Комисия за Защита на Личните Данни

ИНФОРМАЦИОНЕН БЮЛЕТИН

брой 3 (72), май 2018 г.

ТЕМИТЕ В БРОЯ

ЗАПОЧВА ПРИЛАГАНЕТО НА ОБЩИЯ РЕГЛАМЕНТ ЗА ЗАЩИТА НА ДАННИТЕ

"ПО-СИЛНА ЗАЩИТА, НОВИ ВЪЗМОЖНОСТИ" - НАСОКИ НА ЕВРОПЕЙСКАТА КОМИСИЯ ОТНОСНО ПРИЛАГАНЕТО НА ОБЩИЯ РЕГЛАМЕНТ

На 25 май 2018 г. в Европейския съюз започва прилагането на нов единен набор от правила за защита на личните данни. Новата правна рамка е възможност за ЕС да се превърне в световен лидер в тази област. В условията на бързоразвиваща се цифрова икономика, Европейският съюз, неговите граждани и предприятия, трябва да разполагат с всичко необходимо, за да извлекат ползите и да разбират потенциалните последици от икономиката, основана на данни. Предприятията, особено по-малките, ще могат да се възползват от благоприятен за иновациите единен набор от правила, да го използват като свое конкурентно предимство и да въведат ред в собствените си дела по отношение на личните данни с цел спечелване доверието на потребителите. Гражданите ще могат да се възползват от по-добра защита на личните им данни и да придобият по-добър контрол върху начина, по който дружествата боравят с тях.

На 6 април 2016 г. ЕС постигна съгласие за осъществяването на голяма реформа в областта на защитата на данните, като прие пакета за реформа на защитата на данните, включващ Общия регламент за защитата на данните (който заменя двадесетгодишната Директива 95/46/ЕО) и Директивата за полицейското сътрудничество.

На 25 май 2018 г. Общият регламент за защита на данните, ще започне да се прилага пряко, две години след неговото приемане и влизането му в сила. Като осигурява единен набор от правила, пряко приложими в държавите членки на ЕС, той ще гарантира свободното движение на лични данни между тези държави и ще укрепи доверието и сигурността на потребителите, два абсолютно необходими елемента за създаването на истински цифров единен пазар. По този начин регламентът ще открие нови възможности за бизнеса и предприятията, особено за по-малките от тях.

Макар че новият регламент предвижда единен набор от правила, които ще се прилагат пряко във всички държави членки, в някои отношения е необходимо да се направят съществени корекции, например правителствата на страните от ЕС да внесат изменения в действащото законодателство. Държавите членки трябва да приемат по-скоро законодателните мерки на национално равнище и да се уверят, че тези мерки са в съответствие с регламента. Те трябва също така да осигурят на националните си органи необходимите финансови и човешки ресурси, за да се гарантират тяхната независимост и ефикасност.

През последните две години всички заинтересовани страни – от националните администрации и националните органи по защита на данните до администраторите на данни и обработващите лични данни, участваха в редица дейности, за да се гарантира, че значението и мащабът на промените, въведени с новата рамка за защита на данните, са добре разбрани и всички участници са готови за нейното прилагане.

С наслов „По-силна защита, нови възможности", на 24 януари 2018 г. Европейската комисия публикува насоки относно прякото прилагане на Общия регламент, считано от 25 май 2018 г. Комисията прави преглед на подготвителната работа, извършена до момента на ниво ЕС и посочва какво още трябва да се направи от Европейската комисия, националните органи за защита на данните

и националните администрации за успешното приключване на подготовката. Направено е резюме на основните нововъведения и възможности, които се откриват благодарение на новото европейско законодателство за защита на данните, а именно:

• Хармонизирана правна рамка, която ще доведе до еднакво прилагане на правилата в полза на единния цифров пазар на ЕС.

• Равнопоставени условия за всички дружества, осъществяващи дейност на пазара на ЕС.

• Принципите на защита на данните по замисъл и подразбиране

• Засилени права на физическите лица;

• Повече контрол върху личните данни на физическите лица.

• По-силна защита срещу нарушенията на сигурността на личните данни.

• В регламента на всички органи по защита на данните се предоставя правомощието да налагат глоби на администраторите и обработващите лични данни.

• Повече гъвкавост за администраторите на данни и обработващите лични данни поради недвусмислените разпоредби относно отговорността (принципа на отчетност).

• Повече яснота относно задълженията на обработващите лични данни и отговорността на администраторите, когато избират обработващ лични данни;

• Модерна система на управление, за да се гарантира, че правилата се прилагат по-последователно и категорично.

• Защитата на личните данни, гарантирана от регламента, съпътства данните при предаването им извън ЕС и осигурява висока степен на защита.

В насоките на Комисията се посочва, че по отношение засилване правата на физическите лица „регламентът въвежда нови изисквания за прозрачност; засилени права на информация, достъп и изтриване (право „да бъдеш забравен“); мълчанието или липсата на действие вече няма да се разглеждат като валидно съгласие и ще се изисква ясно утвърдително действие за изразяване на съгласие; онлайн защита на децата.“

Посочва се също, че по отношение на администраторите и обработващите лични данни „регламентът се отклонява от система на уведомяване и дава предпочитание на принципа на отчетност. Принципът на отчетност се осъществява на практика чрез задължения, които варират в зависимост от риска (например наличието на длъжностно лице за защита на данните или задължението за провеждане на оценки на въздействието върху защитата на данните). Въвежда се нов инструмент, който да помогне при оценяването на риска преди започването на обработката: оценка на въздействието върху защитата на данните. Оценката се изисква винаги, когато има вероятност обработването на данни да доведе до висок риск за правата и свободите на физическите лица. В този смисъл в регламента изрично са посочени три ситуации: когато дадено дружество оценява систематично и подробно личните аспекти на физическо лице (включително профилиране), когато обработва чувствителни данни в голям мащаб или системно осъществява мониторинг на обществени места в голям мащаб.“

В насоките се посочва, че „регламентът засяга най-силно операторите, чиято основна дейност е обработването на данни и/или боравенето с чувствителни данни. Той също така засяга операторите, които редовно и систематично наблюдават физически лица в голям мащаб. Тези оператори най-вероятно ще трябва да назначат длъжностно лице за защита на данните, да извършват оценка на въздействието върху защитата на данните и да уведомяват за нарушения на сигурността на данните, ако има риск за правата и свободите на физическите лица. За разлика от това, оператори, по-специално малките

