да се каже, че тя сама по себе си предизвиква „риск", т.е. че неотносимите и ненужните данни биха били неправилно използвани. В такъв случай подходящата мярка за избягване на този риск би била да се спре събирането на неотносимите и ненужни данни и да се изтрият всички такива съхранявани данни. Друг пример би бил използването на все още идентифицируеми данни в статистическото обработване, което може да бъде извършвано с помощта на псевдонимизирани или дори напълно анонимизирани данни – в този случай подходящата мярка би била да се гарантира, че използваните данни ще бъдат правилно (сериозно) псевдонимизирани или (за предпочитане) напълно анонимизирани.

Всичко това подчертава, че за общия преглед (Задача 2) и оценката на риска (настоящата Задача 3) администраторът – на практика длъжностното лице по защита на данните – трябва внимателно да разгледа **всички аспекти** на **всяка отделна операция и функция по обработване на лични данни.**

Както е предложено от италианския орган по защита на данните, *Garante*, полезно е да се следва подходът, възприет от ENISA (Агенцията на ЕС за мрежова и информационна сигурност), който от своя страна се основава на широко приетия стандарт ISO 27005: „*Уязвимост от злоупотреби със заплахи за активите за причиняване на вреди на организацията*"; и да се разгледа по-подробно **рискът**, като съставен от следните ***елементи***:

Актив (уязвимости, механизми за контрол)**, Заплаха** (профил на представляващ заплаха агент, вероятност) **и Въздействие**.

Елементите на риска и техните взаимоотношения могат да бъдат илюстрирани както следва:



Източник: ENISA Доклад за състоянието на заплахите от 2016 г., Фигура 4: Елементите на риска и техните взаимоотношения съгласно ISO 15408: 2005, https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016. Вж. също доклада за 2017 г., https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017.

Както още е посочено от *Garante*, **надлежната оценка на риска включва четири стъпки**:[336]

1. Определяне на операцията по обработване и нейния контекст.
2. Разбиране и оценка на въздействието.
3. Определяне на възможни заплахи и оценка на вероятността от възникването им (вероятност от възникване на заплаха).
4. Оценка на риска (съчетаване на вероятността от възникване на заплаха и нейното въздействие).

Първото (определяне на операцията по обработване и нейния контекст) беше направено в Задачи 1 и 2 по-горе.

Втората стъпка включва **определяне на различни нива на въздействие** – които могат разумно да бъдат оставени на четири нива, както следва:[337]

[336] Джузепе д'Акуизиро, презентация на първата обучителна сесия по „T4DATA" относно сигурността на данните, юни 2018 г., слайд за *„Оценка на риска (фокус върху сигурността)*".

[337] *Вж.*, слайд за *„Разбиране и оценяване на въздействието*".

НИВО на въздействие	Описание
Ниско	Лицата могат да се сблъскат с някои незначителни неудобства, които ще преодолеят без никакъв проблем (време, прекарано в повторно въвеждане на информация, досада, раздразнение и т.н.).
Средно	Лицата могат да се сблъскат със значителни неудобства, които ще могат да преодолеят въпреки някои трудности (допълнителни разходи, отказ на достъп до бизнес услуги, страх, липса на разбиране, стрес, незначителни физически неразположения и др.).
Високо	Лицата могат да се сблъскат със значителни последствия, които те би следвало да могат да преодолеят, макар и със сериозни затруднения (злоупотреба със средства, поставяне в черни списъци от финансови институции, имуществени вреди, загуба на работа, призовка, влошаване на здравето и т.н.).
Много високо	Лица, които могат да срещнат значителни или дори необратими последствия, които те не могат да преодолеят (неспособност за работа, дългосрочни психологически или физически неразположения, смърт и т.н.).

Garante отбелязва **четири основни области за оценка** по отношение на **сигурността на данните**, т.е.:

A. Мрежови и технически ресурси (хардуерно оборудване и софтуер)

B. Процеси/ процедури, свързани с обработването на данните

C. Различни страни и хора, участващи в операцията по обработване

D. Бизнес сектор и мащаб на обработването

За всяка зона за оценка, той поставя **пет въпроса**, положителният отговор, на които е индикация за риск, както е посочено в таблицата, на следващата страница.[338]

Лицето, което извършва оценка на риска за сигурността може на базата на тези отговори, да изчисли **вероятността от възникване на заплаха**, както е посочено в двете диаграми в тази точка след таблицата.

Резултатът може да се комбинира с оценка на въздействието, за да се получи **цялостна оценка на риска**, както е посочено в диаграмата .

[338] Същото се отнася и за всяка от четирите основни области на оценка, с допълнително обяснение защо един положителен отговор на въпроса във всеки случай предизвиква риск за сигурността.

ЧЕТИРИТЕ ОСНОВНИ ОБЛАСТИ НА ОЦЕНКА ОТ ГЛЕДНА ТОЧКА НА СИГУРНОСТТА НА ДАННИТЕ:

А. Мрежови и технически ресурси:	**Б. Процеси и процедури**	**В. Включени страни и хора**	**Г. Бизнес сектор и мащаб**
1. Дали някоя част от обработката на лични данни се извършва през интернет?	**6.** Дали ролята и отговорностите по отношение на обработването на личните данни са неясни или неясно определени?	**11.** Обработването на лични данни от неопределен брой служители ли се извършва?	**16.** Смятате ли, че вашият бизнес сектор е предразположен към кибератаки?
2. Възможно ли е да се осигури достъп до вътрешна система за обработване на данни през интернет (например за определени потребители или групи от потребители)?	**7.** Приемливото използване на мрежата, системата и физическите ресурси в рамките на организацията са неясни или неясно определени?	**12.** Има ли част от обработването на данните, която да се извършва от изпълнител / трета страна (обработващ лични данни)?	**17.** Вашата организация претърпявала ли е някаква кибератака или друг вид нарушения на сигурността през последните две години?
3. Системата за обработване на лични данни свързана ли е към друга външна или вътрешна (към вашата организация) ИТ система или услуга?	**8.** Разрешено ли е на служителите да носят и използват свои собствени устройства за свързване към системата за обработване на лични данни?	**13.**Дали задълженията на страните/ лицата, участващи в обработването на лични данни, са нееднозначно или неясно посочени?	**18.** Получавали ли сте някакви уведомления и/или оплаквания във връзка със сигурността на ИТ системата (използвана за обработване на лични данни) през последната година?
4. Могат ли неоторизирани лица да имат лесен достъп до средата за обработка на данни?	**9.** Служителите имат ли право да прехвърлят, съхраняват или обработват по друг начин лични данни извън помещенията на организацията?	**14.** Участва ли персонал в обработката на лични данни, който не е запознат с въпросите на информационната сигурност?	**19.** Дали дадена операция по обработване се отнася до голям брой лица и/или лични данни?

5. Системата за обработване на личните данни проектирана, внедрена и поддържана ли е без да се следват съответните добри практики?	**10.** Могат ли дейностите по обработване на лични данни да се извършват без създаването на лог файлове (файлове дневници)?	**15.** Лицата / страните, участващи в дейностите по обработване на данните, пропускат ли да съхраняват и/или унищожават по сигурен начин лични данни?	**20.** Налични ли са някакви добри практики в областта на сигурността, специфични за Вашия бизнес сектор, които не са били адекватно последвани?

ВЕРОЯТНОСТ ОТ ВЪЗНИКВАНЕ НА ЗАПЛАХА (1):

Област на оценка:	Брой отговори „да”	Ниво	Резултат
А. Мрежови и технически ресурси:	0 – 1	Ниско	**1**
	2 – 3	Средно	**2**
	4 – 5	Високо	**3**
Б. Процеси и процедури	0 – 1	Ниско	**1**
	2 – 3	Средно	**2**
	4 – 5	Високо	**3**
В. Включени страни и хора	0 – 1	Ниско	**1**
	2 – 3	Средно	**2**
	4 – 5	Високо	**3**
Г. Бизнес сектор и мащаб	0 – 1	Ниско	**1**
	2 – 3	Средно	**2**
	4 – 5	Високо	**3**

След това горепосочените резултати могат да бъдат въведени в следната обобщаваща диаграма:

ВЕРОЯТНОСТ ОТ ВЪЗНИКВАНЕ НА ЗАПЛАХА (2):

ОбщСБОР от резултатите:	НИВО НА ВЕРОЯТНОСТ от възникване на заплаха:
4 – 5	**Ниско**
6 – 8	**Средно**
9 – 12	**Високо**

Накрая, тези резултати могат да бъдат комбинирани с резултатите от „Нивото на въздействие”, посочени в първата диаграма по-горе, за да се посочи общият риск, както следва:

ОБЩА ОЦЕНКА НА РИСКА:

	НИВО НА ВЪЗДЕЙСТВИЕ			
ВЕРОЯТНОСТ ОТ ВЪЗНИКВАНЕ НА ЗАПЛАХА		Ниско	Средно	Високо/Много Високо
	Ниско			
	Средно			
	Високо			

Легенда:

[ ] *Нисък риск* [ ] *Среден риск* [ ] *Висок риск*

ВЪПРЕКИ ТОВА, СЛЕДВА ДА СЕ ОТБЕЛЕЖИ, че посочената по-горе схема за оценка на риска се отнася основно до **рисковете за сигурността на данните.**

Това определено е една от основните категории риск, която трябва да бъде оценена и разгледана – и то не еднократно, а непрекъснато, тъй като рисковете могат да се развиват и мутират с течение на времето. Виж. бележката, озаглавена: *„Мониторинг на спазването: Повтаряне на Задачи 1 – 3 (и 4) на текуща база*" в края на обсъждането на Задача 4, точно преди обсъждането на Задача 5 по-долу.

В по-общ план ОРЗД посочва и **„риск[ове] за правата и свободите на физическите лица"** (виж чл. 34, чл. 35 и чл. 36). Първият член, чл. 34, ясно приема, че нарушенията на данните, като такива, могат да доведат до горе описаните рискове и налага важни правила за това как да се справят с тях, както е посочено в Задачи 4 (Оценки на въздействието върху защитата на данните), 5 (Задача по разследване), 10 (Сътрудничество с органа по защита на данните) и 12 (Задача за повишаване на информираността и осведомеността).

Следва да се отбележи , че „**рисковете за правата и свободите на физическите лица" не произтичат само от нарушения на сигурността на данните.** Самият ОРЗД, чл. 35, пар. 1 предвижда, , че *„високи рискове"* от този вид могат да произтекат, по-специално, от:

- систематична и задълбочена оценка на личните аспекти, свързани с физическите лица, която се основава на автоматизирано обработване, включително профилиране, и на която се базират решения, пораждащи правни последици за физическото лице или по подобен начин засягат физическото лице;
- обработване в голям мащаб на специални категории данни, посочени в чл. 9, пар. 1, или на лични данни, свързани с присъди и престъпления, посочени в чл. 10; или
- мащабно систематично наблюдение на публично достъпна зона.

В тези случаи, *точно защото тези дейности по обработване предизвикват* ***неизбежно високи рискове*** *за правата и свободите на физическите лица*, се изисква Оценка на въздействието върху защитата на данните (и в някои случаи трябва да се проведе консултация със съответния орган за защита на данните или органите по защита на данните), както е разгледано в следващата задача.

По-конкретно, автоматизираното вземане на решения, основано на профили, може да доведе до **несправедливи решения** (защото никой не е напълно същият, като всяко друго лице и – надяваме се – нито една система не би могла да знае всичко за дадено лице) или недемократични решения с **дискриминационни, но неоспорими резултати**; [339] използването на чувствителни данни може също да доведе до **дискриминация**

[339] Виж: Дау Корф & Мари Жорж, Записи с имената на пътниците, извличане на данни и защита на данните: необходимостта от строги гаранции, доклад, изготвен за Консултативния комитет по Конвенцията за защита на лицата при автоматизираната обработка на лични данни (T-PD) на Съвета на Европа, 2015 г., раздел I.iii, *Опасностите, присъщи на извличането на данни и профилирането,* намиращ се на:
https://rm.coe.int/16806a601b

(независимо дали е умишлена или не);[340] използването на дори привидно безвредни данни при продажбите, може да разкрие лични здравословни проблеми или бременност; [341] и систематичното наблюдение на хората на обществени места може да има **отрицателен ефект върху упражняването на основни права, като например правото на свобода на изразяване, сдружаване и протест**. [342] В действителност рисковете могат да се комбинират и след това да се **засилват взаимно**, както при използването на технологията за разпознаване на лица при наблюдение на обществени места от страна на полицията, с цел „идентифициране" на нарушители и поведенчески анализ.[343]

Също така, за да се реализират тези рискове, не се изисква нарушаване на сигурността на данните: рисковете произтичат от присъщите опасни характеристики на самите дейности по обработване, дори ако са извършвани в съответствие с техните спецификации и без нарушаване на сигурността на данните, както е определено в Общия регламент относно защитата на данните. ***Това не е обхванато от (иначе много полезната) схема за оценка на риска, очертана от*** **Garante*****, описана по-горе.***

Това се отнася и за по-малките „рискове за правата и свободите на физическите лица", произтичащи от дейностите по обработване, които не са посочени като предизвикващи „висок риск". Това включва, по-специално, дейности по обработване, които не отговарят напълно на изискванията на Общия регламент относно защитата на данните.

ПРИМЕРИ:

- Използване на лични данни – които са събрани за една цел или за друга цел, която е „несъвместима" цел, без надлежно правно основание за вторичното обработване и/или без адекватно информиране на субектите на данни за предвидените вторични обработванияна техните данни, които биха се влошили, ако това включва разкриване на данни на трета страна.

➢ Това може да доведе до това, на субектите на данни да бъде отказана възможността да се съгласят (или да откажат да се съгласят, или да възразят) при вторичното обработване, което може да има негативно влияние (например в заявления за работа или отпускане на кредит). Също така е твърде вероятно личните данни, предоставени за определена цел, да не са достатъчно точни или относими за използване в изцяло различна цел.

---

340 Ето защо в европейските инструменти за защита на данните бяха включени специални, особено ограничителни правила за обработването на лични данни: виж "БЕЛЕЖКАТА" в Част 1, раздел 1.2.3, по-горе.

341 Виж: *How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did* (*Как Target установи, че една тийнейджърка е бременна преди баща ѝ*), Forbes, 16 февруари 2012 г., може да се намери на: https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#2ea04af16668

342 Виж цитата от прочутото преброяване на населението на германския Конституционен съд, стр.10 на този наръчник.

343 Виж: Дау Корф, *Първо не вреди: Потенциалът за причиняване на вреди на основните права и свободи от държавните интервенции за киберсигурност*, раздел 2.4, *Превантивно, предсказуемо определения на политиката*, в: Бен Вагнер, Матиас К. Кетенман и Килиан Виет (Редактори) , Изследователски Наръчник за правата на човека и цифровата технология: глобална политика, право и международни отношения, Център за Интернет и човешки права, Берлин, който трябва да бъде публикуван по-късно през 2018 г.,

- Запазване и/или използване на лични данни (обикновено след като вече не са необходими за първоначалната им цел) в псевдонимизирана или предполагаема анонимизирана форма (обикновено за последваща употреба в тази форма, за нова, вторична цел).

➢ С оглед на нарастващия риск от повторно идентифициране на дори предполагаемо напълно анонимизирани данни,[344] всяко запазване и използване на псевдонимизирани или предполагаемо анонимизирани данни трябва да се разглежда, като предизвикващо рискове за правата и свободите на субектите на данни (които може дори да представляват вероятно „високи рискове", изискващи Оценка на въздействието върху защитата на данните, както е описано в Задача 4). Длъжностното лице по защита на данните следва много внимателно да провери рисковете от повторно идентифициране на такъв тип данни, за която и да е конкретна цел и да наложи силни смекчаващи фактори (като „диференцирана неприкосновеност на личния живот")[345] в подходящи случаи – или да откаже по-нататъшно обработване на данните.

- Използване на неподходяща, неточна или остаряла информация – с възможни подобни негативни последици.

- Да не се придава подходяща тежест на „интересите или основните права и свободи на субекта на данните, които изискват защита на личните данни, по-специално когато субектът на данните е дете", когато се преценява дали личните данни могат да бъдат обработвани въз основа на условието за „легитимен интерес" (чл. 6, пар. 1, б. „е") Общ регламент относно защитата на данните).

➢ Това по дефиниция причинява вреда на тези субекти на данни. Следователно, използването на критерия за „легитимен интерес" като законово основание за обработването, винаги изисква особено внимателно проучване от страна на длъжностното лице по защита на данните в настоящата задача.

➢ **БЕЛЕЖКА:** Държавните органи не могат да се позовават на този критерий „при изпълнение на техните задачи" (чл. .6, пар.1, последно изречение), но това не означава, че въпросът никога не възниква в контекста на публичния сектор, напр. във връзка със задачи, които не са задължителни по закон, като например изпращане на електронни писма до гражданите за културни събития, като се използва регистърът на населението; или във връзка с дейности на частни субекти, изпълняващи задачи от „обществен интерес".

---

344 Резюме на проблемите с премахването и повторното идентифициране, вж. документа, представен от Фондацията за проучване на информационната политика, за консултацията на правителството на Обединеното кралство относно „Превръщане на отворените данни в реалност", който може да бъде намерен на: www.fipr.org/111027opendata.pdf. Това се отнася до творческия документ по проблема: Пол Ом, Нарушени обещания за неприкосновеност на личния живот: отговор на изненадващия провал на анонимизацията, 57 UCLA Law Review (2010) 1701, намиращ се на: http://papers.ssrn.com/sol3/paperscfm?abstract_id=1450006.

345 Диференциалната неприкосновеност на личния живот е важна мярка за предотвратяване на повторното идентифициране на субектите на данни от наборите с данни – но тя работи само, ако се прилага в контролирана среда, в която изследователите са ограничени в запитванията, които могат да изпратят до базата данни, виж:
https://privacytools.seas.harvard.edu/differential-privacy
https://people.eecs.berkeley.edu/~stephentu/writeups/6885-lec20-b.pdf
Тя не дава отговор на обстоятелства, при които личните данни се разпространяват в предполагаемо напълно анонимизирана форма сред широката общественост, или в които големи набори с данни се съгласуват по друг начин без пълен контрол.

- Не се информират по подходящ начин субектите на данни за всички подробности, за които те трябва да бъдат информирани съгласно чл.13 и чл. 14 от Общия регламент относно защитата на данните.

➢ Това може да доведе до невъзможност субектите на данни да упражняват напълно правата си по Общия регламент относно защитата на данните ("интереси или основни права и свободи на субекта на данните, които изискват защита на личните данни").

- Предаване на лични данни в трета държава, за която не е прието, че предоставя „адекватна" защита на личните данни, без да са налице подходящи гаранции или набор от одобрени Обвързващи корпоративни правила (ОКП) или без да има позоваване по друг начин на някоя от посочените дерогации (вж. членове46 – 48 от Общия регламент относно защитата на данните). Това включва използването на „облачна" услуга, която използва сървър (или сървъри), намиращи се в такива трети държави.

➢ Както Европейският надзорен орган по защита на данните е посочил в подробния си съвет относно използването на услуги в облака от институциите на ЕС (които също следва да бъдат проучени от националните публични органи, тъй като голяма част от съветите биха могли да се прилагат в същата степен и за тях), извършването на изчисления в облака предизвиква специфични рискове, следва да бъдат разгледани много внимателно от администраторите (разчитайки на техните длъжностни лица по защита на данните).[346] Всъщност неговият съвет предполага, че изчисленията в облака може да се разглеждат и като предизвикващи високи рискове и, поради това, изискващи Оценка на въздействието върху защитата на данните. Това се отбелязва в следващата задача.

- Възлагане на външни изпълнители за обработване на лични данни от публични органи, по-специално, ако данните са чувствителни в технически-правния смисъл на Общия регламент относно защитата на данните („специални категории данни" – чл.9), или чувствителни в по-общ план като финансови данни или данни от преброяване.

➢ Европейският надзорен орган по защита на данните отбелязва, че използването на изчислителни облаци повишава рисковете, присъщи на аутсорсинга на обработване.[347]

Ако след извършване на оценката, становището на длъжностно лице по защита на данните е, че операцията по обработване на лични данни представлява риск за съответните интереси, длъжностното лице по защита на данните трябва **да уведоми** съответното вътрешно отговорно лице или лица за тези рискове, и да предложи **смекчаващи или алтернативни действия**. Често легитимната цел може да бъде

---

[346] Европейски надзорен орган по защита на данните (ЕНОЗД), Guidelines on the use of cloud computing services by the European institutions and bodies (Насоки относно използването на услугите за изчисления в облак от европейските институции и структури), март 2018 г., намиращи се на: https://edps.europa.eu/sites/edp/files/publication/18-03-16_cloud_computing_guidelines_en.pdf
вж. по-специално *Приложение 4: Специфични за обработването на данни рискове от изчислението в облака*

[347] Европейски надзорен орган по защита на данните (ЕНОЗД), Guidelines on the use of cloud computing services by the European institutions and bodies (Насоки относно използването на услугите за изчисления в облак от европейските институции и структури) (предишна бележка под линия) „се фокусира върху използването на услуги по изчислителния в облака, предоставяни от търговски субекти [но] [к]ато такива, тя също разглежда – като естествена последица – въпросите, възникнали от аутсорсинга на ИТ услуги, които обработват лични данни."(стр. 5).

постигната с различни, по-малко натрапчиви средства или чрез използване на по-малко (и по-малко чувствителни) данни – и в тези случаи, длъжностното лице по защита на данните следва принудително да предложи това. В случай, че този съвет не бъде спазен, длъжностното лице по защита на данните следва отново да **отнесе** въпроса към висшето ръководство (вж. по-надолу „*Консултативни задачи*“).

Длъжностното лице по защита на данните следва да води пълна **документация** за всички тези оценки на риска и за изложените съвети.

Ако се следва съветът на длъжностното лице по защита на данните, тези записи ще „**докаже[ат]**, че обработването се извършва в съответствие с настоящия регламент” – т.е. че тези рискове наистина са били оценени и че мерките, предприети в светлината на тази оценка, са били подходящи за тези рискове (Виж чл. 24, пар. 1 и обсъждането на „задължението да се покаже съответствие” с Общия регламент относно защитата на данните в раздел 2.2 по-горе).

Имайте предвид, че ако общата оценка на риска показва, че предложеното обработване представлява вероятен „**висок риск**” за правата и свободите на физическите лица, длъжностното лице по защита на данните следва да уведоми администратора, че е необходима пълна Оценка на въздействието върху защитата на данните (ОВЗД), както е обсъдено по-долу, в Задача 4.

Дори ако не се изисква Оценка на въздействието върху защитата на данните, длъжностното лице по защита на данните ще трябва да продължи да наблюдава текущо всички дейности по обработване на лични данни на неговия администратор: вж. описанието след Задача 4, в точка „*Мониторинг на спазването: Повтаряне на задачи 1 – 3 (и 4) на текуща база*”.

Отбележете също така, че често националните законодатели вече са се опитвали да обърнат внимание на специални рискове, които според тях са породени от специални дейности по обработване или дейности, в техните национални правила – нещо, което до голяма степен може да бъде продължено съгласно „уточнителните разпоредби“ в Общия регламент относно защитата на данните.[348]

Примери:

В **Хърватия** е забранено обработване на ***генетични данни*** за изчисляване на риска от заболяване и други здравни аспекти на субекта на данни във връзка със сключването или изпълнението на животозастрахователни договори и договори с клаузи за преживяване – и тази забрана не може да бъде премахната от съгласието на субекта на данни (чл. 20 от Закона за прилагане на Общия регламент относно защитата на данните).

Там, както и в други държави, използването на ***биометрични данни*** и **камери за видеонаблюдение за сигурност (CCTV)** също се урежда от специални условия, като например изискване за особено ясно и недвусмислено съгласие и ограничения, като например поставянето на ограничения относно запазването на данни.

Тези правни условия, разбира се, следва да бъдат взети изцяло предвид при всяка оценка на риска: естествено, никой администратор или длъжностно лице по защита на

348 Виж Част 2, раздел 2.2.

данните не може да направи заключение, че рискът е приемлив, въпреки че не са спазени специалните законодателни условия и ограничения.

- o – O – o -

ЗАДАЧА 4: Работа с дейности, които е вероятно да породят „висок риск": извършване на Оценка на въздействието върху защитата на данните (ОВЗД)

Казаното по-горе относно общите оценки на риска (Задача 3) се прилагат с още по голямо основание, спрямо дейности за обработване на лични данни, които въз основа на горепосочената обща оценка на риска се счита, че вероятно пораждат „**висок риск** за правата и свободите на физическите лица" (чл. 35, пар. 1). В Общия регламент относно защитата на данните става ясно, че това може да е така, по-специално, когато се използват „нови технологии".

Ако предварителната оценка на риска, извършена в Задача 3, наистина показва, че дадена конкретна операция по обработване на данните предизвиква вероятен „висок риск", то тогава администраторът трябва да извърши **Оценка на въздействието върху защитата на данните** (ОВЗД), преди да продължи с обработването.

Общият регламент относно защитата на данните постановява, че ОВЗД трябва да се осъществява в случаи на напълно автоматично/ базирано на профили вземане на решения, мащабно обработване на чувствителни данни, или мащабно наблюдение на публично достъпна зона (чл. 35, пар. 3). Националните органи за защита на данните трябва също да приемат списъци с дейности, които ще бъдат предмет на оценки на въздействието върху защитата на данните на тяхна територия, и могат да приемат списъци с дейности, които няма да изискват такива, но тези списъци трябва да бъдат представени на Европейския комитет по защита на данните и могат да бъдат оспорени от други органи по защита на данните в рамките на „механизма за съгласуваност" на Общия регламент относно защитата на данните (чл.35, пар. 4 – 6). Общият регламент относно защитата на данните позволява, също така на Европейския комитет по защита на данните да издаде свой собствен отрицателен и положителен списък, като стъпва на дейностите, които са му представени от националните органи по защита на данните (които са длъжни да направят това съгласно чл. 64, пар. 1, б. а)) от ОРЗД.

На практика това, което се случи, е, че на първо място Работната група по чл. 29 излезе с подробни съвети и насоки за провеждането на ОВЗД, както и в нейните Насоки за длъжностните лица по защита на данните от декември 2016 г., преработени през април 2017 г. (WP243 rev.1)[349] така и в следващите, по-подробни Насоки за ОВЗД, приети на 4 април 2017 г., преработени и приети на 4 октомври 2017 г. (т.е. още преди прилагането на ОРЗД).[350] И двете бяха одобрени от Европейския комитет по защита на данните на 25 май 2018 г.[351] Освен това ЕНОЗД предостави и полезни по-нататъшни насоки в своя

[349] Виж бележка под линия 209, по-горе.

[350] Работна група по чл. 29 Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (Насоки за оценка на въздействието върху защитата на данните (ОВЗД) и определяне дали обработването „има вероятност да породи висок риск" за целите на Регламент 2016/679) (WP248 rev 1, оттук нататък наричани Насоки за ОВЗД на Работната група по чл.29), страница със съдържанието, намиращи се на: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

[351] Виж бележка под линия 215, по-горе.

доклад относно Отчетността на място[352], включително и временен списък на обработените дейности, които според него изискват или не изискват ОВЗД.[353]

Ревизираните насоки за ОВЗД, приети от Работната група по член 29 и одобрени от Европейския комитет по защита на данните, излагат **девет критерия**, които следва да бъдат взети предвид при определяне на това дали една операция по обработване предизвиква вероятност за довеждане до „висок риск" и посочват, че:[354]

> ***В повечето случаи*** администраторът на данни може да счете, че обработване, отговарящо на **два критерия,** би изисквало извършването на ОВЗД. Като цяло Работна група по член 29 счита, че колкото повече критерии се изпълняват при обработването, толкова по-вероятно е то да представлява висок риск за правата и свободите на субектите на данни, и – следователно – да изисква ОВЗД, независимо от мерките, които администраторът предвижда да приеме.

Това е допълнително разгледано по-долу в точката *„Как да се прецени дали предложената операция по обработване* е възможно да доведе до *„висок риск*", където са дадени примери, взети от Насоките на Работната група по член 29 и документа на ЕНОЗД, в подточка *„Фактори, които сочат за „висок риск"*.

Тук следва да отбележим, че повечето от националните органи по защита на данните (22 от общо 28)[355] приеха свои временни списъци и ги представиха на Европейския комитет по защита на данните за преглед. Европейският комитет по защита на данните извърши тези прегледи в светлината на Насоките на Работната група по чл. 29, като на 25 септември 2018 г. издаде 22 становища по тези списъци (по едно за всеки проектосписък).[356] Основният въпрос, който се разглежда от Европейския комитет по защита на данните в тези становища, е препоръка към органите по защита на данните, че те не трябва да включват дейности по обработаване в списъка с дейностите, за които ОВЗД е задължителна, ако въпросната операция отговаря само на *един* от критериите за определяне дали е налице вероятен „висок риск", изложени в Насоките. Така например в становището си относно проекта за списък, представен от Обединеното кралство, той посочва следното:[357]

---

352 ЕНОЗД, Accountability on the ground Part I: Records, Registers and when to do Data Protection Impact Assessments (Отчетност на място Част I: Записи, регистри и кога да се правят оценки на въздействието върху защитата на данните) (бележка под линия 267, по-горе), раздел 4, *Кога да се извършва ОВЗД?*, на стр.9 – 11.

353 Виж, Приложение 5.

354 Работна група по чл.29 Насоки за ОВЗД (бележка под линия 315, по-горе), стр.11, добавено подчертаване.

355 Австрия, Белгия, България, Република Чехия, Германия, Естония, Гърция, Финландия, Франция, Унгария, Ирландия, Италия, Литва, Латвия, Малта, Нидерландия, Полша, Португалия, Румъния, Швеция, Словакия и Обединеното кралство.

356 Всички те са достъпни чрез връзки, предоставени на адрес: https://Европейски комитет по защита на данните.europa.eu/our-work-tools/consistency-findings/opinions_en

357 Европейски комитет по защита на данните, Становище 22/2018 относно проекта за списък на компетентния надзорен орган на Обединеното кралство по отношение на дейностите по обработване, изискващи Оценка на въздействието върху защита на данните (член 35, параграф 4 от Общия регламент относно защитата на данните), прието на 25 септември 2018 г., намиращо се на: https://edpb.europa.eu/sites/edpb/files/files/file1/2018-09-25-opinion_2018_art._64_uk_sas_dpia_list_en.pdf

> Списъкът, представен от Надзорния орган на Обединеното кралство за становище на Комитета, посочва, че обработването на биометрични данни попада в рамките на задължението за самостоятелно извършване на ОВЗД. Комитетът е на мнение, че обработването на биометрични данни само по себе си не е вероятно да представлява висок риск. Въпреки това, обработката на биометрични данни с цел еднозначно идентифициране на физическо лице във връзка с поне още един критерий, изисква извършването на ОВЗД. С оглед на това, Комитетът изисква от Надзорния орган на Обединеното кралство да измени съответно своя списък, като добави, че точката, отнасяща се до обработването на биометрични данни с цел еднозначно идентифициране на физическо лице, изисква да се извършва ОВЗД, само когато е направено във връзка с поне още един критерий, който се прилага, без с това да се засяга чл. 35, пар. 3 от ОРЗД.

Разбира се, ОВЗД може да се извършва от администратор, дори ако е изпълнен само един от тези критерии, без това да е задължение.

Изискването за ОВЗД може да бъде заобиколено в случаите, когато закон урежда съответния вид операция и е изпълнена обща ОВЗД в контекста на приемането на закона (чл. 35, пар. 10). Освен това, „[в] една оценка може да бъде разгледан набор от сходни дейности по обработване, които представляват сходни високи рискове" (чл. 35, пар. 1, последно изречение). Както Работната група по член 29 обобщава:[358]

> Кога не се изисква ОВЗД? Когато обработваното не е „[вероятно] да доведе до висок риск" или съществува подобна ОВЗД, или е било разрешено преди май 2018 г., или то има законово основание, или е в списъка на дейностите по обработване, за които не се изисква Оценка на въздействието върху защитата на данните.

Обширни насоки за ОВЗД, включително методологични указания, бяха издадени и от националните органи по защита на данните, включително тези на Франция, Испания и Обединеното кралство, както и от германския *Datenschutzzentrum* (одобрен от германските органи по защита на данните).[359] **Френският** орган по защита на данните, CNIL, дори (в сътрудничество с други органи по защита на данните) разработи софтуер с отворен код за оценка на въздействието върху защитата на данните, който „цели да помогне на администраторите на данни да изградят и докажат спазване на Общия регламент относно защитата на данните". Както е обяснено на уебсайта:[360]

---

358 Насоки за ОВЗД на Работната група по член 29 (бележка под линия 315, по-горе), страница със съдържанието, стр.6.

359 Виж списъка с връзки в Приложение 1 към Работна група по член 29 на РДВС (бележка под линия 315, по-горе). Методологиите за ОРЗД са разгледани по-долу в тази рубрика.

360 Намиращи се, с допълнителна информация на английски език, на адрес:
https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment
CNIL използва по-кратък акроним „PIA" (също и в цитирания текст, по-горе), вероятно защото Оценки на въздействието върху защитата на данните произхожда от „Оценки на въздействието на *неприкосновеността* на личния живот". Следва да се отбележи, че инструментът е актуализиран наскоро. Информация за актуализацията можете да намерите тук (само на френски):
https://www.cnil.fr/fr/loutil-pia-mis-jour-pour-accompagner-lentree-en-application-du-rgpd
На тази страница CNIL твърди, че софтуерът е достъпен на 14 езика: френски, английски, италиански, немски, полски, унгарски, финландски, норвежки, испански, чешки, холандски, португалски, румънски и гръцки и че е одобрен (поне временно, в бета версия) от органите по защита на данните на Бавария, Италия, Финландия, Унгария, Полша и Норвегия. Следва обаче да се отбележи, че софтуерът е съсредоточен главно върху техническата сигурност и ще бъде използван предимно за МСП, а не за големи и много сложни звена.

Кой може да използва софтуера за оценка на въздействието върху защитата на данни (ОВЗД) (**PIA)?**

Инструментът е насочен главно към администратори на данни, които са слабо запознати с процеса на ОВЗД . В тази връзка може да се изтегли и лесно да се стартира самостоятелна версия на Вашия компютър.

Също така е възможно да използвате инструмент на сървърите на организацията, за да го интегрирате с други инструменти и системи, които вече се използват в съответната организация.

Какво представлява той?

Инструментът за ОВЗД е проектиран на база на три принципа:

- **Дидактичен интерфейс за извършване на ОВЗД:** Инструментът разчита на удобен за потребителя интерфейс, който позволява лесно управление на вашата оценка на въздействието. Той ясно разгръща методологията за оценка на въздействието върху неприкосновеността на личния живот стъпка по стъпка. Няколко инструменти за визуализация предлагат начини за бързо разбиране на рисковете.
- **Правна и техническа база от знания:** инструментът включва правните точки, гарантиращи законосъобразността на обработването и правата на субектите на данни. Той също така разполага със специализирана база от знания, достъпна на всички стъпки на PIA, като адаптира показаното съдържание. Данните са извлечени от Общия регламент относно защитата на данните, Ръководствата за оценка на въздействието върху неприкосновеността на личния живот и Ръководството за сигурност от CNIL, към аспекта на изследваната обработка.
- **Модулен инструмент:** създаден да ви помогне да постигнете съответствие, като можете да персонализирате съдържанието на инструмента според Вашите специфични нужди или бизнес сектора, например чрез създаване на модел на оценка на въздействието върху неприкосновеността на личния живот, който можете да дублирате и използвате за набор от подобни дейности по обработване. Публикувано с безплатен лиценз, е възможно да се променя програмният код на инструмента, за да се добавят характеристики или за да се включи в инструменти, използвани във вашата организация.

В този наръчник няма място, което да обхваща всички подробни съвети за ОВЗД, предвидени в по-късните, по-специфични насоки за ОВЗД на Работната група по член 29 (одобрени от Европейския комитет по защита на данните), или в националните насоки: **силно насърчаваме читателя да проучи изцяло насоките на Работната група по член 29/ Европейския комитет по защита на данните и съответни национални съвети, където е уместно, и да разчита на него в своите действия и на каквито и да е дадени съвети.**[361]

Читателят, и по-специално длъжностните лица по защита на данните, следва също така да вземе(ат) предвид националния задължителен списък на ОВЗД, публикуван от съответния им орган за защита на данните, тъй като този списък съдържа примери за ситуации, в които прилагането на горните насоки и съвети е довело до предписване на изпълнението на ОВЗД от публични и частни организации; очаква се длъжностните лица

[361] Вж. препратките в бележки под линия 209, 267, 315 и в предишната бележка под линия, по-горе, за основните съвети, които трябва да бъдат проучени.

по защита на данните да осъществяват надзор върху изпълнението на ОВЗД от съответните администратори, когато те са упълномощени да направят това въз основа на посочените списъци. Ако в следващите месеци се издават и „бели списъци" (съгласно чл. 35, пар. 5 от ОРЗД), те също ще бъдат много полезни, тъй като те ще изключват необходимостта администраторът да се включи в това упражнение за набор от не-високо рискови дейности по обработване.

По-долу ще отбележим накратко насоките във връзка с: **различните роли и отговорности на администратора и длъжностното лице по защита на данните**; въпросът е **как да се прецени дали предложена операция по обработване представлява вероятност за „висок риск"**; **методологиите за Оценка на въздействието върху защитата на данните** и **какво да се прави с протокола от ОВЗД**, по-специално ако се стигне до заключението, че някои идентифицирани високи рискове не могат да бъдат напълно смекчени чрез различни възможни мерки, като в този случай Общият регламент относно защитата на данните изисква **провеждане на консултация със съответния орган по защита на данните** (член 36).

Различните роли и отговорности на администратора и длъжностното лице по защита на данните във връзка с ОВЗД

В своите Насоки за длъжностните лица за защита на данните, Работната група по член 29 отново подчертава обособените роли и отговорности на администратора и на длъжностното лице по защита на данните, също във връзка с ОВЗД. В тях се посочва следното:[362]

> 4.2. Ролята на длъжностното лице по защита на данните в оценката на въздействието върху защитата на данните
>
> Съгласно чл. 35, пар. 1 задача на администратора, а не на длъжностното лице по защита на данните, е да извърши, когато е необходимо, оценка на въздействието върху защитата на данните (ОВЗД). Въпреки това, длъжностното лице по защита на данните може да играе много важна и полезна роля за подпомагане на администратора. В съответствие с принципа за защита на данните на етапа на проектиране, чл. 35, пар. 2 изрично изисква администраторът да *„иска становището на*" длъжностното лице по защита на данните при извършването на Оценка на въздействието върху защита на данните. Чл, 39, пар, 1, б, „в", на свой ред, възлага на длъжностното лице по защита на данните задължението да *„при поискване да предоставя съвети по отношение на [ОВЗД] и да наблюдава извършването на оценката"*.
>
> Работната група по член 29 препоръчва администраторът да потърси съвет от длъжностно лице по защита на данните по следните въпроси, наред с другото:[363]
>
> - дали да се извърши ОВЗД или не
> - каква методология да се следва при осъществяването на ОВЗД

---

362 Насоки за длъжностните лица по защита на данните на Работна група по член 29 (бележка под линия 209, по-горе), раздел 4.2, стр.16 – 17, оригинален курсив, подчертан в последния добавен абзац.

363 Чл. 39, пар. 1 посочва задачите на длъжностното лице по защита на данните и посочва, че длъжностното лице по защита на данните трябва да има „най-малко" следните задачи. Следователно нищо не пречи на администратора да възложи на длъжностното лице по защита на данните други задачи, различни от изрично упоменатите в чл. 39, пар. 1, или да определи по-подробно тези задачи. [оригинална бележка под линия]

- дали да се извършва оценка на въздействието върху защитата на данните в рамките на организацията или да се възлага на външни изпълнители
- какви гаранции (включително технически и организационни мерки) да се прилагат за смекчаване на всички рискове за правата и интересите на субектите на данни
- дали оценката на въздействието върху защитата на данните е била извършена правилно и дали нейните заключения (дали да се продължи с обработеното или не и какви гаранции да се прилагат) са в съответствие с Общия регламент относно защитата на данните.

Ако администраторът не е съгласен със съветите, дадени от длъжностното лице по защита на данните, в документацията за ОВЗД трябва конкретно да се направи писмена обосновка защо съветите не са взети под внимание.[364]

Освен това Работна група по член 29 препоръчва администраторът ясно да очертае, например в договора на длъжностно лице по защита на данните, но също така и в информацията, предоставена на служителите, ръководството (и други заинтересовани страни, където е уместно), точните задачи на длъжностното лице за защита на данни и техния обхват, по-специално по отношение на осъществяването на ОВЗД.

По-късните Насоки относно ОВЗД на Работната група по член 29 също подчертават, че ОВЗД трябва да се изпълняват от „администратор, с длъжностното лице по защита на данните и обработващия лични даннии".[365]

На практика, особено в по-малки организации, длъжностното лице по защита на данните често отново ще играе (ако не е наистина негова) водещата роля в оценката.

Как да се прецени дали предложената операция по обработване предизвиква вероятност за „висок риск"

Работната група по член 29/ Европейският комитет по защита на данните обясняват, че:[366]

Задължението администраторите да извършват ОВЗД при определени обстоятелства следва да се разбира на фона на общото им задължение да управляват по подходящ начин рисковете, произтичащи от обработването на личните данни –

т.е. както е отбелязано и по-горе, въпросът дали трябва да се изпълнява ОВЗД естествено произтича от общото задължение на администратора – изпълнено със „съвета", но на практика като цяло разчитайки на длъжностното лице по защита на данните – да се

---

364 Чл. 24, пар. 1 предвижда, че „*Като взема предвид естеството, обхвата, контекста и целите на обработването, както и рисковете с различна вероятност и тежест за правата и свободите на физическите лица, администраторът въвежда подходящи технически и организационни мерки, за да гарантира и да е в състояние да докаже, че обработването се извършва в съответствие с настоящия регламент. Тези мерки се преразглеждат и при необходимост се актуализират*". [оригинална бележка под линия, оригинален курсив]

365 Вж. Насоки за ОВЗД на Работната група по член 29 (бележка под линия 315, по-горе), раздел III.D.b).

366 *Вж.*, стр.6.

оценят рисковете, присъщи на всички дейности на администратора по обработка на данните (Задача 3 по-горе).

Те продължават да изясняват понятието „риск" и защитените интереси, които следва да се вземат предвид:[367]

> „Рискът" е сценарий, описващ събитие и неговите последици, оценени от гледна точка на сериозност и вероятност. „Управление на риска", от друга страна, може да се определи като координирани дейности за насочване и контрол на дадена организация по отношение на риска.
>
> Чл. 35 се отнася до вероятно висок риск „за правата и свободите на физическите лица". Както е посочено в чл. 29 от изложението на Работната група по член 29, относно ролята на основан на риска подход в правните уредби на защитата на данните, позоваването на „правата и свободите" на субектите на данни се отнася главно до правата на защита на данните и на неприкосновеност на личния живот, но може да включва и други основни права като свобода на словото, свобода на мисълта, свобода на движението, забрана на дискриминацията, право на свобода, съвест и религия.

Работната група по член 29 отбелязва вече споменатите примери в чл. 35, пар. 3 от Общия регламент относно защитата на данните за ситуации, които по своята същност предизвикват „високи рискове": когато администраторът използва автоматични, базирани на профили алгоритми, за вземане на решения с правни или други съществени последици; когато администраторът обработва „мащабно" чувствителни данни или данни за присъди; или когато администраторът „систематично наблюдава" публично достъпна зона „мащабно". Тя правилно добавя:[368]

> Както показват думите „по-специално" в уводното изречение на чл. 35, пар. 3 от Общия регламент относно защитата на данните, това е предвидено да бъде изчерпателен списък. Възможно е да има „високорискови" дейности по обработване, които не са обхванати от този списък, но въпреки това предизвикват също толкова висок риск. Тези дейности по обработване също следва да подлежат на оценки на въздействието върху защитата на данните.

Работната група по член 29 изброява редица фактори – повечето, но не всички, свързани с трите примера в чл. 35 – които предполагат, че операцията по обработване предизвиква „високи рискове" и дава допълнителни, по-конкретни примери. ЕНОЗД предоставя допълнителни примери, както в предварителния си списък на дейностите по обработване, които винаги ще изискват ОВЗД, така и в образец, който може да се използва за оценка дали дейностите по обработване, които не фигурират, нито в неговия „положителен" списък (дейности, които според него винаги да изискват ОВЗД), нито в „отрицателния" му (тези, които според него не изискват ОВЗД), следва да бъдат

---

367 *Вж.*. Следва да се отбележи и по-ранното препращане към ISO 31000: 2009, *Управление на риска. Принципи и указания*, Международна организация за стандартизация (ISO); ISO / IEC 29134 (проект), *Информационни технологии – Техники за сигурност – Оценка на въздействието върху неприкосновеността на личния живот – Указания*, Международна организация за стандартизация (ISO) (Насоки относно оценките на въздействието върху защитата на данните на Работната група по член 29, бележка под линия 315, на стр.5).

368 *Вж.*, стр.9.

подложени на Оценка на въздействието върху защитата на данните.[369] Тези примери на Работната група по член 29 и ЕНОЗД са изложени по-долу (донякъде редактирани, като примерите за Работната група по член 29 са премахнати от текста и преместени в кутията, а примерите на ЕНОЗД са посочени с *). Добавихме някои допълнителни примери (или допълнителни подробности или вариации), които са от значение за администраторите в публичния сектор по-специално; тези примери и други. са посочени в *курсив*.

Фактори, указващи „висок риск"[370]

1. Оценка, включително профилиране и прогнозиране, особено от *„различни аспекти, имащи отношение към резултатите в работата на субекта на данни, икономическото състояние, здравето, личните предпочитания или интереси, благонадеждността или поведението, местоположението или движенията"* (съображения 71 и 91).

> **Примери:**
>
> Финансова институция, която проверява своите клиенти в база данни за кредитни справки или за изпиране на пари и борба с финансирането на тероризма (AML/ CTF) или база данни с измами.
>
> Банкови транзакции по проверка в съответствие с приложимото законодателство за откриване на евентуални измамни транзакции. *
>
> Профилиране на членове на персонала въз основа на всичките им транзакции в системата за управление на случаите [*в организацията*] с автоматично преназначаване на задачи. *
>
> Биотехнологична компания, предлагаща генетични тестове директно на потребителите, за да оцени и предскаже рисковете от заболяване/ здраве.
>
> Дружеството, което изгражда поведенчески или маркетингови профили въз основа на използването или навигацията на неговия уебсайт.

2. Автоматизирано вземане на решения с правни или подобни значителни последици: обработване, целящо вземане на решения за субекти на данни, произвеждащи „правни последици за физическото лице" или които „по подобен начин сериозно засягат физическото лице" (чл. 35, пар. 3, б. а)), по-специално (но не само) в случаите, когато обработването може да доведе до изключване или дискриминация на физически лица.

> **Примери:**[371]

---

369 Положителните и отрицателните списъци са изложени в *Приложение 5* към документа на ЕНОЗД Отчетност на място (бележка под линия 267, по-горе); *Образецът за оценка на прага / критериите* са описани в *Приложение 6* към този документ.

370 Както са изброени и номерирани в Насоките относно оценките на въздействието върху защитата на данните на Работната група по член 29 (бележка под линия 315, по-горе), стр.9 – 10. Основните коментари във връзка с факторите също са взети от тези насоки. Следва да се отбележи, че факторите донякъде се припокриват или могат да бъдат комбинирани, както е отбелязано при факторите в точката *„Многофакторни дейности с висок риск"*.

371 Работната група по член 29/ Европейският комитет по защита на данните добавя, че *„Обработването с малко или никакво въздействие върху лицата не отговаря на този специфичен*

Автоматизирана оценка на персонала („ако сте в най-долните 10% от екипа за броя разгледани случаи, ще получите „незадоволително" в оценката си, без обсъждане"). *

Идентифициране на „възможни" или „вероятни" данъчни измамници чрез автоматично определяне на профили на данъкоплатците.[372]

Идентифициране на „възможни" или „вероятни" измамници по схеми за социална закрила въз основа на профил на известни измамници.

Идентифициране на деца „в риск" когато пораснат да бъдат пълни или да станат членове на банди или престъпници или момичета, които е „вероятно" да забременят в тинейджърска възраст, на база на профили.[373]

Идентифицирането на млади хора и възрастни, като „изложени на риск" да бъдат "радикализирани".

3. Систематично наблюдение: обработване, използвано за следене, наблюдение или контрол на субекти на данни, включително данни, събрани чрез мрежи, или „*систематично мащабно наблюдение на публично достъпна зона*" (чл. 35, пар. 3, б. „в") . Този вид наблюдение е критерий, тъй като личните данни могат да бъдат събирани при обстоятелства, при които субектите на данни може да не са наясно, кой събира техните данни и как ще бъдат използвани същите. Освен това, може да е невъзможно лицата да избягват да бъдат подлагани на такова обработване в публично (или публично достъпно) пространство (места).