и средни предприятия, които не се занимават с високорискова обработка като своя основна дейност, обикновено не подлежат на тези специфични задължения по регламента. ... За администраторите и обработващите лични данни е важно да предприемат задълбочен преглед на своята политика относно данните, така че ясно да се определят данните, които те притежават, с каква цел и на какво правно основание. Те също така трябва да направят оценка на действащите договори, по-конкретно тези между администраторите и обработващите лични данни, възможностите за международно предаване на данни и общото управление (какви информационни технологии и организационни мерки да се въведат), включително назначаването на длъжностно лице за защита на данните. .... Предприятията и другите организации, обработващи данни, също така ще могат да се възползват от новите инструменти, предвидени в регламента, като елемент за доказване на съответствието, например кодекси за поведение и механизми за сертифициране. Регламентът предвижда опростен набор от правила за такива механизми, като се вземат предвид пазарните реалности (напр. удостоверяване от сертифициращ орган или от орган за защита на данните).“

Успешното прилагане на регламента изисква сътрудничество между всички участници в областта на защитата на личните данни. В отделните държави членки подготовката се осъществява с различни темпове. Проучванията показват, че ползите и възможностите, които предлагат новите правила, не се познават навсякъде в еднаква степен. Необходимо е да се повиши осведомеността и да се подпомогнат усилията, които полагат малките и средни предприятия, за да спазят изискванията.

От 25 май 2018 г. нататък Европейската комисия ще следи как държавите членки прилагат новите правила и ще предприема съответните действия. Една година след влизането в сила на регламента (т.е. през 2019 г.) Комисията ще обобщи натрупания в прилагането на регламента опит. Направените констатации ще бъдат включени и в доклад за оценка и преглед на регламента, който Комисията трябва да представи до май 2020 г.

Пълният текст на насоките на Европейската комисия е публикуван ТУК.

ИНФОРМАЦИОННО-РАЗЯСНИТЕЛНА ДЕЙНОСТ НА ЕВРОПЕЙСКАТА КОМИСИЯ. ПРАВИЛА ЗА ДРУЖЕСТВАТА И ОРГАНИЗАЦИИТЕ.“

С убеждението, че успехът на Общия регламент за защита на данните се основава на добрата осведоменост на всички страни, засегнати от новите правила (бизнес средите и другите организации, обработващи данни, публичния сектор и гражданите) Европейската комисия предприе редица информационно-разяснителни дейности, свързани с подготовката за прилагането на регламента.

На 24 януари 2018 г. Европейската Комисия стартира онлайн инструмент с практическа насоченост, който да помага на предприятията, в частност малките и средни предприятия (МСП) и организациите да спазват новите правила за защита на данните и да се възползват от тях.

В настоящия брой публикуваме съдържанието на инструмента „**Правила за дружествата и организациите**“. В него Европейската комисия уточнява, че публикуваните информация и насоки са „*само средство за ориентиране - само текстът на Общия регламент относно защитата на данните (ОРЗД) има правна сила. Следователно само ОРЗД може да създава права и задължения за физическите лица. Тези насоки не пораждат никакви права или очаквания, подлежащи на изпълнение.*

Обвързващото тълкуване на законодателството на ЕС е от изключителната компетентност на Съда на Европейския съюз. Гледните точки, изразени в настоящите насоки, не изключват позицията, която може да заеме Комисията пред Съда. Нито Европейската комисия, нито лице, действащо от името на Европейската комисия, носи отговорност за използването на следната информация. Тъй като тези насоки отразяват състоянието на техниката в момента на изготвянето им, те следва да се разглеждат като „жив инструмент“, отворен за усъвършенстване, и съдържанието им може да бъде предмет на изменения без предизвестие.“

Този инструмент е достъпен онлайн ТУК.

ПРАВИЛА ЗА ДРУЖЕСТВАТА И ОРГАНИЗАЦИИТЕ

Научете какво трябва да направи организацията ви, за да спазва правилата на ЕС за защита на данните, както и как можете да помогнете на гражданите да упражняват правата си съгласно регламента.

1. ПРИЛАГАНЕ НА РЕГЛАМЕНТА

1.1. За кого се прилага законът за защита на данните?

Отговор

ОРЗД се прилага по отношение на:

• дружество или организация, което/която обработва лични данни като част от дейностите на един от своите клонове, установени в ЕС, независимо от това къде се обработват данните; или

• дружество, установено извън ЕС и което предлага стоки/услуги (платени или безплатни) или наблюдава поведението на физически лица в ЕС.

Ако Вашето дружество е малко или средно предприятие (МСП), което обработва лични данни, както е описано по-горе, трябва да спазвате ОРЗД. Ако обаче обработката на лични данни не е основна част от вашия бизнес и вашата дейност не създава рискове за физическите лица, някои задължения на ОРЗД няма да се отнасят за вас (напр. назначаването на служител по защита на данните (СЗД)). Имайте предвид, че „основните дейности“ трябва да включват дейности, при които обработването на данни представлява неразделна част от дейностите на администратора или обработващия данни

Примери:

Кога се прилага регламентът:

Вашето дружество е малко дружество за висше образование, работещо онлайн, със седалище извън ЕС. Неговата дейност е насочена предимно към университети в ЕС с обучение по испански и португалски език. Вашето дружество предлага безплатни съвети за редица университетски курсове и студентите имат нужда от потребителско име и парола за достъп до вашия онлайн материал. Вие предоставяте горепосочените потребителско име и парола, след като студентите попълнят формуляр за записване.

Кога не се прилага регламентът:

Вашето дружество е доставчик на услуги, базиран извън ЕС. То предоставя услуги на клиенти извън ЕС. Неговите клиенти могат да използват услугите му, когато пътуват до други страни, включително в рамките на ЕС. При условие че Вашето дружество не насочва специално услугите си към лица в ЕС, то не е обект на уредбата на правилата на ОРЗД.

1.2. Правилата важат ли за МСП?

Отговор

Да, **прилагането на регламента за защита на данните не зависи от размера на вашето дружество/организация, а от характера на вашите дейности.** Дейностите, които представляват висок риск за правата и свободите на физическите лица, независимо дали те се извършват от МСП или голяма корпорация, задействат прилагането на по-строги правила. Някои от задълженията на ОРЗД обаче може да не се прилагат за всички МСП.

Например дружествата с **по-малко от 250 служители не е необходимо да поддържат документация** за дейностите по обработване, освен ако обработването на лични данни не е редовна дейност, не представлява заплаха за правата и свободите на физическите лица или не засяга чувствителни данни или съдебни досиета.