Примери:

Анализ на интернет трафика, пробив на криптирането. *

Скрито видеонаблюдение. *

Интелигентна система за видеонаблюдение CCTV [*например чрез използване на софтуер за разпознаване на лице*] в публично достъпни пространства. *

Инструменти за предотвратяване на загуба на данни, нарушаващи SSL криптирането. *

критерий. Допълнителни обяснения за тези понятия ще бъдат предоставени в предстоящите Насоки относно профилирането на Работната група по член 29."(Стр. 9).

372 Такива определяния бяха направени в **Италия** от Италианската агенция за приходите, използвайки инструмент, наречен *Redditometro*. Профилите бяха основани, наред с другото, на допускания за разходи, направени от данъкоплатците, изведени, според статистически параметри, от тяхното разпределение в конкретни семейни категории или географски области. Този инструмент за профилиране беше разследван от италианския орган по защита на данните, *Garante*. Един от основните въпроси беше ниското качество на данните и произтичащият от това висок процент грешки, базиран на ненадеждни изводи, получени от данните. Въз основа на своето разследване *Garante* издаде предписание, че реалният доход на данъкоплатеца може да се изчисли само от действителни, документирани разходи и не се извежда от базирани на статистика допускания за нива на разходите. Вж.: https://www.garanteprivacy.it/en/home/docweb/-/docweb-display/docweb/2765110

373 Виж Фондация за информационна политика на Обединеното кралство (FIPR), Childrens Databases - Safety & Privacy (Детски бази данни – Безопасност и неприкосновеност на личния живот), проучване за британския информационен комисар, 2006 г., достъпно на: https://www.cl.cam.ac.uk/~rja14/Papers/kids.pdf

Обработване на метаданни *(например, време, характер и продължителност на транзакция по банкова сметка*) за организационни цели или за предоставяне на бюджетни прогнози .[374]

4. Чувствителни данни или данни с високо лично естество: това включва специални категории лични данни, определени в чл. 9 (*лични данни, разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения или членство в синдикални организации, данни за здравословното състояние, генетични данни или биометрични данни и данни за сексуалната ориентация*), както и лични данни, свързани с присъди или нарушения, както е определено в чл. 10. Извън тези разпоредби на ОРЗД, някои категории данни могат да се считат за повишаващи възможния риск за правата и свободите на физическите лица. Тези лични данни се считат за чувствителни (както обикновено се разбира този термин), тъй като те са свързани с битови и частни дейности (*вж. третия пример, по-долу*), или защото оказват влияние върху упражняването на основно право *(вж. четвъртия пример)* или защото тяхното нарушение очевидно включва сериозни последици в ежедневния живот на субекта на данните *(вж. петия пример).* В тази връзка може да има значение дали данните вече са били направени публично достъпни от субекта на данни или от трети лица. Фактът, че личните данни са публично достъпни, може да се счита за фактор в оценката *[като се вземе под внимание дали субектът на данни може разумно да очаква, че данните могат да бъдат използвани от други хора за определени цели: вж. седмия пример, по-долу*].

Примери:

Обща болница [*или служба за социална закрила]*, която съхранява медицинските досиета на пациентите *[или на лицата претендиращи социални помощи*].

Частен детектив, който съхранява подробности за присъди или нарушения, [*или публичен орган, като държавна образователна институция, която съхранява тези данни по отношение на ученици или студенти в такива институции]*.

[*Публичен орган или частно лице (като работодател)*] с достъп до лични документи, електронни писма, дневници или бележки от електронни четци, позволяващи водене на бележки, притежавани от членове на персонала [*или използвани от персонала за лични и професионални цели , както е в „Ситуации на носене на собствено устройство [BYOD]*].

[*Публичен орган или частно лице* (като работодател)] с достъп до много лична информация, съдържаща се в приложенията за водене на дневник за живота*, или използващ информация от социалните мрежа в контекст, който може да има значителни последици за засегнатите лица, като например подбор на лица за работни места (или всъщност интервюта)*.

Медицински прегледи и проверки за съдимост, преди наемане на работа.

Административни разследвания и дисциплинарни производства. *

374 Този пример е взет от **Италианския** списък за Оценка на въздействието върху защитата на данните, одобрен от Европейския комитет по защита на данните.

Всяка употреба на 1: n биометрична идентификация. *

Снимки, използвани със софтуер за разпознаване на лице или използвани за извеждане на други чувствителни данни [*например, когато те могат да доведат до дискриминация в контекста на подбора*]. *

5. Мащабно обработвани данни: Общият регламент за защита на данните не определя какво представлява „в голям мащаб", въпреки че съображение 91 дава някои насоки.[375] Във всеки случай, Работната група по член 29 препоръчва да се вземат предвид, по-специално, следните фактори, когато се определя дали обработването се извършва в голям мащаб:
   a. броят на съответните субекти на данните, или като определен брой, или като процент от съответната популация;
   b. обема на данните и/или обхвата на различните данни, които се обработват;
   c. продължителността или постоянството на дейността по обработване на данни;
   d. географския обхват на дейността по обработване.

Пример:

Бази данни за наблюдение на болести [*национални, но евентуално свързани с ЕС*]. *

Мащабни обмени на данни между администраторите в публичния сектор (например министерства, местни и областни органи и др.) чрез електронни мрежи. [376]

Мащабното събиране на генеалогична информация за семейства на хора, принадлежащи към определена религиозна група.[377]

Създаването на много големи „бази данни за начина на живот" за маркетингови цели (които обаче е възможно - или поне могат – да бъдат използвани и за други цели).

Записването от политическите партии на възприеманите намерения за гласуване на много голям брой гласоподаватели (или домакинства) на

[375] Относителното пояснение в съображение 91 гласи: *„[Ш]ирокомащабни дейности по обработване [са дейности], чиято цел е обработване на значителен обем лични данни на регионално, национално и наднационално равнище, които биха могли да засегнат голям брой субекти на данни и които е вероятно да доведат до висок риск, например поради чувствителното си естество, [или] когато в съответствие с постигнатото ниво на технически познания се използва нова технология в голям мащаб... "*

[376] Този пример е взет от **Италианския** списък на оценката за въздействието върху защитата на данните, одобрен от Европейският комитет по защита на данните .

[377] Срв. решението на френския орган по защита на данните (*CNIL*) относно генеалогичния регистър на мормоните, издадено през 2013 г. и съобщено тук: https://www.nouvelobs.com/societe/20130613.OBS3162/les-mormons-autorises-par-la-cnil-a-numeriser-l-etat-civil-francais.html

национално или общодържавно ниво, въз основа на интервюта при лични посещения и последващия анализ и използване на тези данни. [378]

6. Съпоставяне или комбиниране на масиви от данни, [*по-специално ако те*] произхождат от две или повече дейности по обработване на данни, извършвани с различни цели и/или [*се извършват*] от различни администратори на данни по начин, който би надхвърлил разумните очаквания на субекта на данни.

Пример:

Скрито извършване на насрещна проверка на журналите за контрол на достъпа, компютърните дневници и декларациите за гъвкаво работно време [*от работодателя*] за откриване на отсъствия от работа.*

Данъчна служба сравнява своите записи за данъчни декларации със записите на собственици на скъпи яхти, за да потърси лица, които може евентуално да извършват данъчна измама.[379]

7. Данни относно уязвими субекти на данни (съображение 75): обработването на този вид данни е критерий поради увеличения дисбаланс на силите между субектите на данни и администратора на данни, което означава, че физическите лица може да не са в състояние лесно да дадат съгласие, или да се противопоставят на обработването на техните данни или да упражняват правата си. Сред уязвимите субекти на данни може да са включени **деца** (те могат да се считат за неспособни, съзнателно и разсъдливо да се противопоставят или да дават съгласие за обработване на техните данни), **служители**, по-уязвими групи от населението, които се нуждаят от специална защита (**психично болни, търсещи убежище** или **възрастни пациенти** и т.н.) и във всички случаи, когато може да се установи дисбаланс в отношенията между позицията на субекта на данни и администратора.

Примери:

Използване на системи за видеонаблюдение и геолокация, позволяващи дистанционно наблюдение на дейностите на служителите.[380]

По същество, всяко обработване на лични данни спрямо някоя от горепосочените категории уязвими лица, и със сигурност всяко обработване на чувствителни данни върху тях, или мащабно обработване на такива данни за такива хора, следва да се разглежда като присъщо носещо вероятност за „висок риск".

---

378 Тази практика е обичайна и наистина традиционна в Обединеното кралство, като е признато в съображение 56 от Общия регламент за защита на данните. В това съображение се казва, че това „*може да бъде разрешено* по съображения от обществен интерес, *при условие че са предвидени подходящи гаранции*" (добавено подчертаване). Ако не друго, тази нужда да се прецени дали обработването наистина служи за легитимен обществен интерес и изискването за приемане на „подходящи гаранции" подчертават необходимостта от сериозен анализ на риска и оценка на въздействието.

379 Това беше направено преди известно време в Холандия, при допускането, че големи яхти обикновено се купуват от данъчни измамници. Един човек, който се чувстваше на прицел, дразнещо наричаше кораба си „*Черни пари*".

380 Този пример е взет от **Италианския** списък за оценка на въздействието върху защитата на данните, одобрен от Европейският комитет по защита на данните.

8. Иновативно използване или прилагане на нови технологични или организационни решения. В Общия регламент относно защитата на данните става ясно (чл. 35, пар. 1 и съображения 89 и 91), че използването на нова технология, определена в „съответствие с постигнатото състояние на технологичните познания“ (съображение 91), може да предизвика необходимостта от извършване на Оценка на въздействието върху защитата на данните. Това е така, защото използването на такава технология може да включва нови форми или видове събиране и използване на данни, евентуално невидими и с висок риск за правата и свободите на хората. В действителност, личните и социални последици от внедряването на нова технология може да не са известни. Оценката на въздействието върху защитата на данните ще помогне на администратора на данните да разбере и да предприеме някакво действие спрямо такива рискове – и мерките за смекчаване, следва да позволят субектът на данни и широката общественост да видят как и кога и за какви цели ще се използват новите технологии, така че те да могат да се предпазят от тези, които могат да подкопаят индивидуалните права и свободи и да доведат до авторитарно управление или масово наблюдение от страна на корпорации (или последните да действат заедно).

   Бележка: В много такива случаи на нови технологии или практики, органите по защита на данните (или Европейският комитет по защита на данните) могат да издадат или може вече да са издали становища, насоки или препоръки – и длъжностните лица по защита на данните, трябва да са нащрек и да внимават за такива нови документи. Ако считат, че все още не са издадени съответни насоки и други, те следва да се консултират със своя орган по защита на данните. Вж. също Задачи 4, 8 и 10 по-долу.

   Примери:

   Комбинирано използване на пръстови отпечатъци и разпознаване на лица за по-добър контрол на физическия достъп.[381]

   Нови технологии, предназначени да проследяват времето и присъствието на служителите, включително тези, които обработват биометрични данни, както и други, като например проследяване на мобилни устройства.[382]

   Обработване на данни, генерирани чрез използването на приложения на „Интернет на нещата” (*свързани, „умни” устройства и неща*), ако използването на данните има (или може да има) значително въздействие върху ежедневния живот на физическите лица и неприкосновеността на личните им данни.

   Машинно обучение.*

---

[381] Работната група по член 29 и няколко национални органа по защита на данните издадоха подробни съвети по този въпрос, изискващи, наред с другото, биологичните данни да се съхраняват в микропроцесорен чип в устройството на субекта на данните, а не централно от администратора. Вж.: Работен документ за биометричните данни (Working document on biometrics) на Работна група по член 29 (WP80, приет на 1 август 2003 г.), стр.6, достъпен на адрес: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp80_en.pdf

[382] Виж Opinion 2/2017 on data processing at work (Становище 2/2017 относно обработката на данни на работното място) на Работната група по член 29 (WP249, прието на 8 юни 2017 г.), раздел 5.5, *Дейности по обработване, свързани с времето и присъствието*, на стр. 18 - 19, достъпно на адрес: www.ec.europa.eu/newsroom/document.cfm?doc_id=45631

Свързани коли.* Проверка в социалните мрежи на кандидатите, които са кандидаствали за определена позиция.*

9. Когато обработването само по себе си „*<u>пречи на субекта на данни да упражнява право или да използва услуга или договор</u>*” (чл. 22 и съображение 91). Това включва дейности по обработване, които имат за цел да позволят, променят или откажат достъп до услугата или сключването на договор от страна на субекти на данни.

<u>Примери</u>: Банка, която проверява своите клиенти в база данни със справки за кредити, за да реши дали да им предложи заем. *Финансова институция или агенция за даване на кредитен рейтинг, която взема предвид разликата във възрастта между съпрузите в брака, за да определи кредитоспособността (което може да възпрепятства свободното упражняване на основното право на брак – и поради това е било забранено във Франция от френския орган по защита на данните, CNIL (който е трябвало да направи оценка на системата, тъй като е взела решения въз основа на профили, като е подлежала на „предварително разрешение” от CNIL)*. Бази данни с изключения.* Кредитна проверка.*

<u>Многофакторни дейности с висок риск</u>

Изброените по-горе фактори могат да се припокриват или да се комбинират, например, „систематичното наблюдение” може да се припокрива и съчетава с автоматичното вземане на решения на базата на профили и може да включва „мащабно” обработване на „чувствителни данни”. Работната група по член 29 предоставя редица примери за дейности с такива комбинирани фактори (или критерии), за които се изисква Оценка на въздействието върху защитата на данните, и примери за дейности, при които един или повече от горепосочените фактори (или критерии) са налице, но където не е необходима Оценка на въздействието върху защитата на данните, както следва:[383]

Примери за обработване	**Възможни относими критерии**	**Вероятно ли е да се изисква Оценка на въздействието върху защитата на данните?**
Болницата обработва генетични данни и данни за здравословното състояние на	- <u>Чувствителни данни или данни с много личен характер.</u>	

[383] <u>Насоки за оценки на въздействието върху защитата на данните</u> на Работната група по член 29 (бележка под линия 315, по-горе), стр.11 – 12.

своите пациенти (болнична информационна система).	- Данни относно уязвими субекти на данни. - Данни, обработвани в голям мащаб.	Да
Използването на система от камери за наблюдение на поведението при шофиране по пътищата. Администраторът предвижда да използва интелигентна система за видео анализ, за да изолира автомобили и автоматично да разпознава регистрационни номера.	- Систематиченмониторинг. - Иновативно използване или прилагане на технологични или организационни решения.	
Дружество систематично наблюдава дейностите на своите служители, включително наблюдение на работната станция на служителите, дейността в интернет и др.	- Систематично наблюдение. - Данни относно уязвими субекти на данните.	
Събиране на данни от социалните мрежи за генериране на профили.	- Оценка. - Данни, обработвани в голям мащаб. - Съпоставяне или комбиниране на набори от данни. - Чувствителни данни или данни с високо лично естество:	
Институция, създаваща национален кредитен рейтинг или база данни за измами.	- Оценка. - Автоматизирано вземане на решения с правни или подобни съществени последици. - Не позволява на субекта на данни да упражняват правото си или да използва услуга или договор. - Чувствителни данни или данни с високо лично естество:	
Съхранение за целите на архивирането на псевдонимизирани лични чувствителни данни относно уязвими субекти на данни от изследователски проекти или клинични изпитвания.	- Чувствителни данни. - Данни относно уязвими субекти на данни. - Не позволява на субектите на данни да упражняват правото си или да използват услуга, или договор.	
Обработване на „лични данни на пациенти или клиенти на конкретен лекар, друг здравен работник или адвокат“ (съображение 91).	- Чувствителни данни или данни с много личен характер. - Данни относно уязвими субекти на данните.	Не
Онлайн списание, използващо списък с адреси на електронни пощи, за да изпраща на своите абонати, с тяхно съгласие, общ дневен бюлетин, и което включва лесен начин за отписване от списъка за в бъдеще.	- Данни, обработвани в голям мащаб.	

Уебсайт за електронна търговия, показващ реклами на първокласни автомобилни части, включващи ограничено профилиране въз основа на артикули, прегледани или закупени на собствения му уебсайт – отново, с лесна възможност за отписване.	- Оценка.	

Методологии за Оценки на въздействието върху защитата на данните:

Целите на Оценката на въздействието върху защитата на данните са:

(i) да **установи** точно (високите) рисковете, свързани с предложената операция по обработване, като взема предвид естеството на данните и обработването, обхвата, контекста и целите на обработването и източниците на риска – не само при нормални обстоятелства, но и при специални обстоятелства; и в краткосрочен, средносрочен и дългосрочен план;[384]

(ii) да **оцени** установеният (висок) риск, по-специално неговия произход, естество и особеност, както и вероятността от възникване на риска и възможната му сериозност;[385]

(iii) да определи какви **мерки** могат да бъдат предприети за намаляване на (високите) рискове, които са подходящи с оглед на наличните технологии и разходи за изпълнение, и да предложи тези мерки;[386] и

(iv) да **запише** констатациите, оценката и мерки, които са предприети (или не са предприети, с причините за това), така че да може да „**докаже съответствие**" с изискванията на Общия регламент относно защитата на данните по принципа за „отчетност" във връзка с оцененото обработване.[387]

Чл. 35, пар. 7 от Общия регламент относно защитата на данните предвижда, че (протоколът от) Оценката на въздействието върху защитата на данните трябва да съдържа „най-малко" следното:

а) системен опис на предвидените дейности по обработване и целите на обработването, включително, ако е приложимо, преследвания от администратора законен интерес;

б) оценка на необходимостта и пропорционалността на дейностите по обработване по отношение на целите;

в) оценка на рисковете за правата и свободите на субектите на данни, посочени в параграф 1;и

384 Вж Съображение 90.

385 Вж Съображение 84 и ISO 31000.

386 Вж Съображение 84.

387 Както посочва Работната група по член 29: „*Оценката на въздействието върху защитата на данните е процес за изграждане и демонстриране на съответствие*" – Насоки за оценки на въздействието върху защитата на данните на Работна група по член 29 (бележка под линия 315, по-горе), стр.4. За повече подробности относно принципа на отчетност и свързаните с него задължения за „демонстриране на съответствие", виж част 2 от наръчника.

г) мерките, предвидени за справяне с рисковете, включително гаранциите, мерките за сигурност и механизмите за осигуряване на защитата на личните данни и за демонстриране на спазването на настоящия регламент, като се вземат предвид правата и законните интереси на субектите на данни и на други заинтересовани лица.

Работната група по член 29 подчертава, че:[388]

> Всички съответни изисквания, изложени в Общия регламент относно защитата на данните, предоставят широка, обща рамка за проектиране и провеждане на оценка на въздействието върху защитата на данните. Практическото осъществяване на оценка на въздействието върху защитата на данните ще зависи от изискванията, изложени в Общия регламент относно защитата на данните, които може да бъдат допълнени с по-подробни практически насоки. **Следователно, реализацията на оценка на въздействието върху защитата на данните е мащабируема. Това означава, че дори и малък администратор на данни може да проектира и реализира оценка на въздействието върху защитата на данните, която е подходяща за неговите дейности по обработване.**

Следователно администраторите (в консултация с техните длъжностни лица по защита на данните) могат да изберат подходяща методология за всяка оценка на въздействието върху защитата на данните, която трябва да извършат. Те могат да се възползват от всеки опит, с подходящи налични инструменти за оценки на риска, например по ISO 31000. Въпреки това, Работната група по член 29 правилно отбелязва различната перспектива, от която трябва да се извършват оценки на въздействието върху защитата на данните съгласно Общия регламент относно защитата на данните (във всеки случай, по-тясно ориентирани към сигурността) оценки, основани на ISO:[389]

> Оценката на въздействието върху защитата на данните съгласно Общия регламент относно защитата на данните е инструмент за управление на рисковете за правата на субектите на данни, като по този начин възприема тяхната [т.е. на субектите на данните] гледна точка... Обратно, управлението на риска в други области (напр. информационна сигурност) е фокусирано върху [рисковете за] организацията.

Работната група по член 29 предоставя редица примери на методологии за въздействие върху защитата на данните и неприкосновеността на личния живот, изготвяни от национални органи по защита на данните[390], и *„насърчава разработването на специфични за сектора рамки за оценка на въздействието върху защитата на данните“*. Самата Работна група е публикувала Рамка на Оценка на въздействието върху защитата на данните за приложения за радиочестотно идентифициране и Образец на оценка на въздействието върху защитата на данните за интелигентни мрежови системи и системи за интелигентно измерване. [391]

---

388 Насоки за Оценки на въздействието върху защитата на данните на Работната група по член 29 (бележка под линия 315, по-горе), стр.17,.

389 *Пак там*.

390 Виж отново списъка с връзки в *Приложение 1* към Насоките за оценки на въздействието върху защитата на данните на Работната група по член 29 (бележка под линия 315, по-горе).

391 *Вж.*, бележки под линия 32 и 33.

Тук е достатъчно да се възпроизведат Критериите за приемлива оценка на въздействието върху защита на данните, посочени в насоките на Работната група по член 29[392]:

Приложение 2 – Критерии за приемлива оценка на въздействието върху защитата на данните

Работната група по член 29 предлага следните критерии, които администраторите на данни може да използват, за да преценят дали дадена оценка на въздействието върху защитата на данните или методология за извършване на оценка на въздействието върху защитата на данните е достатъчно изчерпателна, за да отговаря на изискванията на Общия регламент относно защитата на данните:

- **осигурено е систематично описание на обработването** (Член 35, параграф 7, б. „а”)**:**

- естеството, обхватът, контекстът и целите на обработеното се вземат предвид (съображение 90);
- записват се личните данни, получателите и периодът, за който ще се съхраняват личните данни;
- предоставя се функционално описание на операцията по обработване;
- установяват се активите, на които се разчитат личните данни (хардуер, софтуер, мрежи, хора, книжа или канали за предаване на книжа);
- взема се предвид спазването на одобрените кодекси за поведение [*механизми за сертифициране и/или ОКП*] [393] (чл. 35, пар. 8);

- **оценяват се необходимостта и пропорционалността** (чл.35, пар. 7, б. б))**:**

- мерките, предвидени за спазване на регламента, се определят (чл. 35, пар. 7, б. г и съображение 90), като се вземат предвид:
  - мерки, които допринасят за пропорционалността и необходимостта от обработване на базата на:
    - конкретна, изрична и законна(и) цел(и) (чл. 5, пар. 1, б. б));
    - законосъобразността на обработване (чл. 6);
    - подходящи, свързани със и ограничени до необходимото данни (чл. 5, пар. 1, б. „в“);
    - ограничена продължителност на съхранение (чл. 5, пар. 1, б. д))

---

392 *Вж.*, Приложение 2. За по-голяма яснота са добавени акцентите в удебелен шрифт в основните тирета.

393 Работната група по член 29 отбелязва , че:
„Спазването на кодекс за поведение (член 40) трябва да бъде взето предвид (член35, параграф 8) при оценка на въздействието на операция по обработване на данни. Това може да е полезно, за да се докаже, че са избрани или въведени адекватни мерки, при условие че кодексът за поведение е подходящ за операцията по обработване. Механизмите за сертифициране, печатите и маркировките за целите на доказването на съответствие с ОРЗД на дейности по обработване от администратори и обработващи лични данни (член 42), както и Обвързващите корпоративни правила (ОКП), също следва да бъдат взети предвид.”
Насоки за оценки на въздействието върху защитата на данните на Работната група по член 29 (бележка под линия 315, по-горе), стр.16.

- мерки, допринасящи за правата на субектите на данни:
  - информация, предоставена на субекта на данни (членове 12, 13 и 14);
  - право на достъп и на преносимост на данните (членове 15 и 20);
  - право на коригиране и на изтриване (членове 16, 17 и 19);
  - право на възражение и ограничаване на обработването (член 18, 19 и 21);
  - взаимоотношения с обработващите лични данни (чл. 28);
  - гаранции относно международното предаване (Глава V);
  - предварителна консултация (чл. 36).

- **рисковете за правата и свободите на субектите на данни се управляват (чл. 35, пар. 7, б. в)):**

- произходът, естеството, особеностите и сериозността на рисковете се оценяват (вж. съображение 84) или, по-конкретно, за всеки риск (незаконен достъп, нежелана промяна и изчезване на данни) от гледна точка на субектите на данните:
  - вземат се предвид източниците на рискове (съображение 90);
  - потенциални въздействия върху правата и свободите на субектите на данни се установяват в случай на събития, включително незаконосъобразен достъп, нежелано изменение и изчезване на данни;
  - идентифицирани са заплахи, които биха могли да доведат до незаконен достъп, нежелана промяна и изчезване на данни;
  - вероятността и тежестта са оценени (съображение 90);
- мерките, предвидени за третиране на тези рискове, са определени (чл. 35, пар. 7, б. г) и съображение 90);

- **при участие на заинтересувани лица:**

- се иска съвета на длъжностното лице по защита на данните (чл. 35, пар. 2);
- по целесъобразност се търсят становищата на субектите на данни или на техните представители (чл. 35, пар. 9).

Какво да правим с протокола от оценката на въздействието върху защитата на данните

Първата и основна цел на протокола от оценката на въздействието върху защита на данните (която обхваща всички горепосочени „критерии") е да има **доказателства**, относно извършена подходяща, задълбочена оценка на въздействието върху защитата на данните, в съответствие с Общия регламент относно защитата на данните (т.е. отговаряща на горепосочените критерии).

Когато ОВЗД установи едновременно (високи) рискове и мерки, които могат да бъдат предприети за преодоляване на тези рискове, които са „подходящи", като се отчита вероятността и сериозността на рисковете и разходите за мерките и когато такива мерки действително са били одобрени и приети (като това одобрение и приемане е необходимо да е записано), протоколът от ОВЗД може да представлява **важен „елемент" в цялостното доказване на съответствие** и специално доказателствено средство (въпреки че това не се равнява на правна презумция за съответствие и въпреки че длъжностното лице по защита на данните ще трябва регулярно да **проверява и наблюдава** дали смекчаващите мерки, продължават да се прилагат и продължават да

бъдат подходящи в светлината на практическите, организационните или технологичните развития: вж. в тази задача в точка „*Текущо наблюдение на спазването*“).

Примери за **случаи, при които Оценката на въздействието върху защитата на данните установява, както високи рискове, така и мерки за смекчаване, които са били счетени (в случая, от EuroPrise) за достатъчни, за да позволят обработването. Следователно и в двата случая администраторът би могъл уверено да заключи, че резултатът от оценката на въздействието върху защитата на данните показва, че обработването НЕ би трябвало да се представя на компетентния орган по защита на данните за консултация:**[394]

1. Агенция за социална закрила използва биометрично удостоверяване на самоличността, за да се бори с измамите в областта на социалната закрила.

Идентифициране на рисковете: Както Работната група по чл. 29 посочва, три от основните рискове, предизвикани от използването на биометрични данни, са: (i) фактът, че биометричните характеристики на дадено лице са незаменими (което означава, че инструмент удостоверяване на самоличността, базиран на сурови биометрични данни, веднъж загубени, не могат да бъдат заменени); (ii) лекотата, с която биометричните данни могат да се използват за съпоставяне на различни бази данни; и (iii) възможността биометричните данни да бъдат прихванати тайно.

Мерки за смекчаване: Като инструмент за (гласово) биометрично удостоверяване на самоличността, използван за борба с измамите в областта на социалната закрила, се използва уникален *шаблон* за глас, създаден от оригиналните („необработени”) биометрични данни, а не суровите данни, които се унищожават след регистриране на субектите на данни. Гласовият шаблон е уникален за всяко конкретно внедряване и не може да се използва за пресъздаване на оригиналните (необработени) биометрични данни. Това обхваща всички три гореспоменати риска: (i) ако гласовият шаблон бъде компрометиран, много просто може да бъде създаден нов, различен (с помощта на субекта на данни, който би трябвало да бъде записан отново); (ii) различните гласови шаблони, използвани в различни приложения на един и същ инструмент, не могат да бъдат съпоставяни един с друг или с други гласови данни или гласови шаблони; и (iii) гласовият шаблон се създава в процеса на записване лице в лице.

2. ***Една финансова институция проверява местоположението на мобилния телефон на клиента, за да види дали е (приблизително) на същото място, като банковата карта на клиента (която се използва за транзакция и е била маркирана като подозрителна).***

Идентифициране на рисковете: Точните подробности за местоположението на дадено лице в даден момент, могат да бъдат много разкриващи за чувствителни въпроси, и следователно разкриването на тези подробности представлява сериозна намеса в неприкосновеността и

394 Тези примери са взети от продукти, които са получили европейския печат за поверителност, с правните оценки, направени от Дау Корф, вж., съответно:
https://www.european-privacy-seal.eu/EPS-en/4F-self-certification (инструмент за удостоверяване на самоличността с четири фактора, който включва гласово биометрично решение);
https://www.european-privacy-seal.eu/eps-en/valid-pos (инструмент, който съответства на местоположението на подозрителна транзакция с банкова карта с (грубо) определяне на местоположение на мобилния телефон на притежателя на картата).
В оценките и двата продукта бяха похвалени за постигнатото голямо свеждане до минимум на данните и за характеристиките, свързани с неприкосновеността на личните данни на етапа на проектиране, както и за начина, по който те смекчават рисковете, свързани, съответно, с използването на биометрични данни и проверка на местоположението.

личния живот на съответното лице – както Европейския съд по правата на човека потвърди в дело *Naomi Campbell*.[395]

Мерки за смекчаване: В инструмента за предотвратяване на измами с банкови карти, данните за местоположението на мобилния телефон са редуцирани, дори преди да бъдат прехвърлени на потребителя на този инструмент (финансовата институция), на много обширна област, обикновено държава или щат. Това е достатъчно, за да може инструментът да работи ефективно (т.е. да е в състояние да установи с достатъчна сигурност дали въпросната сделка е действителна или измамна), като същевременно намали натрапчивостта на проверката на местоположението до абсолютния минимум.

Записът (протоколът) може също да се предостави (или да се използва) в **консултации**, включващи заинтересовани страни или граждани, или в отговор на **запитвания и оплаквания от субекти на данни и неправителствени организации**, представляващи субекти на данни (или пресата). В това отношение Работната група по чл. 29 отбелязва, че: [396]

> **Публикуването на оценка на въздействието върху защитата на данните не е правно изискване на Общия регламент относно защитата на данните, но администраторът решава да го направи. Въпреки това, администраторите трябва да обмислят публикуването поне на части, като резюме или заключение на тяхната Оценка на въздействието върху защитата на данните.**
>
> Целта на този процес би била да спомогне за насърчаване на доверието в дейностите по обработване на администратора и да демонстрира отчетност и прозрачност. ***Особено добра практика е да се публикува оценка на въздействието върху защитата на данните, когато членовете на обществото са засегнати от операцията по обработване. Това може да се случи по-специално, когато публичен орган извършва оценка на въздействието върху защитата на данните.***
>
> Публикуваната оценка на въздействието върху защитата на данните не трябва да съдържа цялата оценка, особено когато оценката може да представя конкретна информация, относно рисковете за сигурността за администратора на данни или да издава търговски тайни или търговски чувствителна информация. При тези обстоятелства публикуваната версия би могла да се състои само от резюме на основните констатации на оценката на въздействието върху защитата на данните, или дори само от изявление, относно извършена оценка на въздействието върху защитата на данните.

Протоколът от Оценката на въздействието върху защитата на данните е особено важен при разглеждане на всякакви въпроси от органи по защита на данните, независимо дали те действат в общото им надзорно качество или в отговор на жалба.

По-конкретно, когато оценката на въздействието върху защитата на данните установява едновременно два (високи) риска и установи, че **не** съществуват мерки, които могат да бъдат предприети, за да се отговори в достатъчна степен на всички тези рискове (или поне на мерки, които са „подходящи", като се вземе предвид вероятността и

---

395 Европейският съд по правата на човека, *MGN v. the UK*, решение от 18 януари 2011 г., достъпно на: https://hudoc.echr.coe.int/eng#{%22tabview%22:[%22document%22],%22itemid%22:[%22001-102965%22]}

396 Насоки за оценки на въздействието върху защитата на данните на Работната група по член 29 (бележка под линия 315, по-горе) стр.18, оригинално маркиране с удебелен шрифт, добавено маркиране с курсив и удебелен шрифт.

сериозността на рисковете и разходите за мерките), администраторът е длъжен да се **консултира с органа за защита на данните** (чл. 36) – и **протоколът от съответната оценка на въздействието върху защитата на данните, трябва да бъде предоставен на органа за защита на данните**:[397]

> Когато оценката на въздействието върху защитата на данните разкрие наличието на високи остатъчни рискове, от администратора на данните ще се изисква да потърси предварителна консултация за обработването от надзорния орган (чл. 36, пар. 1). Като част от това трябва да се предостави изцяло оценката на въздействието върху защита на данните (чл. 36, пар. 3, б. д). Надзорният орган може да предостави своите съвети[398] и няма да компрометира търговските тайни или да разкрива уязвимости в сигурността, при спазване на принципите, приложими във всяка държава-членка за публичен достъп до официални документи.

Държавите членки могат също така, съгласно **националното** си **законодателство**, да изискват от администраторите да се консултират с органа по защита на данните „във връзка с обработването от администратор за изпълнението на задача, осъществявана от администратора в полза на обществения интерес, включително обработване във връзка със социалната закрила и общественото здраве" (чл. 36, пар. 5), и това е направено за тези последни случаи, напр. във Франция и Италия.

Ако органът по защита на данните не е удовлетворен от информацията в протокола от оценката на въздействието върху защитата на данните (и/или предоставена по друг начин), органът по защитата на данните може да **разпореди** на администратора да предостави всяка допълнителна информация, за която смята, че се изисква за оценка на въпроса (вж. чл. 58, пар. 1, б. „а").

Обикновено органът по защита на данните ще се опита да **помогне** на администратора да намери решение – т.е. да определи мерки, които адекватно да смекчат установените (високи) рискове (по мнението на органа по защита на данните) и при условие, че администраторът изразява съгласие да приеме тези мерки (както и че тяхното приемане и последваща употребата се проверява и наблюдава от длъжностното лице по защита на данните), които биха разрешили проблема (както следва да бъде записано от длъжностното лице по защита на данните и разбира се също ще се запише от органа за защита на данните).

Алтернативно, органът по защита на данните може или да издаде **заповед** на администратора, като изисква администраторът да приеме конкретни мерки за предложената операция по обработване (вж. чл. 58, пар. 2, б. „г"), или действително да **забрани** предложеното обработване (чл. 58, пар. 2, б. „е").

Разбира се, длъжностното лице по защита на данните следва отново да запише всички такива разпореждания и да проверява регулярно спазването им (и да записва своите констатации). Но, както винаги, извън тази проверка, наблюдение и водене на документация, в крайна сметка администраторът ще бъде този, който носи отговорност за всяко неспазване.

---

397 *Вж*.

398 Писмени съвети за администратора са необходими само когато надзорният орган е на мнение, че планираното обработване не е в съответствие с регламента съгласно член 36, параграф 2. [оригинална бележка под линия]

- o – O – o –

Наблюдение на спазването (включително разследвания по жалби):

ЗАДАЧА 5: Повторение на задачи 1 – 3 (и 4) на текуща база

Както отбелязва Работната група по член 29 в своите (Одобрени от Европейския комитет по защита на данните) Насоки за длъжностните лица по защита на данните, чл. 39, пар. 1, б. „б“ възлага на длъжностното лице по защита на данните, наред с другите задължения, задължението да „наблюдава спазването” от своята организация на Общия регламент относно защитата на данните, а съображение 97 допълнително уточнява, че „администраторът или обработващият лични данни следва да бъде подпомаган при наблюдението на вътрешното спазване на настоящия регламент” от длъжностното лице по защита на данните.[399] Както самият термин „наблюдение” показва, това не е еднократна, а постоянна отговорност.

Въпреки това, съгласно нашето обсъждане относно ролята на длъжностното лице по защита на данните в част 2, раздел 2.5.4 по-горе, Работната група по член 29 също (отново) подчерта, че това: [400]

> не означава, че длъжностното лице по защита на данните е, това което е лично отговорно, когато има случай на несъответствие. Общият регламент относно защитата на данните ясно посочва, че администраторът, а не длъжностното лице по защита на данните, е длъжно да *„въвежда подходящи технически и организационни мерки, за да гарантира и да е в състояние да докаже, че обработването се извършва в съответствие с настоящия регламент*” (чл.24, пар. 1). Съответствието в областта на защитата е корпоративна отговорност на администратора на данни, а не на длъжностното лице по защита на данните.

Работната група по член 29 посочва по-нататък, че като част от тези задължения за наблюдение на спазването, длъжностните лица по защита на данните могат, по-специално, текущо да:

- събират информация за установяване на дейности по обработване,
- анализират и проверяват съответствието на дейностите по обработване, и
- информират, съветват и издават препоръки към администратора или обработващият лични данни.

Както отбелязва във връзка с оценките на въздействието върху защитата на данните (Задача 4):[401]

> Трябва да се подчертае, че за да се управляват рисковете за правата и свободите на физическите лица, рисковете трябва да се идентифицират, анализират, изчислят, оценят, третират (например смекчават ...) **и редовно да се преразглеждат**.

---

399 Насоки за длъжностните лица по защита на данните на Работната група по член 29 (бележка под линия 209, по-горе), раздел 4.1, *Наблюдение на спазването на Общия регламент относно защитата на данните*, на стр.16,7.

400 *Вж.*, оригинален курсив.

401 Насоки за оценки на въздействието върху защитата на данните на Работната група по член 29 (бележка под линия 315, по-горе), бележка под линия 10 на стр.6, добавен курсив.

С други думи, задачите от 1 – 4, по-горе (или ако няма дейности с вероятен „висок риск", задачи от 1 – 3), трябва да се повтарят текущо, и по-специално, разбира се, ако организацията промени, която и да е операция по обработване на лични данни, или изпълнява нови дейности. Както посочва Европейският надзорен орган по защита на данните (ЕНОЗД) (в своя съвет към институционалните длъжностни лица по защита на данните на ЕС):[402]

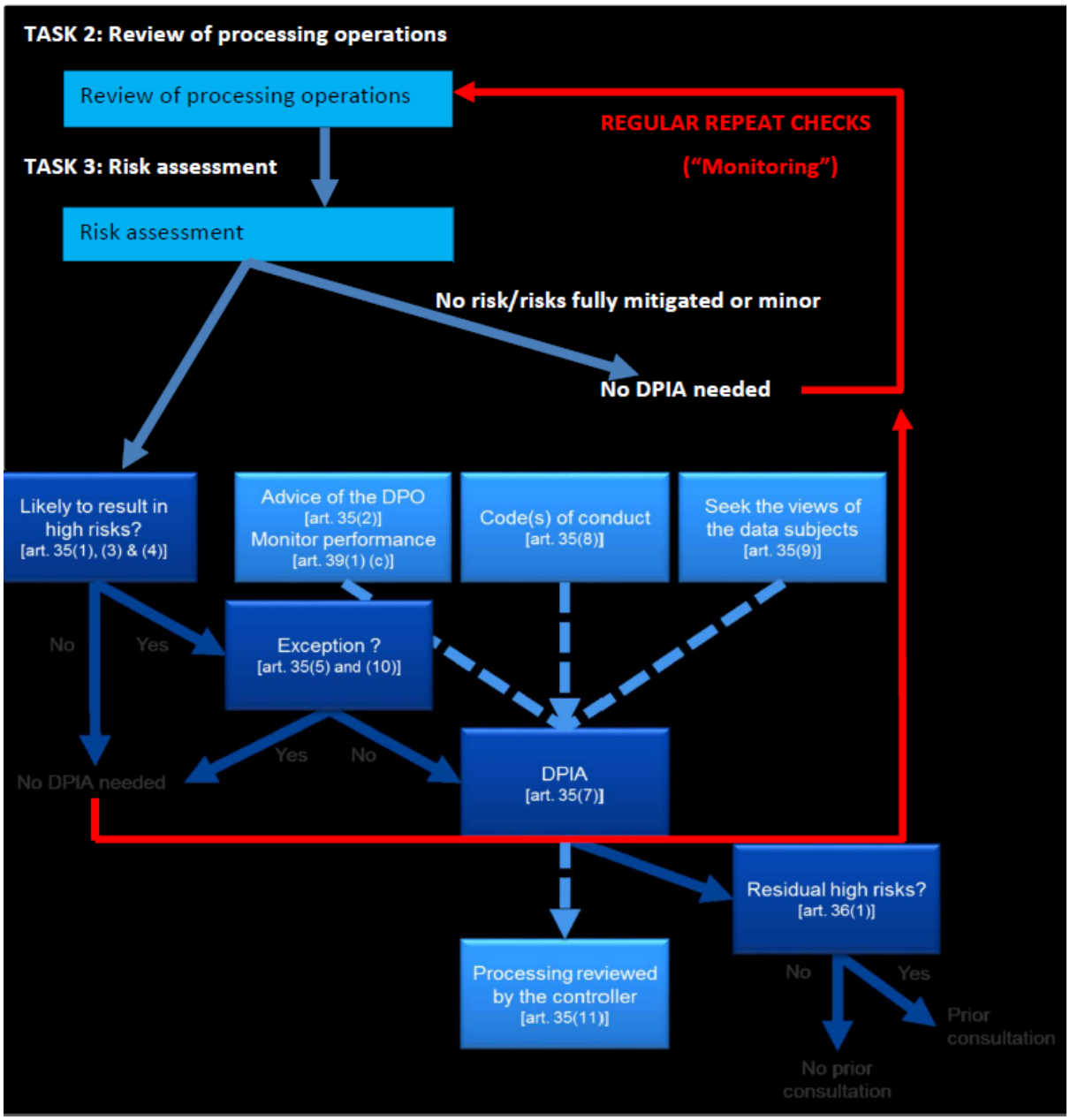
> Вашите записи трябва да отразяват действителността на дейностите по обработване във Вашата [институция]. Това означава, че трябва да сте сигурни, че са актуални. Когато [Вашата институция] планира да прави промени във Вашите дейности по обработване, проверете дали записът се нуждае от актуализиране. Добра идея е официално да включите тази проверка във Вашия процес на управление на промените. Може също да е добра идея да провеждате редовни прегледи независимо от планираните промени, за да уловите промени, които може да са останали незабелязани.

Работната група по член 29 е илюстрирала последната част от тази последователност в полезна диаграма, като са добавени и по-ранните етапи (Задачи 2 и 3).

Диаграма на Работната група по член 29 относно стъпките, които трябва да бъдат следвани във връзка с оценки на въздействието върху защитата на данните[403], като предходните стъпки (задачи 2 и 3) са добавени в горната кутия:

[402] Европейски надзорен орган по защита на данните (ЕНОЗД), Отчетност на място (бележка под линия 267, по-горе).

[403] Насоки за оценки на въздействието върху защитата на данните на Работната група по член 29 (бележка под линия 315, по-горе), стр.7.



Бележка: Изключенията по чл. 35, параграф 5, отбелязани в диаграмата на Работната група по чл. 29, са свързани с националната сигурност, отбраната, превенцията на престъпността и т.н.. Чл. 35, параграф 10 се отнася до разпоредбата, че не се изисква оценка на въздействието върху защитата на данните по отношение на обработване, уредено със закон, ако е извършена обща Оценка на въздействието върху защитата на данните от тази обработка в хода на подготовката на закона (което не включва длъжностното лице по защита на данните).

Като част от задълженията си по „мониторинг на спазването", длъжностното лице по защита на данните следва също така да се увери, че е запознато с всички промени в регулаторната и договорната (и т.н.) рамка, в рамките на която функционира неговата организация, както е предвидено в предварителната задача (Задача 0), така че то да може да установи въздействието на които и да е такива промени върху (текущата законосъобразност и съответствието с ОРЗД) дейностите по обработване на лични данни на организацията му и да може да дава подходящи съвети на съответните лица в неговата организация (включително висшето ръководство, когато е уместно).

В действителност длъжностното лице по защита на данните следва – когато е уместно, заедно с други длъжностни лица по защита на данните в неговата мрежа от ДЛЗД и/или с органа по защита на данните и в консултация с нейното висше ръководство –понякога трябва да бъде готово да заема позиции и възгледи относно предложените промени в тази рамка, като например предложения от правителство, организации като неговата да бъдат задължени, да получат възможност или да бъдат насърчени да споделят определени лични данни за нови цели.

- o – O – o –

ЗАДАЧА 6: Справяне с нарушения на сигурността на личните данни

Две от основните, важни нововъведения, въведени от Общия регламент относно защитата на данните в сравнение с Директивата за защита на данните от 1995 г., са (i) общо изискване за уведомяване на съответния (т.е. „компетентен") орган по защита на данните за всяко нарушение на сигурността на личните данни, което може да доведе до риск за правата и свободите на физическите лица; и (ii) задължение за информиране на субектите на данни за такива нарушения , в случай че водят до вероятност за „висок риск" за правата и свободите на физически лица.

Работната група по Член 29 е издала подробни насоки как трябва да се работи с нарушенията на сигурността на личните данни; [404] и тези насоки са одобрени от Европейския комитет по защита на данните на първото му заседание. [405] Обсъждането по-долу ще се основава в голяма степен на тези насоки и ще препраща към тях. Всички предоставени примери също така са взети от тези Насоки на Работната група по член 29[406].

Уведомяване на съответния орган по защита на данните:

Идеята за уведомяване за нарушения на сигурността на личните данни не е нова. Както е отбелязано по-горе в раздел 1.3.3[407], задължението за уведомяване за нарушение на сигурността на личните данни вече е било включено в директивата за правото на неприкосновеност на личния живот и електронни комуникации. Това задължение обаче е ограничено до доставчиците на електронни съобщителни мрежи и услуги.[408] Общият регламент относно защитата на данните използва същото определение за *„нарушение на сигурността на личните данни"*, каквато се съдържа в директивата за правото на неприкосновеност на личния живот и електронни комуникации, но без това ограничение:

> Нарушение на сигурността, което води до случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до лични данни, които се предават, съхраняват или обработват по друг начин. (чл. 4, параграф 12) [409]

---

[404] Работната група по член 29, Guidelines on Personal data breach notification under Regulation 2016/679 (Насоки относно уведомяване за нарушение на сигурността на личните данни съгласно Регламент 2016/679) (WP250 rev.01, приети на 3 октомври 2017 г., последно преработени и приети на 6 февруари 2018 г. (оттук нататък наричани: „Указания за уведомяване за нарушение на сигурността на данните на Работната група по член 29 или, в този раздел, просто „Насоки на Работната група по член 29"), достъпни на адрес: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052

[405] Виж бележка под линия 215, по-горе.

[406] Насоките на Работната група по член 29 също разглеждат задълженията за уведомяване по други нормативни актове: вж. Раздел VI от Насоките. Те не се обсъждат повече тук.

[407] В под-раздела за *„Основни характеристики на Регламента за неприкосновеността на личния живот и електронните съобщения"*, в подточка „Уведомление за нарушение на сигурността на данните".

[408] Както е отбелязано във въведението на Насоките на Работната група по член 29, някои държави-членки също вече имаха по-широки изисквания за уведомяване за нарушение на сигурността на данните.

[409] Директивата за правото на неприкосновеност на личния живот и електронни комуникации добавя, след същите тези думи, думите: *„във връзка с предоставянето на обществено достъпна електронна съобщителна услуга в Общността"* (чл. 2, б. „и").

Насоките на Работната група по член 29 уточняват в подробности какви съответни термини следва да се приемат, като смисъл и излага различните видове нарушения на сигурността на личните данни (*„нарушение на поверителността"; „нарушение на целостта"; „нарушение на наличността*");[410]

> **Примери**
>
> Пример за загуба на лични данни може да включва ситуация, в която устройство, съдържащо копие на базата данни с клиенти на администратора, е било изгубено или откраднато. Друг пример за загуба може да бъде, когато единственото копие на набор от лични данни е било криптирано от рансъмуер (злонамерен софтуер, който криптира данните на администратора, докато не бъде платен откуп), или е бил криптиран от администратора с помощта на ключ, който вече не е в него.
>
> Сред примерите за загуба на наличност са ситуации, в които данните са били заличени случайно или от неупълномощено лице, или в примера на сигурно криптирани данни, ключът за дешифриране е загубен. В случай, че администраторът не може да възстанови достъпа до данните, например от резервно копие, тогава това се смята за постоянна загуба на наличност.
>
> Загуба на наличност може да възникне и при значителни прекъсвания на нормалната услуга в дадена организация, например при прекъсване на електрозахранването или атака с отказ на услуга, което прави личните данни недостъпни.

Дори временна загуба на наличност може да представлява нарушение на сигурността на личните данни:

> **Примери:**
>
> В контекста на една болница, ако важни медицински данни за пациентите не са налични, дори и временно, това може да представлява риск за правата и свободите на физическите лица; например, могат да бъдат отменени операции и може да бъдат изложени на риск човешки животи.
>
> Обратно, в случай, че системите на медийната компания не са налични в продължение на няколко часа (напр. поради прекъсване на електрозахранването), и ако тази компания не може да изпраща бюлетини на своите абонати, това е малко вероятно да представлява риск за правата и свободите на физическите лица.
>
> Заразяването с рансъмуер би могло да доведе до временна загуба на наличност, ако данните могат да бъдат възстановени от резервно копие/архивирани данни. Въпреки това все пак е налично проникване в мрежата и би могло да се изиска уведомяване, ако инцидентът е квалифициран като нарушение на поверителността (т.е. нападателят е осъществил достъп до лични данни) и това представлява риск за правата и свободите на физически лица.