Също така МСП ще трябва да назначат **служител по защита на данните** само ако основната им дейност е обработване на данни и представлява конкретна заплаха за правата и свободите на физическите лица (например наблюдение на физически лица или обработване на чувствителни данни или съдебни досиета), по-специално защото се прави в голям мащаб.

1.3. Правилата за защита на данните важат ли за данните за дружество?

Отговор

Не, правилата важат само за лични данни за физически лица, не се отнасят до данни за дружества или други юридически лица. Въпреки това, информацията във връзка с еднолични дружества може да представлява лични данни, когато позволява идентифицирането на физическо лице. Правилата важат и за всички лични данни, свързани с физически лица в хода на професионалната дейност, като служителите на дружеството/организацията, служебни имейл адреси „име.фамилия@дружество.eu“ или служебни телефонни номера на служителите.

Позовавания

- членове 1, 2 и 3; съображения (13), (14), (15), (18), (19) и (21) от ОРЗД;
- вж. Решение на Съда от 9 март 2017 г. по дело C-398/15, *Manni,* ECLI:EU:C:2017:197;

2. ПРИНЦИПИ НА ОРЗД

2.1. Какви данни можем да обработваме и при какви условия?

Отговор

Видът и количеството лични данни, които дадена организация/дружество може да обработва, зависят от причината за обработването им (използвана правна причина), и от целената употреба. Организацията/дружеството трябва да спазва няколко основни правила, включително:

- личните данни трябва да се обработват **законосъобразно и по прозрачен начин**, като се гарантира добросъвестност по отношение на физическите лица, чиито лични данни се обработват („законосъобразност, добросъвестност и прозрачност“);
- трябва да бъдат налице **конкретни цели** за обработването на данните и организацията/дружеството трябва да посочи тези цели на физическите лица, когато събирате техните лични данни. Организация/дружество не можете просто да събира лични данни за неопределени цели („ограничение на целите“);
- организацията/дружеството трябва да събира и обработва **само личните данни, които са необходими за постигането на тази цел** („свеждане на данните до минимум“);

• организацията/дружеството трябва да бъде сигурна/-о, че личните данни са точни и актуални, като се имат предвид целите, за които те се обработват, а в случай че не е, да ги коригира („точност“);

• организацията/дружеството не може да използва по-нататък личните данни за други цели, които не са **съвместими** с първоначалната цел на събирането;

• организацията/дружеството трябва да бъде сигурна/-о, че личните данни **се съхраняват не повече от необходимото** за целите, за които са били събрани („ограничение на съхранението“);

• организацията/дружеството трябва да въведе подходящи **технически и организационни предпазни мерки**, които гарантират сигурността на личните данни, включително защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане, като се прилага подходяща технология („цялостност и поверителност“).

Пример

Вашето дружество/организация управлява туристическа агенция. Когато получавате личните данни на клиентите си, трябва да обясните с ясни и недвусмислени формулировки защо имате нужда от данните, как ще ги използвате и колко дълго искате да ги запазите. Обработването трябва да бъде съобразено с основните принципи за защита на данните.

Позовавания

• член 5, параграф 1 и съображение (39) от ОРЗД;

• Становище 03/2013 на работната група по член 29 относно ограничението на целите (WP 203).

2.2. Цел на обработването на данни

2.2.1 Може ли личните данни да бъдат обработвани за всякакви цели?

Отговор

Не. Трябва да знаете за каква цел искате да обработвате лични данни и да информирате физическите лица, чиито данни обработвате. Не можете просто да посочите, че ще бъдат събирани и обработвани лични данни. Това е известно като принципа на „ограничение на целите“.

2.2.2. Може ли данните да бъдат използвани за друга цел?

Отговор

Да, но само в някои случаи. Ако Вашето дружество/организация е събрало/-а данни въз основа на **законен интерес, договор** или **жизненоважни интереси**, можете да ги използвате за друга цел, но само след като проверите дали **новата цел е съвместима с първоначалната цел.**

Трябва да се обърне внимание на следното:

• връзката между първоначалната цел и новата/бъдещата цел;

• контекста, в който са събрани данните (каква е връзката между Вашето дружество/организация и физическото лице);

• вида и естеството на данните (чувствителни ли са);

• възможните последици от планираната по-нататъшна обработка (как ще се отрази на физическото лице?);

• наличието на подходящи предпазни мерки (като криптиране или псевдонимизиране).

Ако Вашето дружество/организация иска да използвате данните за статистика или за научни изследвания, не е необходимо да провеждате теста за съвместимост.

Ако Вашето дружество/организация е събрало данните въз основа на **съгласие или законово изискване**, не е възможно извършване на по-нататъшна обработка извън областите, обхванати от първоначалното съгласие или разпоредбата на закона. По-нататъшната обработка изисква ново съгласие или ново правно основание.

Примери

По-нататъшната обработка е възможна

Банка има договор с клиент да предостави на клиента банкова сметка и личен заем. В края на първата година банката използва личните данни на клиента, за да провери дали има право на по-добър тип заем и спестовна схема. Тя информира клиента. Банката може отново да обработва данните на клиента, тъй като новите цели са съвместими с първоначалните цели.

По-нататъшната обработка не е възможна

Същата банка иска да сподели данните на клиента със застрахователни компании въз основа на същия договор за банкова сметка и личен заем. Това обработване не е разрешено без изричното съгласие на клиента, тъй като целта не е съвместима с първоначалната цел, за която са обработени данните.

Позовавания

• член 5, параграф 1, буква б), член 6, параграф 4 и член 89, параграф 1; съображения (39) и (50) от ОЗДР;

• Становище 03/2013 на работната група по член 29 относно ограничението, 2 април 2013 г. (WP 203).

2.3. Колко данни може да бъдат събрани?

Отговор

Личните данни трябва да се обработват само когато не е разумно да се извърши обработването им по друг начин. Когато е възможно, предпочита се да се използват анонимни данни. Когато са необходими лични данни, те трябва да са подходящи, свързани със и ограничени до необходимото във връзка с целите, за които се обработват („свеждане на данните до минимум“). Отговорността на Вашето дружество/организация като администратор е да се прецени колко данни са необходими и да гарантирате, че не се събират неподходящи даннПример

Вашето дружество/организация предлага услуги за споделяне на автомобили за физически лица. За тези услуги може да поискате името, адреса и номера на кредитната карта на клиентите и евентуално дори информация за това дали лицето има увреждане (т.е. данни за здравословното състояние), но не и за техния расов произход.