Чл. 33, пар. 1 предвижда, че:

---

410 Насоките на Работна група по член 29, стр.7, във връзка с по-ранно (от 2014 г.) становище на Работната група по член 29 за уведомяване за нарушение.

> В случай на нарушение на сигурността на личните данни администраторът, без ненужно забавяне и когато това е осъществимо — не по-късно от 72 часа след като е разбрал за него, уведомява за нарушението на сигурността на личните данни надзорния орган, компетентен в съответствие с чл. 55, освен ако не съществува вероятност нарушението на сигурността на личните данни да породи риск за правата и свободите на физическите лица. Уведомлението до надзорния орган съдържа причините за забавянето, когато не е подадено в срок от 72 часа. (чл. 33, пар. 1)

Обработващият лични данни „*уведомява администратора без ненужно забавяне, след като узнае за нарушаване на сигурността на лични данни*“ (чл. 33, пар. 2). Работната група по член 29 препоръчва на обработващият лични данни:

> **Незабавно** да уведоми администратора, като допълнителна информация за нарушението се предоставя на етапи при получаване на допълнителни подробности. Това е важно**,** за да се помогне на администратора да изпълни изискването за уведомяване на надзорния орган в рамките на 72 часа. (Насоки на Работната група по член 29, стр.14)

Администраторът ще бъде считан за „**осведомен**” за нарушението, след като обработващият лични данни го е уведомил;[411] след това администраторът трябва да уведоми органа по защита на данните (както е посочено), освен ако не се прилага *предупреждението*, че нарушението на данните е вероятно да доведе до риск за правата и свободите на физически лица.

В някои случаи обработващият лични данни може да действа за определен брой – може би дори голям брой – различни администратори, например като доставчик на пространство в облак за съхранение за данни. Работната група по член 29 дава следния съвет за такива ситуации:

> Когато обработващият лични данни предоставя услуги на множество администратори, които са засегнати от един и същ инцидент, обработващият лични данни ще трябва да съобщи подробности за инцидента на всеки администратор.
>
> Обработващият лични данни може да даде уведомление от името на администратора, ако администраторът е дал на обработващия лични данни надлежното разрешение и това е част от договорните споразумения между администратора и обработващия лични данни. Такова уведомление трябва да бъде направено в съответствие с чл. 33 и чл. 34. Важно е обаче да се отбележи, че юридическата отговорност за уведомяване остава на администратора. (стр.14)

В уведомлението за нарушението на сигурността на данните до съответния („компетентен”) орган по защита на данните[412], „се съдържа най-малко следното”:

> а. описание на естеството на нарушението на сигурността на личните данни, включително, ако е възможно, категориите и приблизителният брой на засегнатите субекти на данни и категориите и приблизителното количество на засегнатите записи на лични данни;

---

411 Насоки на Работната група, стр.14.

412 За указания относно уведомяването за трансгранични нарушения и за нарушения, които се извършват в предприятия извън ЕС, виж раздел С в Насоките на Работната група по член 29 (стр. 16 – 18).

б. посочване на името и координатите за връзка на длъжностното лице по защита на данните или на друг контакт, от който може да се получи повече информация;

в. описание на евентуалните последици от нарушението на сигурността на личните данни;

г. описание на предприетите или предложените от администратора мерки за справяне с нарушението на сигурността на личните данни, включително по целесъобразност мерки за намаляване на евентуалните неблагоприятни последици.

(чл.33, пар.3)

В това отношение Работната група по член 29 заявява, че администраторът може:[413]

ако е необходимо, да избере да предостави допълнителни подробности. Различните видове нарушения (поверителност, цялост или наличност) могат да изискват предоставяне на допълнителна информация, за да се обяснят напълно обстоятелствата за всеки отделен случай.

Пример

Като част от уведомлението, което прави до надзорния орган, администраторът може да намери за полезно да посочи лицето, което обработва личните данни, ако той е в основата на нарушението, особено ако това е довело до инцидент, засягащ регистрите с лични данни на много други администратори, които използват същия обработващ лични данни.

Във всеки случай, надзорният орган може да поиска допълнителни подробности в рамките на разследването на нарушението.

Още повече:

Когато и доколкото не е възможно да се предостави информацията едновременно, информацията може да бъде предоставена на етапи без ненужно допълнително забавяне. (чл. 33, пар. 4)[414]

Пример:

Администраторът уведомява надзорния орган в рамките на 72 часа след откриването на нарушение, че е загубил USB ключ, съдържащ копие от личните данни на някои от клиентите му. По-късно USB ключът е намерен неправилно подреден в помещенията на администратора и се възстановява. Администраторът уведомява надзорния орган и иска изменение на уведомлението.

Време за уведомяване:

Насоките на Работната група по член 29 пояснява кога може да се каже, че администратор (или обработващ лични данни) е „**разбрал**" за нарушение на сигурността на данни и подчертава, че има и задължения за предвиждане и подготовка за такова събитие:[415]

413 Насоки на Работната група по член 29, стр.15.

414 За подробности и допълнителни насоки по този въпрос, вж. Насоките на Работната група по член 29, стр.15 - 16.

415 Насоки на Работната група по член 29, стр.10 – 11.

Както е посочено подробно по-горе, ОРЗД изисква в случай на нарушение администраторът да уведоми за нарушението без ненужно забавяне и, когато е възможно, не по-късно от 72 часа след като е узнал за това. Това може да повдигне въпроса, кога администраторът може да се счита, че е „разбрал" за нарушението. Работна група по чл. 29 счита, че администраторът трябва да се разглежда като „разбрал", когато администраторът притежава разумна степен на сигурност, за възникналия инцидент, свързан със сигурността, който е довел до компрометиране на лични данни. Въпреки това, както е посочено по-горе, Общият регламент относно защитата на данните изисква от администратора да приложи всички подходящи технически и организационни мерки за защита, за да установи незабавно дали е настъпило нарушение и да информира незабавно надзорния орган и субектите на данни. В него се посочва също така и факът, че уведомлението е направено без ненужно забавяне. Следва да се установи, като се вземат предвид по-специално естеството и тежестта на нарушението и неговите последици и неблагоприятни последици за субекта на данните. Това налага на администратора задължение да гарантира, че той ще е „разбрал" за всякакви нарушения своевременно, така че да може да предприеме подходящи действия.

Кога точно администратор може да се счита за „разбрал" за конкретно нарушение, зависи от обстоятелствата на конкретното нарушение. В някои случаи ще бъде сравнително ясно от самото начало, че е имало нарушение, докато в други случаи може да отнеме известно време, за да се установи дали личните данни са били компрометирани. Въпреки това, акцентът трябва да бъде поставен върху незабавни действия за разследване на инцидент, за да се определи дали сигурността на личните данни наистина е била нарушена, и ако е така, да се предприемат коригиращи действия и да се даде уведомление при необходимост.

Примери

1. В случай на загуба на USB ключ с некриптирани лични данни често е невъзможно да се установи дали неупълномощените лица са придобили достъп до тези данни. Въпреки това, макар че администраторът може да не е в състояние да установи дали е настъпило нарушение на поверителността, такъв случай трябва да бъде съобщен, тъй като има разумна степен на сигурност, че е настъпило нарушение на наличността; администраторът ще е „разбрал", когато открие, че USB ключът е бил изгубен.

2. Трето лице уведомява администратора, че случайно е получило личните данни на един от неговите клиенти и предоставя доказателства за неразрешено разкриване. Тъй като на администратора са били представени ясни доказателства за нарушение на поверителността, тогава не може да има съмнение, че е „разбрал".

3. Администраторът открива, че е имало възможно проникване в неговата мрежа. Той проверява системите си, за да установи дали личните данни, държани в тази система, са компрометирани и потвърждава, че е така. Още веднъж, тъй като администраторът вече има ясни доказателства за нарушение, не може да има съмнение, че той е „разбрал".

4. Киберпрестъпник се свързва с администратора, след като е хакнал системата му, за да поиска откуп. В този случай, след проверка на системата, за да потвърди, че е бил атакуван, администраторът има ясни доказателства, че е настъпило нарушение и няма съмнение, че е разбрал.

5. Дадено лице уведомява администратора, че е получило електронно писмо, представящо се за администратора, което съдържа лични данни, свързани с (действително) използване от негова страна на услугата на администратора, което предполага, че сигурността на администратора е била компрометирана. Администраторът провежда краткотрайно разследване и установява проникване в мрежата му и доказателства за непозволен достъп до лични данни. Сега администраторът ще се счита за „разбрал" и е необходимо уведомяване на надзорния орган, освен ако не е вероятно това да представлява риск за правата и свободите на физическите лица. Администраторът ще трябва да предприеме подходящи коригиращи действия за отстраняване на нарушението.

Документиране и оценка на нарушението:

Общият регламент относно защитата на данните също така предвижда че:

> Администраторът документира **всяко** нарушение на сигурността на личните данни, включително фактите, свързани с нарушението на сигурността на личните данни, последиците от него и предприетите действия за справяне с него. Тази документация дава възможност на надзорния орган да провери дали е спазен настоящият член. (чл. 33, пар. 5), добавено подчертаване)

Следва да се отбележи, че последното изискване се отнася до **всяко** („което и да е") нарушение на сигурността на личните данни: то не се ограничава до нарушения на сигурността на данни, за които трябва да бъде уведомен органът по защита на данните, т.е. записът трябва да включва и всяко нарушение на сигурността на данни, което (според мнението на администратора) „не съществува вероятност да породи риск за правата и свободите на физическите лица ".

На практика, длъжностното лице по защита на данните ще трябва да бъде тясно и в дълбочина ангажирано с тези въпроси. Често е вероятно подозрението за нарушение първо да бъде съобщено в организацията (и/или на Директора по технологиите или на сигурността) – и тогава длъжностното лице по защита на данните трябва (по целесъобразно, с тези други директори) да направи първата, незабавна оценка поне на следните въпроси:

- дали действително е имало нарушение на сигурността на личните данни, както е определено в Общия регламент относно защитата на данните (вж. определението в чл. 4, пар. 12, цитиран по-горе) –

и ако се установи, че е имало нарушение, или че е вероятно да е имало нарушение:

- кои (категории) субекти на данни са били или може да са били засегнати от нарушението и кои (категории) лични данни може да са били загубени или засегнати по друг начин–

БЕЛЕЖКА: Работната група по член 29 препоръчва тези категории също да бъдат съобщени на органа по защита на данните при всяко уведомление за нарушение, и всъщност: [416]

> Ако видовете субекти на данни или видовете лични данни показват риск от настъпване на конкретни вреди в резултат на нарушение (например кражба на самоличност, измама, финансова загуба, заплаха за професионална тайна), тогава

[416] Насоки на Работна група по член 29, стр.14.

е важно уведомлението да посочва тези категории. По този начин то е свързано с изискването за описване на **вероятните** последици от нарушението.

и като вземат предвид тези въпроси:

- дали нарушението е „вероятно" или „не е вероятно" да доведе до риск за правата и свободите на физическите лица –

Работната група по член 29 обсъжда въпроса кога не се изисква уведомяване в подробности[417] и дава следния пример:

> **Пример**
>
> Нарушение, което не би изисквало уведомяване на надзорния орган, е загубата на сигурно криптирано мобилно устройство, използвано от администратора и неговия персонал. При условие, че ключът за криптиране остава в защитеното притежание на администратора и това не е единственото копие на личните данни, тогава личните данни ще бъдат недостъпни за нападателя. Това означава, че не е вероятно нарушението да доведе до риск за правата и свободите на въпросните субекти на данни. Ако по-късно стане очевидно, че ключът за кодиране е компрометиран или че софтуерът за криптиране или алгоритмът е уязвим, рискът за правата и свободите на физическите лица ще се промени и по този начин вече може да се изиска уведомяване.

но ако оценката е, че има вероятност от такъв потенциален риск:

- дали рискът е „висок риск за правата и свободите на [тези] физически лица" (тъй като това би изисквало не само уведомяване за нарушението на органа по защита на данните, но и информирането на субектите на данни, както е отбелязано в следващата подточка).[418]

Както посочва Работната група по член 29, важността на възможността да се установи нарушение, да се оцени рискът за физическите лица и след това да се даде уведомление, ако е необходимо, се подчертава в съображение 87 от Общия регламент относно защитата на данните:

> Следва да се установи дали са били приложени всички подходящи мерки за технологична защита и организационни мерки, за да се определи незабавно дали е налице нарушение на личните данни и своевременно да се информира надзорният орган и субектът на данни. Фактът, че уведомлението е направено без ненужно забавяне следва да бъде установен, като се отчитат по-конкретно естеството и тежестта на нарушението на личните данни и последиците и неблагоприятното въздействие от него върху субекта на данни. Такова уведомление може да доведе до намесата на надзорния орган в съответствие със задачите и правомощията, които са му предоставени с настоящия регламент.

---

[417] Насоки на Работна група по член 29, стр. 18 – 19. Виж също неизчерпателния списък от примери, представени в приложение (Приложение Б) към Насоките, възпроизведени по-долу, в следващата подточка.

[418] Виж по-специално обсъждането в подточката „*Оценка на риска и висок риск*".

И разбира се, ако оценките показват, че е било налице нарушение и че съществуват рискове за интересите на физическите лица, тогава спешно трябва да се потърсят **мерки за ограничаване.**

Посочените по-горе въпроси също трябва **спешно**, **възможно най-рано**, да бъдат предадени на най-висшето ръководство. В действителност, никоя вътрешна дискусия по горепосочените въпроси не следва да забави информирането на най-висшето ръководство веднага щом бъде установено нарушение.

Фактът, че тези оценки са извършени добросъвестно, следва да бъде **внимателно записан**, [419] заедно с резултатите от съответните оценки и с причините за тези оценки; разглежданите мерки за ограничаване; фактът, че оценките и предложените мерки за ограничаване са съобщени на най-висшето ръководство; действителните мерки, разрешени от ръководството, и дали, и кога са били извършени; и, разбира се, фактът, че нарушението (ако е установено, подлежи на съобщаване) е съобщено на съответния орган по защита на данните и кога, с копие от уведомлението; и когато е необходимо, фактът, че субектите на данни са били информирани и как, с копие на съответното известие и всяко съответно съобщение за пресата и т.н. (както е обсъдено в следващата точка). Освен това, както е посочено в Насоките на Работната група по член 29:

> Документирането на нарушението следва да се извърши докато то се развива (стр. 12).

В организации, които са назначили длъжностно лице по защита на данните, то ще играе важна роля в това отношение, като работната група по член 29 подчертава следното:[420]

> Администратор или обработващ лични данни може да има длъжностно лице по защита на данните (ДЛЗД), било то в съответствие с изискването на чл. 37, или доброволно като въпрос на добра практика. Чл. 39 от ОРЗД определя поредица от задължителни задачи за длъжностното лице по защита на данните, но не възпрепятства разпределянето на допълнителни задачи от администратора, ако е целесъобразно.
>
> От особено значение за уведомяването за нарушение, задължителните задачи на длъжностното лице по защита на данните включват, наред с другите задължения, предоставяне на съвети за защита на данните и информация на администратора или обработващия лични данни, наблюдение на спазването на Общия регламент относно защитата на данните и даване на съвети във връзка с оценки на въздействието върху защитата на данните. Освен това длъжностното лице по защита на данните трябва и да си сътрудничи с надзорния орган и да действа като звено за контакт между надзорния орган и субектите на данни. Следва също така да се отбележи, че при уведомяване на надзорния орган за нарушението, чл. 33, пар. 3, б. „б“ изисква администраторът да посочи името и данните за контакт на своето длъжностно лице по защита на данните или друга форма за контакт.
>
> Що се отнася до документирането на нарушения, администраторът или обработващият лични данни може да поиска да получи становището на своето длъжностно лице по защита на данните относно структурата, създаването и

---

419 Работната група по член 29 препоръчва това да бъде направено *„в плана за съобщаване на инциденти на администратора и/или договореностите за управление“* (стр.12). Това е допълнително подробно разгледано в Насоките на Работната група по член 29, Раздел V, *Отчетност и водене на записи*”.

420 Насоки на Работната група по член 29, Раздел V.B, стр.27 – 28.

администрирането на тази документация. Освен това на длъжностно лице по защита на данните може да бъде възложено допълнително да поддържа такива записи.

Тези фактори означават, че длъжностното лице по защита на данните следва да играе ключова роля в подпомагането на предотвратяването или подготовката за нарушение, като предоставя консултации и наблюдение на спазването, както и по време на нарушение (т.е. когато уведомява надзорния орган) и по време на всяко последващо разследване от надзорния орган. В тази светлина, Работната група по член 29 препоръчва длъжностното лице по защита на данните да бъде своевременно информирано за съществуването на нарушение и да бъде включено в целия процес на управление на нарушението и съобщаване на същото.

Насоките на Работната група по член 29 изясняват, че организациите следва не просто да реагират в това отношение. По-скоро те трябва да разполагат с **политика за сигурност**, която ***предварително*** се стреми да избягва всякакви нарушения на данните и съдържа планове за тяхното предотвратяване, ограничаване и прекратяване. Във връзка с дейностите по обработване на личните данни, които вероятно предизвикват „високи рискове" за интересите на физическите лица, разработването на такава политика може да бъде част от съответната оценка на въздействието върху защитата на данните (както е разгледано в Задача 4 по-горе).[421]

Информиране на субектите на данни:

Работната група по член 29 изяснява изискванията за информиране на субектите на данни за нарушения на сигурността на данните, както следва:

В някои случаи, освен да уведоми надзорния орган, администраторът също така е длъжен да съобщи за нарушението на засегнатите лица.

Чл. 34, пар. 1 гласи:

> Когато има вероятност нарушението на сигурността на личните данни да породи висок риск за правата и свободите на физическите лица, администраторът, без ненужно забавяне, съобщава на субекта на данните за нарушението на сигурността на личните данни.

Администраторите трябва да си припомнят, че уведомяването на надзорния орган е задължително, освен ако няма вероятност да представлява риск за правата и свободите на физическите лица в резултат на нарушение. Освен това, когато има вероятност за висок риск за правата и свободите на лицата в резултат на нарушение, трябва да бъдат информирани и лицата. Следователно прагът за съобщаване на нарушение на физически лица е по-висок, отколкото за уведомяване на надзорните органи, поради което не всички нарушения ще трябва да бъдат съобщени на физическите лица, като по този начин ще ги предпази от ненужно затрупване с уведомления.

Общият регламент за защита на данните предвижда, че съобщаването за нарушения на физически лица следва да се извършва „без ненужно забавяне", което означава възможно най-скоро. Основната цел на уведомяването на лицата е да се предостави конкретна информация за стъпките, които следва да предприемат, за да защитят себе си. Както е отбелязано по-горе, в зависимост от естеството на нарушението и предизвикания от него риск, своевременната

421 Насоки на Работната група по член 29, стр.6.

комуникация ще помогне на лицата да предприемат стъпки, за да се предпазят от всякакви отрицателни последици от нарушението.

Приложение (Приложение B) към насоките на Работната група по член 29, което предоставя (неизчерпателен) списък с 10 примера за нарушения на сигурността на личните данни и кой трябва да бъде уведомен, е приложено към обсъждането на настоящата задача като Приложение.

Насоките на Работната група по член 29 продължават както следва:[422]

Информация, която трябва да бъде предоставена

При уведомяване на лицата, чл. 34, пар. 2 уточнява че:

> В съобщението до субекта на данните, посочено в параграф 1 от настоящия член, на ясен и разбираем език се описва естеството на нарушението на сигурността на личните данни и се посочват най-малко информацията и мерките, посочени в чл. 33, пар. 3, б. „б“, „в“ и „г“.

Според тази разпоредба администраторът трябва да предостави поне следната информация за:

- описание на естеството на нарушението;
- името и данните за контакт на длъжностно лице по защита на данните или на друга форма за контакт;
- описание на вероятните последици от нарушението;
- описание на предприетите или предложените от администратора мерки за справяне с нарушението на сигурността на личните данни, включително по целесъобразни мерки за намаляване на евентуалните неблагоприятни последици.

Пример:

Като пример за мерките, предприети за отстраняване на нарушението и за намаляване на евентуалните неблагоприятни последици от него, администраторът може да заяви, че след като е уведомил за нарушението съответния надзорен орган, администраторът е получил съвет относно управлението на нарушението и намаляването на неговото въздействие. Администраторът следва също, когато е уместно, да предостави конкретни съвети на лицата, за да се предпазят от възможни неблагоприятни последици от нарушението, като например нулиране на пароли в случая, когато техните данни за достъп са компрометирани. И относно администраторът може да избере да предостави информация в допълнение към това, което се изисква тук.

Насоките изясняват също така, че:[423]

> По принцип съответното нарушение следва да бъде съобщено директно на засегнатите субекти на данни, освен ако това не включва несъразмерни усилия. В такъв случай вместо това, трябва да има публично съобщение или подобна мярка, чрез която субектите на данни се информират по също толкова ефективен начин (чл. 34, пар, 3, б. „в“).

422 Раздел III.B, стр.20. Текстът е редактиран само за презентация.

423 Раздел III.C, стр.21; виж за повече указания относно алтернативните начини за съобщаване на нарушение на сигурността на данните на засегнатите субекти на данни.

Съобщенията до субектите на данни следва да се правят „веднага щом това е разумно осъществимо и в тясно сътрудничество с надзорния орган" (съображение 86). Както се отбелязва в насоките:[424]

> Следователно администраторите могат да пожелаят да се свържат и да се консултират с надзорния орган не само, за да потърсят съвет, но и относно информирането на субектите на данните за нарушение в съответствие с чл. 34, но също и за подходящите съобщения, които трябва да бъдат изпратени на физическите лица, и за най-подходящия начин за връзка с последните.
>
> Свързан с това е съветът, даден в съображение 88, че при уведомяването за нарушение следва да „се отчитат законните интереси на правоприлагащите органи, когато ранното разкриване, може ненужно да попречи при разследването на обстоятелствата, свързани с нарушението на сигурността на личните данни". Това може да означава, че при определени обстоятелства, когато това е оправдано, и по препоръка на правоприлагащите органи, администраторът може да забави съобщаването на нарушението на засегнатите лица до момента, в който това не би засегнало неблагоприятно тези разследвания. След този срок обаче субектите на данни все пак, ще трябва да бъдат своевременно информирани.
>
> Когато администраторът не е в състояние да съобщи за нарушение на дадено лице, тъй като няма достатъчно съхранени данни, за да се свърже с лицето, в този конкретен случай администраторът следва да информира лицето веднага щом това е разумно осъществимо (напр. когато лицето упражнява правото си на достъп до лични данни по чл. 15 и предоставя на администратора необходимата допълнителна информация, за да се свърже с него).

Изключения:

Както отбелязват Насоките на Работната група по член 29:[425]

> чл. 34, пар, 3 предвижда три условия, които, ако са изпълнени, не изискват уведомяване на физическите лица в случай на нарушение. Това са:
>
> - Администраторът да е приложил подходящи технически и организационни мерки за защита на личните данни преди нарушението, по-специално тези мерки, които правят личните данни неразбираеми за всяко лице, което няма разрешение за достъп до тях. Това би могло, например, да включва защита на личните данни с най-съвременно криптиране или чрез токен.
> - Незабавно след нарушение, администраторът да е предприел стъпки, за да гарантира, че предизвиканият висок риск за правата и свободите на физическите лица вече не е вероятно да се материализира. Например, в зависимост от обстоятелствата по случая, администраторът може веднага да е идентифицирал и предприел действия срещу лицето, осъществило достъп до лични данни, преди то да е успяло да направи нещо с тях. Все пак е необходимо да се обърне дължимото внимание на възможните последици от всяко нарушение на неприкосновеността, отново в зависимост от естеството на съответните данни.
> - Това би изисквало несъразмерни усилия за контакт с лица, вероятно когато техните данни за контакт са били изгубени в резултат на нарушението или

424 *Вж.*, стр. 21 – 22.

425 Раздел III.D, стр.22,

на първо място не са известни. Например, складът на статистическа служба е наводнен и документите, съдържащи лични данни, са съхранени само на хартиен носител. Вместо това администраторът трябва да направи публично съобщение или да предприеме подобна мярка, с която лицата да бъдат информирани по също толкова ефективен начин. В случай на несъразмерни усилия могат да се предвидят и технически договорености за предоставяне на информация за нарушението при поискване, което може да се окаже полезно за онези лица, които могат да бъдат засегнати от нарушение, но с които администраторът не може да се свърже по друг начин.

В съответствие с принципа за отчетност администраторите следва да могат да докажат пред надзорния орган, че отговарят на едно или повече от тези условия. Трябва да се има предвид, че макар първоначално уведомяването да не се изисква, ако няма риск за правата и свободите на физически лица, това може да се промени с времето и рискът да трябва да бъде преоценен.

Ако администратор реши да не съобщи за нарушение на лицето, чл. 34, параграф 4 обяснява, че надзорният орган може да изиска от него да направи това, ако счита, че нарушението има вероятност да породи висок риск за физическите лица. Като алтернатива, той може да счете, че са изпълнени условията в чл. 34, пар. 3, в който случай не се изисква уведомяване на физически лица. Ако надзорният орган определи, че решението за несъобщаване на субектите на данни не е добре обосновано, той може да обмисли възможността да използва наличните си правомощия и санкции.

Оценка на риска и висок риск:

За пореден път може да е достатъчно да се цитират Насоките на Работната група по член 29:[426]

Въпреки че Общият регламент относно защитата на данните въвежда задължението за уведомяване за нарушение, няма изискване то да се прави при всички обстоятелства:

- Необходимо е уведомяване на компетентния надзорен орган, освен ако няма вероятност нарушението да породи риск за правата и свободите на физическите лица.
- Съобщаването на нарушение на лицето се задейства, само когато е вероятно да породи висок риск за неговите права и свободи.

Това означава, че веднага след узнаването за нарушение е жизнено важно администраторът не само да се стреми да ограничи инцидента, но и да оцени риска, който може да произтече от него. Има две важни причини за това: първо, познаването на вероятността и потенциалната сериозност на въздействието върху индивида ще помогне на администратора да предприеме ефективни стъпки за ограничаване и справяне с нарушението; второ, то ще му помогне да определи дали е необходимо уведомяване на надзорния орган и, ако е необходимо, на заинтересуваните лица.

Както е обяснено по-горе, уведомяването за нарушение се изисква, освен ако няма вероятност то да породи риск за правата и свободите на физическите лица, а ключовият фактор, изискващ съобщаване на нарушение на субектите на данни, е

[426] Раздел IV.A и B, стр.23, препратките са пропуснати; отново донякъде редактирани за презентационни цели.

когато има вероятност да породи висок риск за правата и свободите на физическите лица. Този риск съществува, когато нарушението може да доведе до физически, материални или нематериални вреди за лицата, сигурността на чиито данни е била нарушена.

Примери:

Примери за такива вреди са дискриминация, кражба на самоличност или измама, финансова загуба и увреждане на репутацията. Когато нарушението включва лични данни, които разкриват расов или етнически произход, политически убеждения, религиозни или философски убеждения или членство в синдикална организация, или включват генетични данни, данни относно здравословното състояние или данни относно сексуалния живот, или присъди и нарушения или свързани с тях мерки за сигурност, тези вреди трябва да се считат за вероятни.

Фактори, които трябва да се вземат предвид при оценката на риска

Съображения 75 и 76 от Общия регламент относно защитата на данните предполагат, че като цяло при оценката на риска следва да се обърне внимание както на вероятността, така и на сериозността на риска за правата и свободите на субектите на данни. По-нататък се посочва, че рискът следва да се оценява въз основа на обективна оценка.

Следва да се отбележи, че оценката на риска за правата и свободите на субектите на данни, в резултат на нарушение има различен фокус върху риска, разглеждан в оценката на въздействието върху защитата на данните. В ОВЗД се отчитат, както рисковете от обработването на данните, които се извършват както е планирано, така и рисковете в случай на нарушение. При разглеждане на потенциално нарушение, се разглежда принципно вероятността това да се случи, както и вредите за субекта на данните, които могат да възникнат; с други думи, това е оценка на хипотетично събитие. При действително нарушение, събитието вече е настъпило и така фокусът е изцяло върху произтеклия риск от въздействието на нарушението върху физическите лица.

Пример:

ОВЗД показва, че предложеното използване на конкретен софтуерен продукт за сигурност за защита на личните данни е подходяща мярка за гарантиране на ниво на сигурност, съответстващо на риска, който иначе би представлявал обработването за физическите лица. Ако обаче уязвимостта стане известна впоследствие, това би променило способността на софтуера да ограничи риска до защитените лични данни и следователно рискът ще трябва да бъде преоценен като част от текуща Оценка на въздействието върху защитата на данните.

По-късно се използва уязвимостта в продукта и възниква нарушение. Администраторът следва да оцени конкретните обстоятелства на нарушението, засегнатите данни и потенциалното ниво на въздействие върху физическите лица, както и вероятността този риск да се осъществи.

Съответно, когато се оценява рискът за физическите лица в резултат на нарушение, администраторът следва да вземе предвид конкретните обстоятелства на нарушението, включително тежестта на потенциалното въздействие и

вероятността това да се случи. Поради това Работната група по член 29 препоръчва оценката да вземе предвид следните критерии:[427]

Видът нарушение

Видът на нарушението, което е възникнало, може да повлияе на нивото на риска за физическите лица.

Пример:

Нарушение на поверителността, при което медицинската информация е разкрита на неупълномощени лица, може да има различен набор от последици за дадено лице в сравнение с нарушение, при което медицинските данни на дадено лице са загубени и вече не са налични.

Естеството, чувствителността и обема на личните данни

Разбира се, когато се оценява рискът, ключов фактор е видът и чувствителността на личните данни, които са били компрометирани от нарушението. Обикновено колкото по-чувствителни са данните, толкова по-голям е рискът от увреждане на засегнатите хора, но трябва да се вземат предвид и други лични данни, които може вече да са налични, за субекта на данните. Например разкриването на името и адреса на физическо лице, при обичайни обстоятелства, няма вероятност да причини значителни вреди. Въпреки това, ако името и адресът на осиновителя са разкрити на рожден родител, последствията могат да бъдат много тежки както за осиновителя, така и за детето.

Нарушения, включващи данни за здравословното състояние, документи за самоличност или финансови данни, като например данни за кредитни карти, могат да причинят вреда самостоятелно, но ако се използват заедно, те могат да бъдат използвани за кражба на самоличност. Комбинацията от лични данни обикновено е по-чувствителна от един елемент от личните данни.

Някои видове лични данни могат да изглеждат първоначално относително безвредни, но това, което тези данни могат да разкрият за засегнатото физическо лице, трябва да бъде внимателно обмислено. Списък с клиенти, приемащи редовни доставки, може да не е особено чувствителен, но същите данни за клиентите, които са поискали техните доставки да бъдат спрени, докато са на почивка, биха били полезна информация за престъпниците.

По същия начин, малко количество силно чувствителни лични данни може да окаже силно въздействие върху дадено физическо лице, а голям набор от подробности може да разкрие по-широка гама от сведения за този индивид. Също така, нарушение, което засяга големи обеми от лични данни за много субекти на данни, може да има ефект върху съответния голям брой физически лица.

Улесняване на идентификацията на физически лица

[427] Член 3.2 от Регламент 611/2013 предвижда насоки за факторите, които следва да бъдат взети предвид във връзка с уведомяването за нарушения в сектора на електронните съобщителни услуги, които могат да бъдат полезни в контекста на уведомлението съгласно Общия регламент относно защитата на данните. Вж.:
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:en:PDF
[оригинална бележка под линия]

Важен фактор, който трябва да се вземе под внимание, е колко лесно ще бъде за лице, което има достъп до компрометирани лични данни, да идентифицира конкретни лица или да съпостави данните с друга информация, за да идентифицира лица. В зависимост от обстоятелствата, идентифицирането може да бъде възможно, директно от личните данни с нарушена сигурност, без да е необходимо специално изследване, за да се разкрие самоличността на лицето, или може да бъде изключително трудно да се съпоставят личните данни с конкретно лице, но това все пак да може да бъде възможно при определени условия. Идентификацията може да бъде пряко или непряко възможна от нарушените данни, но може да зависи и от специфичния контекст на нарушението и от публичната достъпност на свързаните лични данни. Това може да е по-относимо за нарушения на поверителността и наличността.

Както е посочено по-горе, личните данни, защитени с подходящо ниво на криптиране, ще бъдат неразбираеми за неупълномощени лица без ключа за декриптиране. Освен това, надлежно извършената псевдонимизация (определена в чл. 4, пар. 5 като „обработването на лични данни по такъв начин, че личните данни не могат повече да бъдат свързвани с конкретен субект на данни, без да се използва допълнителна информация, при условие че тя се съхранява отделно и е предмет на технически и организационни мерки с цел да се гарантира, че личните данни не са свързани с идентифицирано физическо лице или с физическо лице, което може да бъде идентифицирано"), също може да намали вероятността лицата да бъдат идентифицирани в случай на нарушение. Техниките по псевдономизиране обаче не могат, сами по себе си, да се разглеждат като правещи данните неразбираеми.

Тежест на последиците за физическите лица.

В зависимост от естеството на личните данни, засегнати в дадено нарушение, например специални категории данни, потенциалната вреда за лицата, която би могла да произтече, може да бъде особено тежка, особено когато нарушението може да доведе до кражба на самоличност или измама, физическо увреждане, психологически стрес, унижение или увреждане на репутацията. Ако нарушението се отнася до лични данни за уязвими лица, те биха могли да бъдат изложени на по-голям риск от увреждане.

Дали администраторът е наясно, че личните данни са в ръцете на хора, чиито намерения са неизвестни или вероятно злонамерени, може да има отношение към нивото на потенциалния риск. Може да има нарушение на поверителността, при което личните данни се разкриват на трета страна, както е определено в чл. 4, пар. 10, или друг получател по погрешка. Това може да се случи, например, когато личните данни се изпращат случайно в грешен отдел на организация, или в често използвана организация-доставчик. Администраторът може да поиска от получателя или да върне, или да унищожи сигурно данните, които е получил. И в двата случая, като се има предвид, че администраторът е в текуща връзка с тях и може да е запознат с техните процедури, история и други относими данни, получателят може да се счита за „доверен". С други думи, администраторът може да има ниво на сигурност с получателя, така че да може разумно да очаква от тази страна да не чете или да не осъществява достъп до изпратените по погрешка данни и да спазва инструкциите му да ги върне. Дори ако до данните е бил осъществен достъп, администраторът все още може да се довери на получателя да не предприема допълнителни действия с него. Получателят е възможно да върне данните на администратора своевременно и да си сътрудничи с него за възстановяването им. В такива случаи това може да бъде включено в оценката на

риска, която администраторът извършва след нарушението – фактът, че получателят е доверен, може да премахне сериозността на последиците от нарушението, но не означава, че нарушението не е настъпило. Това, обаче, от своя страна, може да премахне вероятността от риск за физическите лица, като по този начин вече не се изисква уведомяване на надзорния орган или на засегнатите лица. Отново, това ще зависи от конкретния случай. Независимо от това, администраторът все още трябва да пази информация относно нарушението като част от общото задължение за поддържане на записи за нарушения.

Следва да се вземе предвид и трайността на последиците за лицата, когато въздействието може да се разглежда като по-голямо, ако последиците са дългосрочни.

Специални характеристики на индивида

Нарушението може да повлияе върху личните данни, засягащи деца или други уязвими лица, които могат – в резултат на това – да бъдат изложени на по-голям риск от опасност. Възможно е да има други фактори за физическото лице, които могат да повлияят на нивото на въздействие на нарушението върху тях.

Специални характеристики на администратора на данни

Характерът и ролята на администратора и неговите дейности могат да повлияят на нивото на риск за физическите лица в резултат на нарушение. Например, една медицинска организация ще обработва специални категории лични данни, което означава, че има по-голяма заплаха за лицата, ако сигурността на техните лични данни е нарушена, в сравнение със списък на вестник с адреси на електронни пощи.

Броят на засегнатите физически лица

Нарушението може да засегне само едно или няколко физически лица или няколко хиляди, ако не и много повече. Като цяло, колкото по-голям е броят на засегнатите лица, толкова по-голямо може да бъде въздействието на нарушението. Нарушението обаче може да има сериозно въздействие дори върху едно лице, в зависимост от естеството на личните данни и контекста, в който са били компрометирани. Отново, ключът е да се разгледа вероятността и сериозността на въздействието върху засегнатите физически лица.

Общи положения

Следователно, когато се извършва оценка на риска, който е вероятно да възникне в резултат на нарушение, администраторът следва да обмисли комбинация от сериозността на потенциалното въздействие върху правата и свободите на физическите лица и вероятността от възникването им. Ясно е, че когато последствията от нарушението са по-тежки, рискът е по-висок и по подобен начин, когато вероятността от възникването им е по-голяма, рискът също се засилва. Ако има съмнения, администраторът следва да действа внимателно и да предостави уведомление. Приложение В съдържа някои полезни примери за различни видове нарушения, включващи риск или висок риск за физическите лица.

Агенцията на Европейския съюз за мрежова и информационна сигурност (ENISA) е изготвила препоръки за методология за оценка на тежестта на нарушението, която

администраторите и обработващите лични данни могат да намерят за полезна при разработването на плана им за реакция на управлението на нарушенията.[428]

- o – O – o -

[428] Агенция на Европейския съюз за мрежова и информационна сигурност (ENISA), Препоръки за методология за оценка на тежестта на нарушенията на сигурността на личните данни, https://www.enisa.europa.eu/publications/dbn-severity [оригинална бележка под линия]

Приложение:

Примери за нарушения на сигурността на лични данни и кой да се уведомява
(От Насоките на работната група по член 29)

Пример	**Уведомяване на надзорния орган?**	**Уведомяване на субекта на данни?**	**Бележки / препоръки**
i. Администраторът е направил архив на архивирани лични данни, шифровани на USB ключ. Ключът е откраднат при проникване с взлом.	Не.	Не.	Доколкото данните са криптирани с модерен алгоритъм, съществуват резервни копия на данните, уникалният ключ не е компрометиран и данните могат да бъдат възстановени в разумен срок, това не подлежи на съобщаване за нарушение. Ако обаче те бъдат компрометирани по-късно, се изисква уведомление.
ii. Администратор поддържа онлайн услуга. В резултат на кибератака срещу тази услуга, са изтеглени лични данни на физически лица. Администраторът има клиенти в една държава-членка.	Да, съобщете на надзорния орган, ако има вероятност за последици за физически лица.	Да, съобщете на физическите лица в зависимост от естеството на засегнатите лични данни и дали тежестта на вероятните последици за лицата е висока.	
iii. Кратко прекъсване на електрическото захранване, което трае няколко минути в центъра за обаждания на администратора, което означава, че клиентите не могат да се обадят на администратора и да осъществят	Не.	Не.	Това не е нарушение, което подлежи на уведомяване, но все пак представлява инцидент, подлежащ на записване, съгласно чл. 33, пар. 5. Администраторът трябва да поддържа подходящи записи.

достъп до своите записи.			
iv. Администратор е подложен на атака от рансъмуер, което води до криптиране на всички данни. Не са налични резервни копия и данните не могат да бъдат възстановени. При разследването става ясно, че единствената функционалност на рансъмуера е да криптира данните и че в системата няма друг зловреден софтуер.	Да, съобщете на надзорния орган, ако има вероятни последици за хората, тъй като това е загуба на наличност.	Да, съобщете на физическите лица, в зависимост от естеството на засегнатите лични данни и възможния ефект от липсата на наличност на данни, както и други вероятни последици.	Ако има налично резервно копие и данните могат да бъдат възстановени своевременно, това не трябва да се докладва на надзорния орган или на лицата, тъй като няма да има постоянна загуба на наличност или поверителност. Ако обаче надзорният орган е разбрал за инцидента чрез други средства, той може да обмисли разследване, за да оцени спазването на по-широките изисквания за сигурност на чл. 32.
v. Лице се обажда в телефонния център на банка, за да съобщи за нарушаване на сигурността на данни. Лицето е получило месечно извлечение за някой друг. Администраторът предприема кратко разследване (т.е. извършено в рамките на 24 часа) и установява с разумна увереност, че е настъпило нарушение на сигурността на лични данни и дали има системен недостатък, който може да означава, че други лица са или биха могли да бъдат засегнати.	Да.	Само засегнатите лица се уведомяват, ако съществува висок риск и е ясно, че други не са засегнати.	Ако след по-нататъшно разследване се установи, че са засегнати повече лица, трябва да се съобщи това на надзорния орган и администраторът да предприеме допълнителна стъпка за уведомяване на други лица, ако съществува висок риск за тях.

vi. Администратор управлява онлайн пазар и има клиенти в много държави членки. Пазарът е подложен на кибератака и потребителски имена, пароли и история на покупките са публикувани онлайн от нападателя.	Да, съобщете на водещия надзорен орган, ако включва трансгранично обработване.	Да, тъй като може да доведе до висок риск.	Администраторът трябва да предприеме действия, напр. чрез налагане на нулиране на паролите на засегнатите профили, както и други стъпки за намаляване на риска. Администраторът следва също така да разгледа всички други задължения за уведомяване, напр. по Директивата за МИС като доставчик на цифрови услуги.
vii. Дружество за уеб хостинг, което действа като обработващ лични данни, установява грешка в кода, който контролира оторизацията на потребители. Ефектът от недостатъка означава, че всеки потребител може да осъществява достъп до данните за профила на всеки друг потребител.	Като обработващ лични данни, дружеството за хостинг трябва да уведоми засегнатите си клиенти (администраторите) без ненужно забавяне. Ако приемем, че дружеството за хостинг е извършило собствено разследване, засегнатите администратори следва да бъдат разумно уверени за това дали всеки е претърпял нарушение и следователно е вероятно да се счита, че е „осведомен", след като са били уведомени от хостинг дружеството (обработващия лични данни). След това администраторът	Ако е вероятно да няма висок риск за физическите лица, те не трябва да бъдат уведомявани.	Дружеството за хостинг на (обработващ лични данни) трябва да разгледа всички други задължения за уведомяване (напр. Съгласно Директивата за МИС като доставчик на цифрови услуги). Ако няма доказателства, че тази уязвимост се експлоатира с някой от нейните администратори, може да не е настъпило нарушение, което подлежи на уведомление, но да е вероятно то да е подлежащо на записване или да е въпрос на неспазване съгласно чл. 32.

	трябва да уведоми надзорния орган.		
viii. Медицинските досиета в болница са недостъпни за период от 30 часа поради кибератака.	Да, болницата е длъжна да уведоми, тъй като може да възникне висок риск за благосъстоянието на пациента и неприкосновеността на личния му живот.	Да, съобщете на засегнатите лица.	
ix. Лични данни на голям брой студенти погрешно се изпращат до неправилен списък с адреси на електронни пощи с повече от 1000 получатели.	Да, съобщете на надзорния орган	Да, съобщете на физическите лица в зависимост от обхвата и вида на включените лични данни и от сериозността на възможните последствия.	
x. На получателите се изпраща електронно писмо за директен маркетинг в полетата „до:" или „с копие до:", като по този начин всеки получател може да види адреса на електронна поща на други получатели.	Да, уведомяването на надзорния орган може да бъде задължително, ако са засегнати голям брой физически лица, ако се разкрият чувствителни данни (например пощенски списък на психотерапевт) или ако други фактори представляват висок риск (например писмото съдържа първоначалните пароли).	Да, съобщете на физическите лица в зависимост от обхвата и вида на включените лични данни и от сериозността на възможните последствия.	Уведомяване може да не е необходимо, ако не се разкрият никакви чувствителни данни и ако се разкрият само незначителен брой адреси на електронна поща.

- o – O – o -

ЗАДАЧА 7: Задача за разследване (включително обработването на вътрешни и външни жалби)

Забележка: Тази задача е отделна и различна от обработката на заявките на субекти на данни за достъп, корекция и др., както е посочено в Задача 8.

Разследване

Въпреки че не е изрично посочено в Общия регламент относно защитата на данните, от широките описания на общото положение и задачи на длъжностното лице по защитата на данните – и по-специално от неговото задължение да „наблюдава съответствието“ с Общия регламент относно защитата на данните: чл. 39, пар. 1, б. „б” – следва, че длъжностното лице по защитата на данните може по своя собствена инициатива или по искане на ръководството или например на представителния орган или на синдикалната организация на персонала, или реално на всяко друго физическо лице (от или извън организацията, или дори лица, подаващи сигнали, които се надяваме, че са защитени в съответната страна), да **разследва** въпроси и събития, пряко свързани с неговите задачи, и да **докладва** обратно на лицето или органа, който му е възложил или поискал от него разследването и/или на висшето ръководство. Както Европейският надзорен орган по защита на данните посочва в своето Становище относно длъжностните лица по защита на данните:[429]

> **Наблюдение на спазването** (…): длъжностното лице по защита на данните трябва да осигури прилагането на Регламента в рамките на институцията. Длъжностното лице по защита на данните може по своя собствена инициатива или по искане на институцията или органа, администратора, комитета на персонала или което и да е лице да разследва въпроси и събития, пряко свързани с неговите задачи, и да докладва на лицето, което е възложило разследването, или на администратора.

Общият регламент относно защитата на данните ясно посочва, макар и не толкова изрично, колкото *приложението* към регламента за защита на данните на институциите на ЕС, че длъжностните лица по защита на данните трябва да получат **всички съответни ресурси и достъп до всички данни и помещения, инсталации за обработване на данни и носители на данни** (с всички съответни и необходими правомощия за ***удостоверяване на самоличност*** и ***влизане и*** **съхранение**), необходими за изпълнение на техните задачи (вж. чл. 38, пар. 2), т.е. също във връзка с такива разследвания. [430] По същия начин, въпреки че това отново е посочено по-категорично във връзка с институционалните длъжностни лица по защита на данните на ЕС в сравнение с длъжностните лица по защита на данните, назначени съгласно Общия регламент относно защитата на данните, **всички служители на съответния администратор – и всъщност персоналът на всички външни агенции, включително по-специално обработващите лични данни (включително доставчиците на облачни услуги, използвани от администратора) – следва да окажат пълно съдействие на**

---

[429] Европейски надзорен орган по защита на данните, Position paper on the role of Data Protection Officers in ensuring effective compliance with Regulation (EC) 45/2001 (Становище относно ролята на Длъжностните лица по защита на данните при осигуряването на ефективно спазване на Регламент (ЕО) 45/2001) (бележка под линия 210, по-горе), стр.6, оригинален акцент в удебелен шрифт.

[430] *Приложението* към Регламент (ЕС) № 45/2001 постановява, че длъжностното лице по защита на данните на институтициите на ЕС: *„има по всяко време достъп до данните, които са обект на дейности по обработка, както и до всички помещения, инсталации за обработка на данни и носители на данни*“ , *Приложение*, член 4, второ изречение).

длъжностното лице по защита на данните при такива разследвания и да дават ***пълни отговори*** **и** ***информация*** в отговор на всякакви въпроси или искания на длъжностното лице по защита на данните.[431] **Администраторите следва ясно и точно да ги опишат във вътрешните насоки на персонала, като включат ясни и относими към темата клаузи в своите договори с външни доставчици и обработващи лични данни.**

Приложение

Въпреки че е компетентно да наблюдава съответствието с Общия регламент относно защитата на данните, да преглежда жалби и да разследва възможни нарушения на Регламента, **длъжностното лице по защита на данните има ограничени правомощия за прилагане**. По принцип, както е отбелязано по-горе, ако длъжностното лице по защита на данните установи, че организацията му или някой външен доставчик или обработващ лични данни не е спазил(а) ОРЗД в някое отношение, длъжностното лице по защита данните следва да съобщи това на висшето ръководство – и в такъв случай е отговорност на висшето ръководство да предприеме коригиращи действия, включително, когато е уместно, санкции срещу служител или агенти или обработващи лични данни, които не са изпълнили съответните си задължения, например като издава предупреждения или други санкции или, в изключителни случаи, уволнение или прекратяване на договори. Например, ако се използва външен доставчик на услуги за събиране на данни (например чрез автоматизирани системи, управлявани от доставчика), и този доставчик не отговаря на изискванията по Общия регламент относно защитата на данните, напр. от гледна точка на информационни уведомления или, по-лошо, като използва събраните данни тайно за по-нататъшни (недекларирани) цели, длъжностното лице по защита на данните следва да предложи администраторът да използва друг доставчик и същевременно да предупреди органа за защита на данните.

Липсата на такова действие ще бъде на сметка на администратора (организацията) при разглеждането на принудително действие от страна на държавния орган по защита на данните, включително при определяне на нивото, на която и да е „административна глоба", която може да бъде наложена (вж. чл. 83).

Освен това една от задачите на длъжностното лице по защита на данните е „да се консултира" със съответния орган по защита на данните, „по целесъобразност", по отношение на всеки възникнал въпрос (чл. 39, пар. 1, б. „д")). В случай на сериозна разлика във вижданията между длъжностното лице по защита на данните и висшето ръководство на неговата организация, когато според длъжностното лице по защита на данните конкретна операция по обработване е или ще бъде в (съществено) нарушение на Общия регламент относно защитата на данните и/или съответното национално законодателство, но ръководството все пак иска да я предприеме, или възнамерява да не налага санкции срещу нея, то със сигурност ще изглежда „целесъобразно" за длъжностното лице по защита на данните да упражнява това право и (ефективно) да отнесе въпроса до органа по защита на данните. След това органът по защита на данните ще използва своите правомощия за разследване и правоприлагане, включително възможността да разпореди неизпълнението или спирането на операцията, тъй като той

---

431 *Приложението* към Регламент (ЕС) № 45/2001 предвижда, че: *„Всеки съответен контролиращ орган е длъжен да оказва съдействие на длъжностното лице за защита на данните при изпълнение на неговите/нейните задължения, както и да предоставя информация в отговор на поставени въпроси*." (*Приложение*, член 4, първо изречение).