Позовавания

• член 5, параграф 1, буква в); съображение (39) от ОРЗД.

2.4. Колко дълго може да се съхраняват данните и трябва ли да бъдат актуализирани?

Отговор

Данните трябва да се съхраняват за **възможно най-кратко време.** Този период разбира се трябва да бъде съобразен с причините, поради които Вашето дружество/организация трябва да обработва данните, както и с всички законови задължения за съхранение на данните за определен период от време (напр. национални трудови и данъчни закони или закони за борба с измамите, които изискват

от вас да съхранявате личните данни на вашите служители за определен период, продължителност на гаранцията на продукта и др.).

Вашето дружество/организация трябва да определи **срокове** за **изтриване или преглед** на съхранените данни.

По изключение личните данни могат да се съхраняват за по-дълъг период от време за целите на архивирането от обществен интерес или научни или исторически изследвания, при условие че се предприемат подходящи технически и организационни мерки (като анонимност, криптиране и т.н.).

Също така Вашето дружество/организация трябва да бъде сигурно/-а, че данните, които съхранява, са точни и се поддържат актуални.

Пример

Данните се съхраняват твърде дълго без актуализация

Вашето дружество/организация ръководи кантора за набиране на персонал и за тази цел събира автобиографии на търсещите работа, които в замяна на вашите посреднически услуги ви плащат такса. Имате намерение да съхранявате данните за 20 години и не разполагате с мерки за актуализиране на автобиографиите. Срокът на съхранение не изглежда пропорционален на целта за намиране на работа на лице в краткосрочен до средносрочен план. Освен това фактът, че не изисквате актуализации на автобиографиите на редовни интервали, прави някои от търсенията безполезни за търсещия работа след определен период от време (например, защото този човек е придобил нови квалификации).

Позовавания

- член 5, параграф 1, буква д); съображение (39) от ОРЗД.

2.5. Каква информация трябва да бъде давана на хората, чиито данни събираме?

Отговор

По време на събирането на данните хората трябва да бъдат ясно информирани най-малкото относно:

- **кое е** Вашето дружество/организация (Вашите данни за контакт и тези на вашия СЗД, ако има такъв);
- **защо** Вашето дружество/организация ще използва личните им данни (цели);
- категориите на съответните лични данни;
- **правното основание** за обработката на данните им;
- **колко дълго** ще запазите данните;
- **кой друг** може да ги получи;
- дали техните лични данни ще бъдат **прехвърлени** на получател извън ЕС;
- че имат право на **копие на данните** (право на достъп до личните данни) и други **основни права** в областта на защитата на данните;
- **правото им да подадат жалба** до орган за защита на данните (ОЗД);
- **правото им да оттеглят съгласието си** по всяко време;
- когато е приложимо, наличието на **автоматизирано вземане на решения** и съответната логика, включително последиците от това.

Вижте **пълния списък с информация**, която трябва да бъде предоставена.

Информацията може да бъде предоставена **писмено, устно** по искане на физическото лице, когато самоличността на това лице е доказана по друг начин, или по електронен път, когато е уместно. Вашето дружество/организация трябва да направи това по **кратък, прозрачен, разбираем и лесно достъпен начин**, с **ясни и недвусмислени формулировки** и **безплатно**.

Когато данните са получени от друго дружество/организация, Вашето дружество/организация трябва да предостави горепосочената информация на лицето най-късно до 1 месец, считано от получаването на личните данни; или ако Вашето дружество/организация комуникира с физическото лицето, когато данните се използват за комуникация с тях; или ако бъде предвидено оповестяване пред друго дружество, когато личните данни бъдат разкрити за пръв път.

От Вашето дружество/организация също се изисква да информира лицето за категориите данни и източника, от който е получило данните; включително ако то и получило данни от обществено достъпни източници. При специални обстоятелства, изброени в член 13, параграф 4 и член 14, параграф 5 от ОРЗД, Вашето дружество/организация може да бъде освободено от задължението да информирате лицето. Моля, проверете дали това изключение се прилага за Вашето дружество/организация.

Позовавания

- член 12, параграфи 1, 5 и 7, членове 13 и 14 и съображения (58)−(62) от ОРЗД;
- Насоки на работната група по член 29 относно прозрачността.

3. ПУБЛИЧНА АДМИНИСТРАЦИЯ И ЗАЩИТА НА ДАННИТЕ

3.1. Кои са основните аспекти на Общия регламент относно защитата на данните (ОРЗД), с които трябва да сме запознати?

Отговор

Като публична администрация вие сте подчинени на правилата на ОРЗД, когато обработвате лични данни, свързани с дадено физическо лице. Националните администрации имат отговорността да подпомагат регионалните и местните администрации при подготовката им за прилагането на ОРЗД.

Повечето от личните данни, съхранявани от публичните администрации, обичайно се обработват въз основа на правно задължение или поради това че те са необходими за изпълнението на задачи от обществен интерес или за упражняването на официално правомощие, предоставено на администрацията. Личните данни трябва да се събират и обработват само дотолкова, доколкото е необходимо да се изпълняват тези задачи.

Трябва да се уверите, че спазвате **основни принципи** при обработването на лични данни, като например:

- честна и законна обработка;
- ограничение на целта;
- свеждане на данните до минимум и запазване на данните.

В случай на обработване на данни по силата на законодателство, това законодателство следва да гарантира, че се спазват тези принципи (напр. видове данни, период на съхранение и подходящи гаранции).

Преди да обработвате лични данни, трябва да информирате физическите лица за обработването, като например за целите, видовете събрани данни, получателите и правата им за защита на данните.

Като публична администрация вие сте длъжни да **назначите служител по защита на данните (СЗД)**; може **обаче** да се определи един единствен служител по защита на данните за няколко публични

организации, който съответно да работи за всички тях, или тази работа може да се възложи на външен СЗД. Също така трябва да сте сигурни, че сте въвели подходящи технически и организационни мерки за **защита на личните данни**. Ако прехвърляте части от обработването на външна организация (т.нар. „обработващ данни“), трябва да има договор или друг правен акт, който да гарантира че обработващият данни предоставя достатъчно гаранции за прилагането на подходящи технически и организационни мерки, които отговарят на стандартите на регламента.

В случаите, когато лични данни, които съхранявате, бъдат разкрити случайно или незаконно на неоторизирани получатели или временно са недостъпни или променени, трябва да **уведомите за нарушението органа за защита на личните данни (ОЗД)** без ненужно забавяне и най-късно до 72 часа, след като сте узнали за нарушението. Също така може да се наложи да информирате и физическите лица за нарушението.