(органът по защита на данните) счита това за целесъобразно (виж, по-специално, чл. 58, пар. 2, б. „г“ и „е“).

Вж. по-долу, в точки *„Сътрудничество и консултиране с органа за защита на данните*” и *„Разглеждане на запитвания и жалби*”.

- o – O – o -

Консултативни задачи

ЗАДАЧА 8: Консултативна задача – общи положения

Длъжностните лица по защита на данните трябва да гарантират спазването на Регламента и да дават съвети на администраторите за изпълнението на задълженията им. Поради това, длъжностното лице по защита на данните може да **информира**, да предлага **съвет** или да отправя **препоръки** за ***практическото подобряване*** на защитата на данните от организацията и/или по въпроси, свързани с прилагането на разпоредбите за защита на данните (т.е. на Общия регламент относно защитата на данните и други закони на ЕС в областта на защитата на данните – като например за Директивата от 2002 г. за правото на неприкосновеност на личния живот и електронни комуникации и, в бъдеще, възможен регламент за неприкосновеността на личния живот и електронните съобщения – и на всеки национален закон, разгръщащ „уточнителните клаузи“ в Общия регламент относно защитата на данните или приложим по друг начин); и за ***изменение и актуализиране на политиките и практиките за защита на данните на организацията*** в светлината на нови нормативни актове, решения, мерки или насоки (вж. чл. 39, пар. 1, б. „а“).

За тази цел следва да се даде възможност на длъжностното лице по защита на данните да **следи отблизо законодателното и регулаторно развитие в областта на защитата на данните, сигурността на данните и т.н.**, за да предупреди съответното ръководство за предстоящите ***нови инструменти на ЕС*** (като например току що споменатия регламент за неприкосновеността на личния живот и електронните съобщения) или нови ***изпълнителни или съдебни решения на равнище ЕС*** (като всяко ново решение за „адекватност” на Европейската комисия, отнасящо се до трети държави, към които организацията на длъжностното лице по защита на данните предава данни или съответните решения на Съда на ЕС); ***нови насоки на равнище ЕС*** (по-специално всякакви становища или препоръки и т.н., издадени от ***Европейския комитет по защита на данните***); и ***подобни инструменти, решения, мерки или насоки, издадени от собствената държава*** (или държави) по установяване на ***длъжностното лице по защита на данните***. Общият регламент относно защитата на данните наистина **изисква** всеки администратор, който има длъжностно лице по защита на данните, да предостави на длъжностното лице по защита на данните „***[всички] ресурсите, необходими*** *за изпълнението на [неговите] задачи ... а така също* ***да поддържа неговите експертни знания***” (чл. 38, пар. 2). Поради това на длъжностното лице по защита на данните следва да бъде разрешено – и дори да бъде насърчено – да участва в съответните семинари, конференции и срещи, по-специално организирани от националния или регионалния държавен орган (или органи) по защита на данните.

Длъжностното лице по защита на данните **може също да предоставя консултации** на ръководството, представителния орган или синдикалната организация на персонала или всъщност на всеки член на персонала, включително, разбира се, по-специално всички „отговорници за дейност”/ лица в организацията със специфични отговорности за конкретна операция по обработване, когато това лице евентуално поиска съвет – и всъщност принципно **трябва да се обръщат към него за консултация** по съответните въпроси (вж. също задача 7).

Както Работната група по член 29 посочва в своите Насоки за длъжностните лица за защита на данните (след като бяха официално одобрени от Европейския комитет по защита на данните):[432]

Следователно организацията трябва да гарантира, например, че:

- Длъжностното лице по защита на данните се приканва да участва редовно в срещи на висшето и средното ръководство.
- Неговото или нейното присъствие се препоръчва, когато се вземат решения, които имат отношение към защитата на данните. Цялата съответна информация трябва своевременно да бъде предадена на длъжностното лице по защита на данните, за да му позволи да предоставя адекватни съвети.
- Становището на длъжностното лице по защита на данните трябва винаги да бъде надлежно отчетено. В случай на несъгласие, Работната група по член 29 препоръчва, като добра практика, да се документират причините, поради които не е последван съветът на длъжностното лице по защита на данните.
- След като е възникнало нарушение на сигурността на данните или друг инцидент, трябва незабавно да се направи консултация с длъжностното лице по защита на данните.

Когато е целесъобразно, администраторът или обработващият лични данни може да разработи насоки или програми за защита на данните, които посочват кога трябва да бъде извършена консултация с длъжностното лице по защита на данните.

- o – O – o -

[432] Насоки за длъжностните лица по защита на данните на Работната група по член 29 (бележка под линия 209, по-горе), стр. 13 – 14.

ЗАДАЧА 9: Подпомагане и насърчаване на „Защита на данните на етапа на проектирането и по подразбиране”

Както е отбелязано в Задача 6 по-горе, по принцип трябва да бъде провеждана консултация с длъжностно лице по защита на данните по всеки въпрос, свързан със защитата на данните, който възниква в рамките на неговата организация, включително при изготвянето на указания за общата политика и т.н.

Има обаче един въпрос, който е от особено значение в това отношение. Това е новото специално изискване на Общия регламент относно защитата на данните (което не е посочено в Директивата за защита на данните от 1995 г., въпреки че е било тълкувано в нея),[433] администраторите да включат принципа на „**защита на данните на етапа на проектирането и по подразбиране**” (което включва принципа на „***сигурност на етапа на проектирането [и по подразбиране]***”)[434] във всичките си дейности. Както е постановено в чл. 25:

Член 25

Защита на данните на етапа на проектирането и по подразбиране

1. Като взема предвид достиженията на техническия прогрес, разходите за прилагане и естеството, обхвата, контекста и целите на обработването, както и породените от обработването рискове с различна вероятност и тежест за правата и свободите на физическите лица, администраторът въвежда, както към момента на определянето на средствата за обработване, така и към момента на самото обработване, подходящи технически и организационни мерки (например псевдонимизация), които са разработени с оглед на ефективното прилагане на принципите за защита на данните (например свеждане на данните до минимум, и интегриране на необходимите гаранции в процеса на обработване, за да се спазят изискванията на настоящия регламент и да се осигури защита на правата на субектите на данни).
2. Администраторът въвежда подходящи технически и организационни мерки, за да се гарантира, че по подразбиране се обработват само лични данни, които са необходими за всяка конкретна цел на обработването. Това задължение се отнася до обема на събраните лични данни, степента на обработването, периода на съхраняването им и тяхната достъпност. По-специално, подобни мерки гарантират, че по подразбиране без намеса от страна на физическото лице личните данни не са достъпни за неограничен брой физически лица.
3. … [435]

---

433 Вж., например, многократното позоваване на принципа в Opinion 8/2014 on the on Recent Developments on the Internet of Things (Становище 8/2014 относно „Последните развития в интернет на нещата“) (WP223) на Работната група по член 29, прието на 16 септември 2014 г., на разположение на: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf

434 Вж. WP223 (предишната бележка под линия), стр.22, предпоследно тире.

435 Третият параграф предвижда, че: *„Одобреният механизъм за сертифициране съгласно член 42 може да се използва като елемент, за да се докаже спазването на изискванията, предвидени в параграфи 1 и 2 от настоящия член.”* Това се обсъжда във връзка със задача 9 по-долу.

Можем само накратко да обсъдим принципа тук. Европейският надзорен орган по защита на данните обобщава **общата концепция и нейната основа**, както следва:[436]

> Терминът „неприкосновеност на личния живот на етапа на проектирането" първоначално е използван от Ан Кавукян докато е била Комисар по информацията и неприкосновеността на личния живот на Онтарио, Канада. В нейната концепция, неприкосновеността на личния живот на етапа на проектирането може да бъде разбита на „**7 основни принципа**",[437] подчертавайки необходимостта от **проактивност** при разглеждането на идеята изискванията за неприкосновеност на личния живот [или казано на езика на ЕС: защита на данните] от фазата на проектиране през целия жизнен цикъл на данните, да бъдат *„вградени в дизайна и архитектурата на ИТ системите и бизнес практиките ... без да се намалява функционалността ..."*, където неприкосновеността на личния живот е настройката по подразбиране, цялостна сигурност, включително безопасно унищожаване на данните и висока прозрачност, подлежаща на независима проверка. Принципът на неприкосновеност по подразбиране беше извлечен като вторият от основополагащите принципи, установявайки, че неприкосновеността на личния живот на етапа на проектирането включва *„гарантиране, че личните данни са автоматично защитени във всяка дадена ИТ система или бизнес практика. Ако лицето не прави нищо, тяхната неприкосновеност остава непокътната. Не се изисква действие от страна на лицето за защита на неприкосновеността на личния му живот – **тя е включена в системата, по подразбиране***". Това твърдение е мощно оперативно определение на принципа на неприкосновеност на личния живот по подразбиране, където индивидът не носи тежестта на стремеж към защита при използване на услуга или продукт, но се ползва „автоматично" (няма нужда от активно поведение) от основното право на неприкосновеност на личния живот и защита на личните данни.

Според Европейския надзорен орган по защита на данните „защитата на данните на етапа на проектирането" има **няколко измерения**:[438]

- първото **измерение** е, че дейностите по обработване на лични данни следва винаги да са ***резултат от проект на дизайн***, обхващащ **целия**

---

[436] Европейски надзорен орган по защита на данните, Preliminary Opinion on privacy by design (Предварително становище относно неприкосновеността на личния живот на етапа на проектирането) (Становище 5/2018), издадено на 31 май 2018 г., стр.4, пар.17 (оригинален курсив), налично на: https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf (добавено подчертаване)
Следва да се отбележи, че Европейският надзорен орган по защита на данните разграничава по-широкия принцип на „неприкосновеност на личния живот на етапа на проектирането", който има „визионерско(напредничево) и етично измерение", от по-специфичните правни изисквания за „защита на данните на етапа на проектирането" и „защита на данните по подразбиране" на чл. 25 от Общия регламент относно защитата на данните: стр.1, пар.4.

[437] Вж.: "Седемте основополагащи принципа" са: 1. Проактивни, а не реактивни, превантивни, а не коректривни; 2. Поверителност като настройка по подразбиране; Поверителност, вградена в дизайна; 4. Пълна функционалност – положителна сума, а не нулева сума; 5. Цялостна защита – защита през целия жизнения цикъл; 6. Видимост и прозрачност – поддържайте ги отворени; 7. Уважение към личния живот на потребителя - запазете го за центриран върху потребителя. [оригинална бележка под линия] https://www.ipc.on.ca/wp-content/uploads/2018/01/pbd.pdf.

[438] За пълни подробности за тези измерения, както ги вижда Европейският надзорен орган по защита на данните, вж. неговото предварително становище 5/2018 (бележка под линия 401, по-горе), стр. 6 – 7 (параграфи 27 – 32).

жизнен цикъл на проекта, в рамките на който трябва ясно да се идентифицират рисковете и изискванията за защита на данните;

- **второто измерение** е, че проектът следва да се основава на **подход за управление на риска**, в рамките на който активите, които трябва да бъдат защитени, са ***лицата, чиито данни трябва да бъдат обработвани, и по-специално техните основни права и свободи***;
- **третото измерение** е, че мерките, които трябва да се предприемат за защита на тези лица, както и правата и свободите, трябва да бъдат ***подходящи и ефективни*** по отношение на тези рискове, разглеждани в светлината на принципите за защита на данните, изложени в чл. 5 от ОРЗД, които могат да се разглеждат като **цели, които трябва да се постигнат**;
- **четвъртото измерение** е задължението за ***интегриране на идентифицираните [необходими, подходящи и ефективни] гаранции в обработването***.

Той добавя че:[439]

> **Всичките четири измерения са еднакво важни и се превръщат в неразделна част от отчетността** и ще подлежат на надзор от компетентните надзорни органи по защита на данните, когато е уместно.

ЕНОЗД подчертава значението на защитата на данните на етапа на проектирането и по подразбиране във връзка с различни участници: администратори и обработващи лични данни като цяло;[440] разработчиците на (чувствителни към неприкосновеността на личния живот) продукти и технологии;[441] електронни съобщителни услуги;[442] Услуги за електронна идентичност;[443] доставчици на „интелигентни" измервателни уреди и мрежи. [444] По отношение на **публичните администрации** Европейският надзорен орган по защита на данните подчертава че: [445]

> Чл. 25 се прилага за всички видове организации, действащи като администратори, включително **публичните администрации**, които, като се има предвид тяхната роля да служат на общественото благо, **трябва да дават пример за защита на основните права и свободи на физическите лица**. ОРЗД подчертава ролята на защитата на данните на етапа на проектирането и по подразбиране, когато публичните администрации трябва да идентифицират своите доставчици на продукти и услуги в съображение 78, като посочва, че: „***Принципите на защита на данните на етапа на проектирането и по подразбиране следва да се вземат предвид и в контекста на процедурите за възлагане на обществени поръчки***". **Публичната администрация се призовава да застане начело при**

---

439 *Вж.*, стр.7, параграф 32, добавен подчертаване с удебелен шрифт.

440 *Вж*, стр.7, параграфи 35 – 36.

441 *Вж.*, стр.7, параграф 37.

442 *Вж.*, стр. 8 – 9, параграфи 42 – 44 (във връзка с директивата за правото на неприкосновеност на личния живот и електронни комуникации и предложения регламент за за неприкосновеността на личния живот и електронните съобщения).

443 *Вж.*, стр.9, параграф 45 (във връзка с регламента за eIDAS).

444 *Вж.*, стр. 9 – 10, параграфи 46 – 50 (с препратка към Smart Meter DPIA Template Recommendation (Препоръка за шаблон за ОВЗД на интелигентни измервателни уреди)).

445 *Вж.*, стр.8, параграф 38, оригинален курсив, добавено подчертаване в удебелен шрифт.

> **прилагането на тези принципи по отговорен начин, готова да демонстрира тяхното прилагане,** ако е необходимо, пред компетентния надзорен орган**.**

Препращането към **обществените поръчки** е особено важно: длъжностните лица по защита на данните следва да ***уведомят*** организацията си, че при обявяването на такива поръчки публичните администрации трябва изрично да търсят кандидати, които могат да „демонстрират", че техният продукт или услуга е в пълно съответствие с Общия регламент относно защитата на данните (и други съответни закони на ЕС и от националното законодателство в областта на защита на данните)[446] и които са включили „защита на данните на етапа на проектирането и по подразбиране" в съответния продукт или услуга. Действително следва да е възможно да се даде ***конкурентно предимство*** на такива кандидати пред кандидати с продукти или услуги, които не може да се докаже, че отговарят на тези изисквания.[447]

ЕНОЗД обсъжда надълго различните **методологии**, разработени за прилагане на защитата на данните на етапа на проектирането и по подразбиране. [448] Те не могат да бъдат изложени изцяло или дори перифразирани тук – но длъжностните лица по защита на данните, следва да се запознаят напълно с тях (всъщност по-подробно, отколкото е предвидено в документа на ЕНОЗД). Достатъчно е да се отбележи, че **Европейският надзорен орган по защита на данните правилно свързва неприкосновеността на личния живот на етапа на проектирането и по подразбиране с оценките на въздействието върху защитата на данните (ОВЗД),** както се обсъжда в Задача 4 по-горе);[449] и по-общо, че – както изрично подчертава Европейският надзорен орган по защита на данните:[450]

> **Ролята на неприкосновеността на личния живот и длъжностните лица за защита на данните е централна и тяхното участие е от решаващо значение за подход на неприкосновеност на личния живот на етапа на проектирането.** Те трябва да бъдат във веригата от ранните етапи, когато организациите планират системи за обработване на лични данни, така че да могат да подкрепят ръководителите, отговорниците за дейността и ИТ и технологичните отдели, както е необходимо. Уменията им следва да отговарят на тези изисквания.

Този „набор от умения" е необходимо да включва да бъдат **напълно образовани и обучени в съответните методологии** и технологии (ако е необходимо, чрез допълнително обучение на работното място) и да бъдат **ангажирани в дълбочина с проектирането, разработването, тестването и настройката на всички чувствителни към неприкосновеността на личния живот продукти, услуги и действия на тяхната организация** (включително провеждане на обществени поръчки, както току-що беше отбелязано) на всички етапи.

---

446 Виж обсъждането на принципа на отчетност в Част две, раздел 2.4, по-горе.

447 Този подход е изрично приет съгласно закона за защита на данните Шлезвиг-Холщайн.

448 ЕНОЗД, Предварително становище 5/2018 (бележка под линия 401, по-горе), стр.13 – 15, параграфи 63 – 72. Виж също конкретните препратки към програмата на САЩ на NIST за инженерни методи за осигуряване на неприкосновеността на личния живот и нейния доклад относно инженерните методи за осигуряване на неприкосновеността на личния живот и управлението на риска за федералните системи на САЩ (стр. 11, параграф 56, бележки под линия 76 и 74) и анализа на ENISA на ЕС за 2014 г. на (тогавашното) състояние на техниката (стр. 12, параграф 59, бележка под линия 82).

449 *Вж.*, стр.8, параграфи 39 – 40.

450 *Вж.*, стр.15, параграф 76, добавено подчертаване.

- o – O – o –

ЗАДАЧА 10: Съветване и извършване на мониторинг на спазването на политиките за защита на данните, на договори между съвместни администратори, между администратори и между администратор и обработващ лични данни, на Обвързващи корпоративни правила и клаузи за предаване на данни

За да спазят Общия регламент относно защитата на данните и особено с цел „демонстриране" на това съответствие, администраторите могат и следва да приемат или да подпишат редица мерки. Както е отбелязано в раздел 2.4.2 по-горе, те включват:

- изготвяне и официално приемане на вътрешни **политики за защита на данните** (вж. чл. 24, пар. 2) за регулиране на въпроси като:
  - ✓ **хартиените формуляри**, **уеб формулярите** и **декларациите за защита на данните/поверителността на уебсайтове** на организацията, използването на „**бисквитки**" и други следящи средства;
  - ✓ **дневници за достъп и промяна** и т.н. в съответния софтуер и хардуер;
  - ✓ издаването на „**пачове**" за собствения софтуер;
  - ✓ и така нататък;
- приемане на **административни споразумения („договорености")** между публични органи или структури, особено ако те могат да се считат за „**съвместни администратори**" по отношение на някои дейности по обработване;
- изготвяне и съгласуване на съответни **договори с други администратори и обработващи лични данни**; и;
- подписване или изготвяне на **стандартни или индивидуално одобрени договори за предаване на данни**.

Основният момент, който трябва да се подчертае отново тук е, че това са всички отговорности (средства да се „докаже спазване") на администратора, а не на длъжностното лице по защита на данните (вж. под-раздел *„Липсата на отговорност на длъжностното лице по защита на данните за съответствие с Общия регламент относно защитата на данните"* част две, раздел 2.5.4 по-горе).

На практика обаче длъжностното лице по защита на данните трябва отново да бъде тясно ангажирано с всички тези въпроси. Най-малкото, всяко ново ДЛЗД, и по-специално всяко едно ДЛЗД, назначено за организация, която преди това не е имала такова, трябва да **преразгледа** всички съществуващи документи и инструменти от този вид, за да провери дали те все още напълно отговарят на всички правни изисквания за защита на данните.

Въз основа на този преглед ДЛЗД следва да **препоръча промени в съществуващите документи и т.н**. – особено ако те са изготвени и приети преди приемането и влизането в сила на Общия регламент относно защитата на данните; и то следва да **препоръча изготвянето и приемането на такива документи** и т.н., когато (според него) следва да има такива документи и т.н., но такива липсват.

И след това на длъжностното лице по защита на данните се възлага официално **наблюдението** на съответствието с всички политики, договорености и договори, приети

или сключени от администратора във връзка с обработването на лични данни (вж. чл. 39, пар. 1, б. „б“).

ЗАДАЧА 11: Участие в кодекси за поведение и системи за сертифициране

В Част две, раздел 2.4.2, отбелязахме, че придържането към и пълното съответствие с одобрен **кодекс за поведение** или одобрена **схема за сертифициране за защита на данните,** би могло да служи и като важен елемент или средство за демонстриране на съответствие с Общия регламент относно защитата на данните във връзка с въпросите, обхванати в тези кодекси или схеми за сертифициране (без това да се равнява на правно доказателство за съответствие).

Отново, в крайна сметка администраторът – а не длъжностното лице по защита на данните – ще реши дали да подпише съответния код за сектора, в който извършва дейност организацията, или да се стреми да получи сертификат за защита на данните от вида, предвиден в регламента (вж. членове 40 – 43). Въпреки това е напълно приемливо ДЛЗД да **препоръча** такова действие.

Всъщност може да е доста уместно длъжностните лица по защита на данните на организациите, извършващи дейност в даден сектор, да бъдат включени в **изготвянето на кодекс(и) за поведение** за този сектор, въпреки че следва да се включват и правен консултант и членове на персонала на секторната организация, под чието крило е изготвен кодексът (включително, по-специално, персонала в областта на ИКТ, ако кодексът засяга технически въпроси като сигурност на ИКТ, криптиране и т.н.).

Длъжностното лице по защита на данните може също така да **съдейства за получаване на сертификат** от неговата организация, като помогне за събирането или предостави на въпросния Сертифициращ орган „цялата информация и достъп до своите дейности по обработване, които са необходими за извършване на процедурата по сертифициране" (чл. 42, пар. 6). Когато дадена схема за сертифициране се базира на **оценка** на дейностите по обработването на лични данни на администратора от един или повече ***независими експерти***, акредитирани от съответния сертифициращ орган (както е в настоящата схема в ЕС, схемата на *Европейския печат за поверителност [EuroPriSe]*),[451] длъжностното лице по защита на данните не може да действа в тази роля: това би представлявало конфликт на интереси.

Бележка: В известна степен подробният запис на оценките на въздействието върху защитата на данните (ОВЗД), описан в Задача 4 по-горе, и редовното наблюдение на дейностите, описано в Задача 5 по-горе (и регистъра на това наблюдение) изпълняват подобна функция на сертифицирането, тъй като показват, че администраторът и неговият персонал внимателно са прегледали последствията за неприкосновеността на личния живот/ защитата на данните от съответните дейности по обработване на лични данни; идентифицирали са и са определили количествено рисковете, свързани с основните права на засегнатите лица; и са приели подходящи смекчаващи мерки. Предимството на схемите за сертифициране пред това е, че оценката се извършва от външни независими експерти. Много ще зависи от качеството на акредитираните схеми за сертифициране и от това как длъжностното лице по защита на данните ще си съдейства със съответния орган по защита на данните при прилагането на правната рамка.

- o – O – o -

[451] Вж.: https://www.european-privacy-seal.eu/EPS-en/fact-sheet

Сътрудничество и консултиране с органа по защита на данните

ЗАДАЧА 12: Сътрудничество с органа по защита на данните

Длъжностното лице по защита на данните е натоварено със задачата да отговаря на искания на органа по защита на данните и в рамките на неговата компетентност да си сътрудничи с ОЗД по искане на последния или по своя собствена инициатива (чл. 39, пар. 1, б. „г“).

В тази връзка, Работната група по член 29 е заявила, че:[452]

> Тези задачи се отнасят до ролята на „посредник” на длъжностното лице по защита на данните, спомената във въведението към настоящите Насоки. ДЛЗД се явява свързващо звено, за да улеснява достъпа на надзорния орган до документите и информацията за изпълнението на задачите, посочени в чл. 57, както и за упражняването на неговите правомощия по разследване, коригиране, разрешаване и консултиране, споменати в чл. 58. Както вече беше споменато, ДЛЗД е обвързано от тайна или поверителност във връзка с изпълнението на своите задачи, в съответствие със законодателството на Съюза или на държавата членка (чл. 38, пар. 5). Задължението за пазене на тайна/ поверителност обаче не забранява на ДЛЗД да се свързва и да търси съвет от надзорния орган. Чл. 39, пар. 1, б. „д“ предвижда, че длъжностно лице по защита на данните може да се консултира с надзорния орган по всеки друг въпрос, когато е необходимо.

Европейският надзорен орган по защита на данните разшири допълнително еквивалентните задължения на длъжностните лица по защита на данните от институциите на ЕС в техните отношения с ЕНОЗД, както е посочено в цитатите по-долу с текстови изменения за съответно прилагане на думите на ЕНОЗД към взаимоотношенията между органите по защита на данните (ОЗД) на държавите членки (и Европейския комитет по защита на данните) и длъжностните лица по защита на данните, определени съгласно ОРЗД. На първо място, той отбелязва, най-общо, че:[453]

> Длъжностното лице по защита на данните е натоварено със задачата да отговори на исканията на [съответния орган по защита на данните] и в рамките на своята компетентност да си сътрудничи с [органа по защита на данните] по искане на последния или по своя инициатива. Тази задача подчертава факта, че ДЛЗД улеснява сътрудничеството между ОЗД и институцията, по-специално в рамките на разследвания, разглеждане на жалби или предварителни проверки. Длъжностното лице по защита на данните не само познава отвътре институцията, но също така е вероятно да знае кой е най-подходящият човек, с когото да се свърже в институцията. Възможно е също така ДЛЗД да е наясно и своевременно да информира [органа по защита на данните] за последните събития, които биха могли да повлияят на защитата на личните данни.

След това ЕНОЗД конкретизира това по отношение на различните въпроси по начин, който до голяма степен се отнася и до въпросите по Общия регламент относно защитата на данните, както следва:[454]

---

452 Работна група по член 29, Насоки за длъжностните лица по защита на данните (бележка под линия 209, по-горе), стр.18.

453 Европейски надзорен орган по защита на данните, Становище относно длъжностните лица по защита на данните (бележка под линия 210, по-горе), стр.6. Текстови промени в квадратни скоби.

454 *Вж.*, Част IV (стр. 10 – 11).

IV. Взаимоотношения между длъжностно лице по защита на данните и орган по защита на данните

Гарантирането на спазването на Регламента ще бъде повлияно от работните взаимоотношения между длъжностно лице по защита на данните и съответния ОЗД. ДЛЗД не трябва да се разглежда като агент на ОЗД, а като част от институцията/ органа, в която работи. Както вече споменахме, тази идея за близост го поставя в идеална ситуация, за да гарантира спазването отвътре и да съветва или да се намесва на ранен етап, като по този начин избягва възможна намеса от надзорния орган. В същото време ОЗД може да предложи ценна подкрепа на длъжностните лица за защита на данните при изпълнението на техните функции. [455]

Поради това от [органите по защита на данните може да се очаква да][456] подкрепят идеята за развитие на възможни взаимодействия между ДЛЗД и ОЗД, които биха допринесли за постигането на общата цел за ефективна защита на личните данните в рамките на институциите.....

IV. 1. Осигуряване на съответствие

Осигуряването на спазването на изискванията, най-вече започва, чрез повишаване на осведомеността. Както бе споменато по-горе, длъжностните лица по защита на данните играят важна роля за развитието на знания по въпросите на защитата на данните в рамките на институцията/ структурата. Може да се очаква, че [органите по защита на данните][457] приветстват това и неговите последици по отношение на стимулирането на ефективен превантивен подход, а не на репресивен надзор върху защитата на данните.

Освен това длъжностното лице по защита на данните предоставя съвет на институцията/ структурата относно практически препоръки за подобряване на защитата на данните в рамките на институцията/ органа или относно тълкуването или прилагането на [Общия регламент относно защитата на данните][458]. Тази консултативна функция се споделя с [органите по защита на данните], които съветват всички [техни национални] институции/структури по въпроси, свързани с обработването на лични данни (чл. 57, пар. 1, б. „в“ от ОРЗД). В тази област [националните органи по защита на данните и преди] често са били призовавани да съветват длъжностните лица по защита на данните по конкретни въпроси, свързани със защитата на данните (случай по случай). [Може да се очаква Органите

---

455 Вж. предоставянето от **френския** орган по защита на данните, CNIL, на специална „*extranet*“ за регистрирани ДЛЗД, достъпна само за тях с потребителско име и парола, която им предоставя правни текстове (закони, укази и т.н.) и обучение и информация, включително информация за нови доклади или насоки, издадени от CNIL, и за други правни и практически разработки и им позволява да обменят мнения и да водят дискусии. Виж под-раздел 2.3. 5 „Обучение и сертификация“ и бележка под линия 228, по-горе.

456 В оригиналното изречение се казва, че Европейският надзорен орган по защита на данните „подкрепя” идеята. От органа по защита на данните (и Европейският комитет по защита на данните) може да се очаква да имат същото мнение.

457 В първоначалното изречение се казва, че Европейският надзорен орган по защита на данните „приветства“ този подход, но (също и в светлината на минали практики) Органа по защита на данните (и Европейският комитет по защита на данните) отново могат да приемат същото мнение.

458 Препращането в документа на Европейският надзорен орган по защита на данните е към регламента за определяне на правилата за защита на данните за самите институции на ЕС (Регламент (ЕО) № 45/2001) (бележка под линия 207, по-горе), но същото е, разбира се, вярно по отношение на ОРЗД, що се отнася до ДЛЗД, назначени съгласно последния регламент. Направихме подобни замени на други места в цитата.

по защита на данните и Европейският комитет по защита на данните] да изготвят становища по определени теми, така че да дадат насоки на институциите/ структурите по някои по-общи теми.[459]

IV.2 Предварителни проверки

Становища, представени от орган по защита на данните в рамките на предварителната консултация по чл.36, пар.5 от ОРЗД и мнения, изразени от органи по защита на данните в процеса на издаване на предварителни разрешения, както е предвидено в чл. 36, пар.5 от ОРЗД, също са повод ОЗД да осъществява наблюдение и да осигурява спазването на ОРЗД. ...[460]

… Преди окончателното приемане на становище по предварителна проверка, [органът по защита на данните] [461] може да изпрати предварителен проект на ДЛЗД с информация за планираните препоръки, като по този начин се откриват възможности за дискусия относно ефективността и последствията от планираните препоръки. Може да се очаква органите по защита на данните да бъдат внимателни спрямо опасенията на институцията, изразени от ДЛЗД, така че да се работи за практически препоръки.

IV. 3. Прилагане

В областта на прилагането на конкретни мерки за защита на данните се появяват възможности за синергия между длъжностните лица по защита на данните и органите по защита на данните по отношение на приемането на санкции и разглеждането на жалби и запитвания.

Както вече беше споменато, ДЛЗД имат ограничени правомощия за прилагане. Органът по защита на данните ще допринесе за гарантиране на съответствието с ОРЗД, като предприема ефективни мерки в областта на предварителните [консултации или разрешения] и на жалбите и другите запитвания. Мерките са ефективни, ако са добре насочени и осъществими: длъжностното лице по защита

---

459 В оригиналното изречение се казва, че Европейският надзорен орган по защита на данните „възнамерява да изготви" становища и насоки. Отново може да се очаква, че националните органи по защита на данните и Европейският комитет по защита на данните ще направят същото във връзка с Общия регламент относно защитата на данните.
Изложеното изречение гласи: „По отношение на длъжностните лица по защита на данните, назначени в рамките на Общия регламент относно защитата на данните, националните Органи по защита на данните, но най-вече и новият Европейски комитет по защита на данните, без съмнение ще издаде подобни насоки".

460 Останалата част от този абзац, както и пропуснатото изречение в началото на следващия параграф, се отнасят до факта, че разликата във времето между влизането в сила на регламента и назначаването на Европейският надзорен орган по защита на данните създаде голям струпване на дела, които се подлагат последващо на „предварителна проверка". Все още не е ясно дали възникват подобни проблеми по Общия регламент относно защитата на данните. Ако е така, призивът на Европейският надзорен орган по защита на данните към длъжностните лице по защита на данните и регулатора да бъдат „стратегически партньори" при разрешаването на този въпрос също следва да бъде взет под внимание в този контекст.

461 Практиката по изпращане на „временни проекти на препоръки" на администратор в контекста на процес на „предварителна консултация"/„предварително одобрение" не е посочена в Общия регламент относно защитата на данните (или в Регламент 45/2001). Самият факт обаче, че ОРЗД споменава „предварителна консултация", категорично предполага, че съгласно този инструмент органите по защита на данните ще предприемат подобен подход; и това е отразено в текста в квадратни скоби, добавен два пъти към този параграф.

на данните може да се разглежда и като стратегически партньор при определянето на добре целенасочено прилагане на дадена мярка.

Разглеждането на жалби и запитвания от страна на ДЛЗД на местно равнище[462] трябва да се насърчава поне по отношение на първата фаза на разследване и решаване. Поради това [от органите по защита на данните може][463] да се очаква да са на мнение, че ДЛЗД следва да се опитват да разследват и вземат решение по жалби на местно равнище, преди да сезират органа по защита на данните. Освен това ДЛЗД следва също така ... да се консултира с органа по защита на данните, когато изпитва съмнения относно процедурата или съдържанието на жалбите. Това обаче не възпрепятства възможността субектът на данни да се обръща директно към ОЗД, съгласно чл. 77, пар. 1 от ОРЗД. Ограничените правомощия на ДЛЗД също така показват, че в някои случаи жалбата или запитването трябва да бъде препратена(о) до органа по защита на данните. Поради това ОЗД предоставя ценна подкрепа в областта на прилагането. На свой ред, длъжностното лице по защита на данните може да бъде търсено, за да предостави информация на органа по защита на данните и за да осигури последващо действие във връзка с приетите мерки.

IV.4. Измерване на ефективността[464]

Що се отнася до измерването на ефективността на прилагането на изискванията за защита на данните, ДЛЗД трябва да се разглежда като полезен партньор за оценка на напредъка в тази област. Например, когато става въпрос за измерване на изпълнението на вътрешния надзор на защитата на данните, може да се очаква органите по защита на данните да насърчават длъжностните лица по защита на данните да разработват свои собствени критерии за ефикасен надзор (професионални стандарти, специфични планове за институцията, годишна работна програма ...). Тези критерии на свой ред ще дадат възможност на органа по защита на данните, когато бъде поканен да направи това, да оцени работата на ДЛЗД, но също така ще му позволи да измери състоянието на изпълнение на Общия регламент относно защитата на данните в рамките на институцията/структурата.

Също е възможно длъжностни лица по защита на данните от публичния сектор да бъдат призовавани, за да участват в консултации, провеждани от органа по защита на данните и за да съдействат във формирането на официалното мнение на органа по защита на

---

462 Следва да се отбележи, че разглеждането на заявки и жалби от субекти на данни е допълнително разгледано в Задача 11, по-долу.

463 Първите две изречения в този параграф отново препращат към насърчаваната от Европейския надзорен орган по защита на данните практика – но е отново (също и с оглед на минали практики) напълно очаквано националните органи по защита на данните да предприемат същия подход.

464 Няма специфични изисквания, нито в Регламент (ЕО) № 45/2001 (по отношение на институциите на ЕС), нито в ОРЗД (по отношение на организациите, обхванати от този инструмент), за съответния регулатор (съответно, Европейският надзорен орган по защита на данните и националните органи по защита на данните) за „измерване на ефективността" на мерките, приети от администраторите с цел осигуряване на съответствие с приложимия инструмент. В институционалната рамка на ЕС обаче Европейският надзорен орган по защита на данните (с право) счита това за естествена част от работата му. Може да се очаква, че органите по защита на данните на държавите членки (и Европейският комитет по защита на данните) също ще „насърчават" ДЛЗД да допринасят за съответствие, на високо равнище, чрез приемането на или присъединяването към „професионални стандарти, специфични планове за институцията, годишна работна програма" и т.н.;.

данните по законови предложения или проекти в сферата на защитата на данните, които засягат контекста, в който работи длъжностното лице по защита на данните.

И накрая, следва да се отбележи, че **длъжностно лице по защита на данните играе важна роля в подпомагането на органа по защита на данните, при изпълнението от негова страна на проверки на място**, в случаите на консултации на ДЛЗД с администраторите в определени сектори, и т.н. Например, органите по защита на данните рядко извършват проверки без предизвестие – това наистина се прави само по отношение на лица, заподозрени в извършване на злоупотреби, които могат да скрият данни или други доказателства, ако са получили предварително предупреждение за проверка. На практика, органите по защита на данните обикновено предварително организират проверки с помощта на администратора, и по-специално длъжностното лице по защита на данните на администратора, който ще може да гарантира, че са налице правилните хора и правилните места и системи, които могат да бъдат инспектирани. Това често е от решаващо значение, особено във връзка със сложни системи за обработване, където за правилния преглед са необходими задълбочени познания за ИКТ архитектурата и вътрешните процеси. И когато органът по защита на данните иска да прегледа подробно обработването на лични данни в определен контекст или сектор – както повечето от тях правят съгласно годишен план и избор на приоритети – те ще се обърнат към длъжностните лица по защита на данни на администраторите, които са добре запознати със същността на дейността или сектора, като провеждат срещи с тях и съответно ще очакват отговори от консултациите. Това също е част от нещото, което Европейският надзорен орган по защита на данните нарича „стратегическо партньорство" между длъжностните лица по защита на данните и органите по защита на данните.

- o – O – o -

Разглеждане на молби на субекти на данни

ЗАДАЧА 13: Разглеждане на заявки и жалби на субекти на данни

Общият регламент относно защитата на данните предвижда че:

> Субектите на данни могат да се обръщат към длъжностното лице по защита на данните по всички въпроси, свързани с обработването на техните лични данни и с упражняването на техните права съгласно настоящия регламент.
>
> (чл. 38, пар.4)

Субектите на данни, които желаят да упражнят някое от своите **права на субекти на данни** – права за достъп, корекция и изтриване („право да бъдеш забравен"), ограничаване на обработването, преносимостта на данните, правото на възражение по принцип и във връзка с автоматизирано вземане на решения и профилиране – по отношение на дадена организация, или които имат **общи въпроси** или **жалби** във връзка със защитата на данните спрямо организацията, следва, да се обръщат първо към длъжностното лице по защита на данните на тази организация (където има такова).

Това се улеснява от изискването в Общия регламент относно защитата на данните информацията за контакт с длъжностното лице по защита на данните да бъде публикувана от организацията (чл. 37, пар. 7) и администраторът да гарантира, *„че длъжностното лице по защита на данните участва по подходящ начин и своевременно във всички въпроси, свързани със защитата на личните данни [във връзка с организацията]"* (чл. 38, пар. 1). (Поради това, ако даден субект на данни се обърне към някой друг в организацията, като например главния юрисконсулт или главния изпълнителен директор, те следва да предадат искането на длъжностното лице по защита на данните.)

Освен това независимият статут на длъжностното лице по защита на данните (чл. 38, пар. 3) следва да гарантира, че искането, запитването или жалбата се разглеждат от длъжностното лице по защита на данните – или от отговорните служители под надзора на длъжностното лице по защита на данните – **по подходящ начин, без пристрастия в полза на организацията или срещу субекта на данни**. Във всеки случай, ДЛЗД следва или да напише лично или да прегледа отговора към субекта на данни. Това следва да включва съвет, че ако субектът на данни не е удовлетворен от отговора, може да отнесе въпроса към органа по защита на данните.

Това е така, защото във всеки случай правото на субектите на данни да подават молби, запитвания и жалби до организацията (т.е. до длъжностното лице по защита на данните на организацията) не **отменя правото им да подадат жалба до органа по защита на данните**. По-конкретно, всеки орган по защита на данните е задължен и опълномощен на своята собствена територия, да:

> разглежда жалбите, подадени от субект на данни ... и разследва предмета на жалбата, доколкото това е целесъобразно, и информира жалбоподателя за напредъка и резултатите от разследването …
>
> (чл. 57, пар. 1, б. „е")

При такива жалби до органа по защита на данните, субектите на данни могат да бъдат представлявани от съответна структура с нестопанска цел (чл. 80), като горепосоченото

задължение и правомощие на ОЗД да разглежда такива жалби се простира спрямо случаи, заведени по този начин (вж. чл. 57, пар. 1, б. „е“).

В този смисъл би имало смисъл длъжностните лица по защита на данните да са склонни и да приемат молби и **жалби от такива представителни организации**, а не само от субекти на данни.

Както вече беше отбелязано във връзка със Задача 10 (*Сътрудничество с органа по защита на данните*), трябва да се очаква (също и в светлината на миналата практика), че националните органи по защита на данните (като Европейският надзорен орган по защита на данните по отношение на длъжностните лица по защита на данните на институциите на ЕС) ще насърчат субектите на данни (и тези организации) винаги да се заемат първо, с които и да е въпроси заедно с администратора, и по-специално с длъжностното лице по защита на данните на администратора, за да проверят дали въпросите не може вече да бъде задоволително разследвани и разрешени при такива взаимодействия, без да се включва органът по защита на данните, при условие че ДЛЗД следва да се консултира с органа по защита на данните, ако възникнат въпроси относно принципното тълкуване и прилагане на Общия регламент относно защитата на данните. Но не следва да се стига до възпрепятване на субектите на данните (или представителните организации) да повдига(т) въпроси – и разбира се, особено принципни въпроси – пред органа по защита на данните.

Както посочва Европейският надзорен орган по защита на данните, регулаторният орган и длъжностните лица по защита на данните са в „стратегическо партньорство”: ОЗД могат да насърчат субектите на данните на първо място и преди всичко да разрешат всички въпроси, директно с длъжностните лица по защита на данните; и ДЛЗД трябва да могат – и се изисква от тях – да работят с регулатора, за да се гарантира, че отговорите на въпроси и жалби са надлежно разгледани и ако е необходимо да се предизвикат промени в практиките на съответния администратор. Органите по защита на данните трябва да могат да разчитат на длъжностните лица по защита на данните, за да подкрепят истински субектите на данните при всяка жалба; и ДЛЗД трябва да могат да разчитат на органите за защита на данните, за да гарантират, че препоръките за промяна действително се прилагат.

Това засилва деликатността на позицията на длъжностното лице по защита на данните, обсъдена в Част две, раздел 2.5: ДЛЗД са мост между администратора и регулатора – и (за да смесим малко метафорите, освен ако някой разбира „мост” като „проход”) не трябва да се допуска да попадат между кораба и кея.

- 0 – O – o -

Информация и повишаване на осведомеността

ЗАДАЧА 14: Вътрешни и външни задачи за информиране и повишаване на осведомеността

Общият регламент относно защитата на данните предвижда, че задачите на длъжностното лице по защита на данните включват „най-малко”:

> информира[не] и съветва[не на] администратора или обработващия лични данни и служителите, които извършват обработване, за техните задължения по силата на настоящия регламент и на други разпоредби за защитата на данни на равнище Съюз или държава членка
>
> (чл. 39, пар. 1, б.„а“)

Вътрешно (в рамките на организацията, в която работи длъжностно лице по защита на данните), това предполага, от една страна, ДЛЗД да **информира** членовете на персонала за техните права и, от друга страна, длъжностното лице по защита на данните да **инструктира** администраторите и организацията и членовете на персонала – включително, в частност, „отговорниците за дейността“/лицата, отговорни за конкретна операция – за техните задължения и отговорности и да ги **обучава** как да ги изпълняват.

Както ЕНОЗД посочва във вече цитиран по-горе пасаж:[465]

> Осигуряването на спазването на изискванията най-вече започва чрез повишаване на осведомеността. ... длъжностните лица по защита на данните играят важна роля за развитието на знания по въпросите отнасящи се до защитата на данните в рамките на институцията/структурата.

Повишаването на осведомеността „стимулира ефективния превантивен подход, а не репресивния надзор на защитата на данните”.[466]

Мерките, приети от ДЛЗД по отношение на тези цели, могат да включват издаване на **информационни бележки за персонала**, организиране на вътрешни **обучителни сесии** за защита на данните, които следва да имат за цел да създадат у персонала информираност и усет към защитата на данните и правата на субектите на данни – „рефлекс за защита на данните” – във всичките им различни роли в обществото, било то като обикновен гражданин, работник, ръководител на екип или висш ръководител.

Също така, създаването на **вътрешен уеб портал/сайт** информиращ и обучаващ по теми, свързани със защитата на данните, както и изготвянето и публикуването на **декларации за поверителност** на уебсайтове и страници за персонала.[467]

Външно, освен да гарантира, че субектите на данни разполагат с актуална информация, когато първоначално се събират данни за тях (както е предвидено в членове 12 – 14 от Общия регламент относно защитата на данните), напр. в ясни уведомления на уебсайта, длъжностното лице по защита на данните следва да работи и с всички служители в сферата на връзките с обществеността, за да осигури **пълна прозрачност относно дейностите по обработване на лични данни на организацията**: относно целите, за

---

465 ЕНОЗД, Становище относно длъжностните лица по защита на данните paper (бележка под линия 209, по-горе), стр.10.

466 *Вж*.

467 *Вж.*, стр.5.

които събира и обработва лични данни; включените категории субекти на данни и данни; получателите на данните; дали данните се предават на трети държави (извън ЕС/ЕИЗ); и т.н.

Общият регламент относно защитата на данните не изисква администраторите да предоставят изцяло на обществеността регистъра на техните дейности по обработване на лични данни.[468] Със сигурност обаче Общият регламент относно защитата на данните не го и забранява.

Европейският надзорен орган по защита на данните изразява силна подкрепа за публикуването във връзка с институциите на ЕС, по-специално относно факта, че (подобно на Директивата за защита на данните от 1995 г.) се изисквано от тях да публикуват своите „функционално еквивалентни" данни от уведомление:[469]

> Записите са важен инструмент за проверка и документиране на това, че Вашата организация контролира своите дейности по обработване. ….
>
> **Европейският надзорен орган по защита на данните настоятелно препоръчва [институциите на ЕС] да направят записите публично достъпни, за предпочитане чрез публикуване в интернет … .**
>
> Има много причини, поради които регистърът на записите трябва да бъде публичен:
>
> - това допринася за прозрачността на EUIs 12;
> - това спомага за укрепване на общественото доверие
> - това улеснява обмена на знания между институциите на ЕС;
> - ако не се публикува, би било крачка назад в сравнение със старите [правила].

Като цяло същото може да се каже и във връзка с регистъра на дейностите по обработване, който трябва да се поддържа от администраторите съгласно Общия регламент относно защитата на данните – най-малкото когато става дума за публични органи. Някои държави членки могат да наложат в националното си законодателство такова задължение за публикуване на данните от регистъра; но публичните органи в държавите, където това не е задължително, трябва винаги да обмислят възможността да го направят в светлината на наблюденията на Европейския надзорен орган по защита на данните.

Разбира се, администраторите и обработващите лични данни не следва да се чувстват задължени да публикуват информация за своите мерки за сигурност, която би могла да бъде използвана за пробив в тази сигурност (това вече беше признато в разпоредбата от Директивата за защита на данните от 1995 г. относно публикуването на подробности за дейностите по обработване, които са били съобщени на органите по защита на данните).[470]

---

[468] За разлика от това, Директивата за защита на данните от 1995 г. изискваше от органите по защита на данните да предоставят на обществеността подробностите за дейностите по обработване, които са им съобщени (Член 21).

[469] Европейски надзорен орган по защита на данните, Отчетност на място (бележка под линия 267, по-горе), стр.8, оригинално подчертаване.

[470] Вж. чл. 21 от Директивата за защита на данните от 1995 г., който изключва информацията, посочена в чл.19, пар. 1, б. „е" – т.е., общо описание на мерките за сигурност на администратора – от

Във всеки случай, основната информация за дейностите по обработване на лични данни на организацията, следва да бъде лесно достъпна на **уебсайта** на организацията, както и предоставена в **брошури** и **формуляри** (включително версии, достъпни за лица с увреждания).

Уебсайтът и тези формуляри е необходимо, ясно да предоставят информация за това **как субектът на данни може да упражнява правата си** (включително публично уведомление с **данните за контакт на длъжностното лице по защита на данните** – въпреки че не е необходимо да включва име); какви **кодекси на поведение** е подписала организацията и какви **сертификати** е получила (тези въпроси могат да бъдат показани чрез признати **лога** или **печати**); и т.н.

Разбира се, всеки уебсайт трябва също така, изцяло да отговаря на изискванията на правото на ЕС в областта на защитата на данните и на всяко друго съответно бъдещо национално законодателство по въпроси като „**бисквитки**“ и други **средства за проследяване** и т.н.

Задача 15: Планиране и преглед на дейностите на длъжностното лице по защита на данните

И накрая, като се имат предвид големият брой и обхват на задачите на длъжностното лице по защита на данните, то трябва да изготвя годишен план на дейностите си като се съобразява с необходимото време за тяхното изпълнение и с предвидимото развитие на нови аспекти от дейността по защита на данните, както и с предвиждането на време за непредвидими събития. Длъжностното лице по защита на данните трябва редовно да преработва и актуализира плана.

- o – O – o -

Дау Корф & Мари Жорж
Кеймбридж/Париж, декември 2018 г.

информацията, която трябва да бъде направена публично достъпна. Следва обаче да се отбележи, че вярата в „сигурността чрез неяснота” отдавна е била дискредитирана, вж.: https://en.wikipedia.org/wiki/Security_through_obscurity