Можете да намерите повече информация за задълженията си по ОРЗД в раздел „Бизнес и организации“.

Позовавания

- глави II и IV от ОРЗД.

3.2. Публична администрация и защита на данните

Отговор

Физическите лица могат да се свържат с вас, за да упражнят своите права съгласно ОРЗД (права за достъп, коригиране, изтриване, ограничаване, възразяване, да не бъдат обект на автоматизирано вземане на решение).

Обърнете внимание, че физическите лица имат **право да се противопоставят** на обработването на лични данни от публичната администрация, позовавайки се на съображения от обществен интерес. Те трябва да ви изложат пред публичната администрация съображения, свързани с тяхната конкретна ситуация. Публичната администрация може да продължи да обработва данните и по този начин да отхвърли искането им, ако демонстрира убедителни основателни причини за обработването, които имат преимущество пред интересите и правата на физическото лице, или ако данните са необходими за установяване, упражняване или защита на правни искове.

Физическите лица нямат право на прехвърляне на свързани с тях данни, които са необходими за изпълнение на задача от обществен интерес или при упражняване на предоставено официално правомощие.

Трябва да **отговорите** на исканията на физическите лица без ненужно забавяне и по принцип в рамките на **1 месец** от получаване на искането. Можете да ги помолите за допълнителна информация, за да потвърдите самоличността на лицето, подало искането. Ако отхвърлите искането, трябва да информирате физическите лица за причините за това и за правото им да подадат жалба до ОЗД и да потърсят съдебна защита.

Можете да намерите повече информация за задълженията си по ОРЗД в раздел „Бизнес и организации“.

Позовавания

- глава III от ОРЗД.

3.3. Какво ще стане, ако публична администрация не спази правилата за защита на данните?

Отговор

Органите за защита на данните имат на свое разположение различни инструменти в случай на неспазване. В случай на вероятно нарушение може да бъде издадено **предупреждение**. В случай на нарушение възможностите включват: **порицание, временна или окончателна забрана на обработването.** В някои държави публичните органи също могат да бъдат обект на **административни наказания**. Публичната администрация трябва да направи справка с националния закон за защита на данните в своята държава.

Физическите лица могат да предявят иск за обезщетение, когато публичен орган е нарушил ОРЗД и те са понесли материални щети (например финансови загуби) или неимуществени щети (например загуба на репутация или психологически стрес).ОРЗД гарантира, че ще им бъде предоставено обезщетение, независимо от броя на организациите, участващи в обработването на техните данни. Обезщетението може да бъде предявено директно от публичния орган или пред компетентните национални съдилища.

Позовавания

• членове 58 и членове82, 83 и84 и съображения (129), (146), (147), (148), (150) и(151) от ОРЗД.

4. ПРАВНИ ОСНОВАНИЯ ЗА ОБРАБОТВАНЕ НА ДАННИ

4.1. Основания за обработване

4.1.1. Кога могат да бъдат обработвани лични данни?

Отговор

Вашето дружество/организация може да обработва лични данни само при следните обстоятелства:

• със **съгласието** на засегнатите физически лица;

• когато е налице **договорно задължение** (договор между Вашето дружество/организация и клиент);

• за да се изпълни **правно задължение** (съгласно законодателството на ЕС или националното законодателство);

• когато обработването е необходимо за изпълнение на задача, изпълнявана от обществен интерес (съгласно законодателството на ЕС или националното законодателство);

• за да се защитят **жизненоважни интереси** на дадено физическо лице;

• за **законни интереси** на вашата организация, но само след като сте проверили, че основните права и свободи на лицето, чиито данни обработвате, не са сериозно засегнати. Ако правата на лицето имат преимущество пред Вашите интереси, тогава не можете да обработвате въз основа на законен интерес. Преценката дали законните интереси на Вашето дружество/организация за обработване на данните имат преимущество пред тези на засегнатите лица зависи от индивидуалните обстоятелства в дадения случай.

Примери

Съгласие

Вашето дружество/организация предлага музикално приложение и иска съгласието на гражданите, за да обработва музикалните им предпочитания, с цел да им предлага песни и възможни концерти съгласно техните интереси.

Договорно задължение

Вашето дружество/организация продава стоки онлайн. То може да обработва данните, които са необходими за предприемане на стъпки по искане на физическото лице преди сключването на договора и за изпълнението на договора. Така че можете да обработвате името, адреса за доставка, номера на кредитната карта (ако плащането е с карта) и т.н.

Правно задължение

Вие притежавате дружество със служители. За да получите социално осигуряване, законът ви задължава да предоставите на съответния орган лични данни (например седмичния доход на вашите служители).

Обществен интерес

Пример: професионална асоциация, като например адвокатска асоциация или камара на медицинските специалисти, може да извършва дисциплинарни процедури срещу някои от своите членове, ако има официално правомощие за това.

Жизненоважни интереси на дадено лице

Болница лекува пациент след тежка пътна катастрофа; болницата не се нуждае от съгласието му, за да потърси идентификационния му номер и да провери дали това лице съществува в базата данни на болницата, за да намери предишна медицинска история или да се свърже с близък роднина.

Законните интереси на вашата организация

Вашето дружество/организация гарантира своята мрежова сигурност, като следи за използването на ИТ устройствата на своите служители. Вашето дружество/организация може законно да обработва лични данни за тази цел само ако избере метод с най-малка степен на вмешателство по отношение на правото на личен живот и защита на личните данни на вашите служители, например като ограничи достъпността на определени уебсайтове. (Обърнете внимание, че това не може да се направи в държави членки на ЕС, в които националното законодателство определя по-строги правила за обработка в контекста на трудовата заетост).

Позовавания

- член 6 и съображения (40) - (49) от ОРЗД;
- Становище 06/2014 на работната група по член 29 относно понятието за законни интереси на администратора на лични данни съгласно член 7 от Директива 95/46/ЕО.

4.1.2. Какво означава „съображения, свързани със законните интереси“?

Отговор

Като дружество/организация често трябва да обработвате лични данни, за да изпълнявате задачи, свързани с вашите бизнес дейности. Обработването на лични данни в този контекст може да не е непременно оправдано от правно задължение или поради необходимост да се изпълнят условията на договор, сключен с дадено физическо лице. В такива случаи обработването на личните данни може да бъде обосновано със съображения, свързани със законни интереси.

Вашето дружество/организация трябва да информира физическите лица за обработването, когато събира личните им данни.

Вашето дружество/организация също така трябва да провери дали, като преследва законните си интереси, не засяга сериозно правата и свободите на тези физически лица, в противен случай Вашето дружество/организация не може да разчитате на законните си интереси като оправдание за обработването на данните и трябва да намери друго правно основание.

Пример

Вашето дружество/организация ма законен интерес, когато обработването се извършва в рамките на взаимоотношение с клиент, когато обработва лични данни за целите на директния маркетинг, за да предотврати измами или за да осигури мрежова и информационна сигурност на Вашите ИТ системи.

Позовавания

- член 6 и съображения (47), (48) и (49) от ОРЗД;
- Становище 06/2014 на работната група по член 29 относно понятието за законни интереси на администратора на лични данни съгласно член 7 от Директива 95/46/ЕО.

4.1.3. Кога съгласието е валидно?

Отговор

Когато е необходимо да получите **съгласие** да обработвате лични данни, трябва да бъдат изпълнени няколко условия, за да бъде това съгласие валидно:

- то трябва да бъде **дадено свободно;**
- то трябва да бъде **информирано**;
- то трябва да бъде дадено за **конкретна цел**;
- всички причини за обработването трябва да бъдат ясно посочени;
- то е **изрично** и се дава чрез положителен акт (напр. електронно поле за отметка, което физическото лице трябва да отбележи изрично онлайн, или подпис върху формуляр);
- **то е ясно и недвусмислено формулирано** и ясно се вижда;
- **трябва да бъде възможно съгласието** да се оттегли и този факт следва да бъде обяснен (напр. препратка за прекратяване на абонамента в края на електронен бюлетин).

За да бъде съгласието **дадено свободно**, физическото лице трябва да има свободен избор и трябва да може да откаже или да оттегли съгласието си, без да е в неравностойно положение. Съгласието не е дадено свободно, ако например има явен дисбаланс между физическото лице и дружеството/организацията (напр. взаимоотношението работодател/служител) или когато дружеството/организацията изисква от физическите лица да дадат съгласието си за обработването на ненужни лични данни като условие за изпълнението на договор или услуга.

За да бъде съгласието **информирано**, на лицето трябва да бъде предоставена най-малко следната информация:

- идентичността на организацията, обработваща данните;
- целите, за които се обработват данните;
- вида на данните, които ще бъдат обработени;
- възможността да се оттегли даденото съгласие (например: препратка за отписване в края на имейл);
- когато е приложимо, фактът, че данните ще се използват само за автоматизирано вземане на решения, включително профилиране;
- ако съгласието е свързано с международно предаване, възможните рискове от предаването на данните към трети страни, които не са предмет на решение относно адекватно ниво на защита и когато не са налице подходящи гаранции.

Запомнете: когато някой се съгласява с обработването на личните му данни, можете да обработвате данните само за целите, за които е дадено съгласието.

Примери

Свободно съгласие

Вие сте дружество за въздушен превоз и Вашето съобщение за поверителност показва, че личните данни на клиентите могат да бъдат обработени за конкурс, организиран от авиокомпанията, предлагаща безплатен полет като награда. Клиентите, които поставят отметка в квадратчето и с това се съгласяват да участвате в конкурса, следователно ясно показват желанието си личните им данни да се обработват за целите на конкурса. Налице е съгласие да се обработват данни за целите на конкурса, но не и за други цели.

Несвободно съгласие

Вашето дружество/организация предлага онлайн филмови услуги. При събирането на данните, необходими за този договор, също така изисквате допълнителни данни, като например сексуалната ориентация или политическите убеждения на дадено лице. Това лице може да смята, че неговото съгласие за обработването на този тип данни е необходимо за достъп до филмите, които то изисква. Съгласието в този случай не е свободно, а е „обвързано съгласие“.

Позовавания

- член 4, параграф 11 и член 7; съображения (32), (42), (43) от ОРЗД;
- Становище на работната група по член 29 относно съгласието, прието на 28 ноември 2017 г.

4.1.4. Може ли съгласието, дадено преди 25 май 2018 г., да продължи да се използва, след като ОРЗД започне да се прилага, считано от 25 май 2018 г.?

Отговор

Ако съгласието, дадено от лицето преди влизането в сила на Общия регламент относно защитата на данните (ОРЗД), отговаря на условията на ОРЗД, тогава няма нужда да се иска отново съгласието на лицето. Вашето дружество/организация трябва да се увери, че съгласието, дадено преди влизането в сила на ОРЗД, отговаря на условията, определени в ОРЗД.

Примери

Няма нужда от ново съгласие

ОРЗД ще влезе в сила на 25 май 2018 г. Наскоро сте преразгледали политиката на Вашето дружество/организация за защита на личните данни. Проверили сте, че съгласието на клиентите на организацията ви е било получено в писмен вид и отговаря на всички изисквания на ОРЗД. В този случай не е необходимо отново да искате съгласието на клиентите си през май 2018 г.

Необходимо е отново да получите съгласие

Вашето дружество/организация е получило/-а сте съгласие от клиентите преди няколко години, като е използвало/-а онлайн система с предварително маркирани полета. Вече е ясно, че този начин на получаване на съгласие няма да е валиден към 25 май 2018 г. Вашето дружество/организация ще трябва отново да получи това съгласие, ако иска да продължи да обработвате данните.

Позовавания

- член 4, параграф 11 и член 7; съображение (171) от ОРЗД;
- Становище на работната група по член 29 относно съгласието, прието на 28 ноември 2017 г.

4.1.5. Какво ще стане, ако някой оттегли своето съгласие?

Отговор

Трябва да е също толкова лесно да се оттегли съгласие, колкото и да се даде. Ако съгласието е оттеглено, Вашето дружество/организация вече не може да обработвате данните. След като съгласието е оттеглено, Вашето дружество/организация трябва да бъде сигурно/-а, че данните ще бъдат изтрити, освен ако няма друго правно основание за обработването им (напр. изисквания за съхранение или доколкото е необходимо, за да се изпълни договорът).

Ако данните са били обработвани за няколко цели, Вашето дружество/организация не може да използвате личните данни за частта от обработването, за която съгласието е оттеглено, или за някоя от целите, в зависимост от естеството на оттеглянето на съгласието.

Пример

Предоставяте онлайн бюлетин. Вашият клиент дава съгласието си за абонамент за онлайн бюлетина, което ви позволява да обработвате всички данни за интересите му, за да създадете профил за това какви статии разглежда. Една година по-късно той ви информира, че вече не желае да получава онлайн бюлетина. Вие трябва да изтриете от базата данни всички лични данни, свързани с това лице, събрани в контекста на абонамента за бюлетина, включително профила(ите), свързани с това лице.

Позовавания

- член 7 и съображения (32), (33), (42), (43) и (58) от ОРЗД;
- Становище 15/2011 на работната група по член 29 относно определението на съгласие (което предстои да се актуализира със становището, което ще се приеме на 28 ноември 2017 г.).

4.1.6. Как да получим съгласие за обработване на данни за научни изследвания?

Отговор

В контекста на научните изследвания е разрешена известна гъвкавост по отношение на степента на спецификация и детайлността на съгласието. При събирането на лични данни изследователите може да не са в състояние напълно да идентифицират целите на обработването им. В тези случаи те могат да поискат от хората да дадат съгласието си за определени области на научни изследвания или части от изследователски проекти. Във всички случаи съгласието трябва да запази основните си елементи, т.е. то трябва да бъде свободно дадено, информирано, получено чрез ясни положителни действия и специфично до степента, определена от въпросното изследване. Изследователите трябва да се уверят, че спазват както етичните, така и методологичните стандарти, изисквани в тяхната област.

Пример

Група от изследователи иска да проучи конкретен вид рак, но е наясно с възможните последици за други видове рак. В този случай те могат да поискат съгласието на даден човек за обработване на данните, свързани с изследванията на рака.

Позоваване

- съображение (33) от ОРЗД.

4.2. Чувствителни данни

4.2.1. Кои лични данни се считат за чувствителни?

Отговор

Следните лични данни се считат за „чувствителни“ и подлежат на специфични условия на обработване:

• лични данни, разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения;

• членство в професионална организация;

• генетични данни, биометрични данни, обработвани единствено с цел идентификацията Ви като човешко същество;

• данни за здравословното състояние;

• данни за сексуалния живот или сексуалната ориентация на дадено лице.

Позовавания

• член 4, параграфи 13, 14 и 15, член 9 и съображения (51)–(56) от ОРЗД.

4.2.2. При какви условия моето дружество/организация може да обработва чувствителни данни?

Отговор

Вашето дружество/организация можете да обработвате чувствителни данни само ако отговаря на едно от изброените по-долу условия:

• получено е **изрично съгласие** на физическото лице (в някои случаи законът може да изключва тази опция);

• **законодателството на ЕС, националното законодателство или колективен трудов договор изискват от** Вашето дружество/организация да обработва данните, за да изпълни задълженията и правата си, както и тези на физическите лица съгласно законодателството в областта на трудовата заетост, социалната сигурност и социалната закрила;

• **жизненоважните интереси** на лицето или на лице, което физически или юридически неспособно да даде своето съгласие, са изложени на риск;

• вие сте **фондация, асоциация или друга нестопанска организация** с политическа, философска, религиозна или синдикална цел, обработваща данни за своите **членове** или хора, които редовно контактуват с организацията;

• личните данни явно са направени **обществено достояние** от физическото лице;

• изискват се данни за установяване, упражняване или защита на **правни искове**;

• обработват се данните от съображения за **съществен обществен интерес** въз основа на европейското или националното законодателство;

• обработват се данните за целите на: **превантивна или професионална медицина**; оценка на работоспособността на служителя; медицинска диагноза; предоставяне на здравни или социални грижи или лечение, или управлението на здравните или социалните системи и услуги въз основа на европейското или националното законодателство или въз основа на договор като здравен специалист;

• обработват се данните по причини от **обществен интерес в областта на общественото здраве** въз основа на европейското или националното законодателство;

• обработват се данните за **архивиране, за научни или исторически изследователски цели** или за статистически цели въз основа на европейското или националното законодателство.

За обработването на генетични данни, биометрични данни или данни за здравословното състояние могат да бъдат наложени допълнителни условия от националното законодателство. Консултирайте се с вашия национален орган за защита на данните.

Пример

Можете да обработвате чувствителни данни

Лекар преглежда редица пациенти в клиниката си. Той регистрира посещението в база данни, включваща полета, като име/фамилно име на пациента, описание на симптомите и предписаните медикаменти. Тези данни се считат за чувствителни данни. Обработването на здравни данни от клиниката е разрешено съгласно закона за защита на данните, тъй като се изисква за лечението на лицето и това се извършва под отговорността на лекар, който е обект на задължение за професионална тайна.

Не можете да обработвате чувствителни данни

Вие сте дружество, което продава рокли онлайн. С цел да съобразите услугите със специфичните интереси на вашите клиенти, вие ги молите да ви предоставят информация за размера, предпочитания цвят, начина на плащане, името и адреса, така че продуктът да може да бъде доставен. В допълнение Вашето дружество отправя искане към клиентите да посочат политически си възгледи. Нуждаете се от по-голямата част от информацията, за да изпълните вашата страна на договора. Политическите възгледи на клиентите обаче не са необходими за изработката и доставката на роклите им. Вашето дружество/организация не може да поиска тази информация съгласно по този договор.

Позовавания

- член 9 и съображения (51)−(56) от ОРЗД.

4.3. Има ли конкретни предпазни мерки за данните на децата?

Отговор

Вашето дружество/организация може да обработва личните данни на дете само въз основа на съгласие, ако имате **изричното съгласие на родителя или настойника му**, до определена възраст. Възрастовата граница за получаване на съгласието на родителите варира между 13 и 16 години, в зависимост от възрастта, определена в различните държави от ЕС. Консултирайте се с вашия национален орган за защита на данните.

Трябва да бъдат положени разумни усилия, като се вземе предвид наличната технология, за да се провери дали даденото съгласие действително е в съответствие със закона. Това означава, че Вашето дружество/организация трябва да въведе мерки за проверка на възрастта (напр. контролни въпроси, действия на уебсайта).

Трябва да бъде получено съгласие от родителя или настойника, ако Вашата организация работи на онлайн сайтове за социални контакти, които предоставят например безплатни игри на децата или семейни застраховки.

Ако дейността на Вашата организация е насочена към деца, трябва да сте сигурни, че всяка информация и всяко съобщение, адресирани до детето, са лесно достъпни и ясно и недвусмислено формулирани така, че детето да може да ги разбере лесно.

Пряко предлаганите на деца услуги за превенция и консултиране не изискват съгласието на родител, тъй като те имат за цел да защитят висшите интереси на детето.

Позовавания

- членове 8 и 12 и съображения (38) и (58) от ОРЗД.

4.4. Може ли да се използват за маркетинг данни, получени от трета страна?

Отговор

Преди да получите от друга организация списък с контакти или база с данни за връзка с физически лица, тази организация трябва да може да **докаже, че данните са получени в съответствие с Общия регламент относно защитата на данните** и че те **може да се използват за рекламни цели**. Например, ако организацията ги е придобила въз основа на съгласие, съгласието трябва да включва възможността за предаване на данните на други получатели за техния собствен директен маркетинг.

Вашето дружество/организация трябва също така да се увери, че списъкът или базата данни са актуални и че не изпраща реклами на лица, които възразяват срещу обработването на личните им данни за целите на директния маркетинг. Вашето дружество/организация също така трябва да се увери, че ако използва за целите на директния маркетинг комуникации, като например имейл, то спазва правилата, посочени в **Директивата за правото на неприкосновеност на личния живот и електронни комуникации** (Директива 2002/58/ЕО на Европейския парламент и на Съвета от 12 юли 2002 година относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации (ОВ L 201, 31.07.2002 г., стр.37)).

Такива списъци следва да се обработват въз основа на законните интереси и физическите лица ще имат право да възразят срещу подобно обработване. Освен това Вашето дружество/организация трябва да информира физическите лица, най-късно по време на първата комуникация с тях, че е събрало личните им данни и че ще ги обработва за изпращане на реклами.

Пример

Двама приятели, г-жа А и г-н Б, управляват съответно фитнес зала и книжарница. Всеки събира данни от съответните си клиенти. Книжарницата на г-н Б не върви добре. В неговата база данни има вписани няколко клиенти, а в книжарницата му не влизат много хора. Той казва на г-жа А, че има нова биографична книга на известен спортист и пита дали клиентите на г-жа А биха били заинтересовани да получат реклама за книгата. Условията на известието за поверителност на г-жа А информират клиентите ѝ, че тя би могла да сподели данните им с партньори, които предлагат продукти в областта на здравето и фитнеса. При условие че е предоставено конкретно съгласие за предаване на данните на други получатели за техния собствен директен маркетинг, г-жа А може да изпрати списъка на клиентите на г-н Б. Не могат да бъдат изпратени данни за субект на данни, който е възразил срещу обработката на личните му данни.

Позовавания

- член 4, параграф 10 и членове 5, 6, 14 и 21 от ОРЗД;
- Становище на работната група по член 29 относно прозрачността;
- **Директивата за правото на неприкосновеност на личния живот и електронни комуникации,** правила за директния маркетинг, по-специално член 13.

5. ЗАДЪЛЖЕНИЯ

5.1. Администратор/Обработващ данните

5.1.1. Какво е администратор на данни или обработващ данни?

Отговор

Администраторът на данни определя **целите**, за които, и **средствата** , с които се обработват личните данни. Така че, ако Вашето дружество/организация вземе решение „защо“ и „как“ трябва да бъдат обработени личните данни, тое администраторът на данни. Служителите, които обработват лични данни във вашата организация, правят това, за да изпълняват задачите ви като администратор на данни.

Вашето дружество/организация е **съвместен администратор**, когато заедно с една или повече организации съвместно определя „защо“ и „как“ трябва да бъдат обработени личните данни. Съвместните администратори трябва да сключат споразумение, определящо съответните им отговорности за спазване на правилата на ОРЗД. Основните аспекти на споразумението трябва да бъдат съобщени на лицата, чиито данни се обработват.

Обработващият данни обработва лични данни само **от името на администратора**. Обработващият данни обикновено е трета страна, външна за дружеството. Обаче в случай на групи предприятия, едно предприятие може да действа като обработващ данни за друго предприятие.

Задълженията на обработващия данни към администратора трябва да бъдат определени в договор или друг правен акт. Например в договора трябва да се посочи какво се случва с личните данни след прекратяването на договора. Типична дейност на лицата, обработващи данни, е да предлагат ИТ решения, включително съхранение в облак. Обработващият данни може да възложи само част от задачата си на друг обработващ данни или да назначи съвместен обработващ данни, когато е получил предварително писмено разрешение от администратора на данни.

Има ситуации, в които дадено лице може да бъде администратор на данни или обработващ данни, или двете.

Примери

Администратор и обработващ данните

Пивоварна има много служители. Тя подписва договор със счетоводно дружество с цел изплащане на заплатите. Пивоварната уведомява счетоводното дружество кога трябва да бъдат изплатени заплатите, както и когато служител напусне или има повишение в заплащането, и предоставя всички останали подробности за ведомостта за заплати и плащането. Счетоводното дружество осигурява ИТ системата и съхранява данните на служителите. Пивоварната е администраторът на данни, а счетоводното дружество е обработващият данни.

Съвместни администратори

Вашето дружество/организация предлага услуги за гледане на деца чрез онлайн платформа. В същото време Вашето дружество/организация има договор с друго дружество, което ви позволява да предлагате услуги с добавена стойност. Тези услуги включват възможност родителите не само да избират детегледачката, но и да наемат игри и DVD-та, които детегледачката може да донесе. И двете дружества участват в техническата настройка на уебсайта. В този случай двете дружества са решили да използват платформата за двете цели (услуги за гледане на деца и отдаване под наем на DVD/игри) и много често ще споделят имената на клиентите. Следователно двете дружества са съвместни администратори, защото те не само че се съгласяват да предлагат възможност за „комбинирани услуги“, но и разработват и използват обща платформа.

Позовавания

- член 4, параграфи 7 и 8, членове 24, 26, 28 и 29 и съображения (74), (79) и (81) от ОРЗД;
- Становище 1/2010 на работната група по член 29 относно понятията „администратор“ и „обработващ данни“ (WP 169).

5.1.2. Може ли някой друг да обработва данните от името на моята организация?

Отговор

Някой друг (физическо или юридическо лице или друг орган) **може да обработва лични данни** от Ваше име, при условие че **има договор или друг правен акт**. Важно е избраният от вас обработващ

данни да предостави достатъчно гаранции за прилагане на подходящи технически и организационни мерки, за да гарантира, че обработката ще отговаря на стандартите на Общия регламент относно защитата на данните (ОРЗД) и ще гарантира защитата на правата на физическите лица.

Назначеният обработващ данни впоследствие не може да назначава друг обработващ данни без вашето предварително, конкретно или общо писмено разрешение. Договорът или правният акт, сключен между Вашето дружество/организация и обработващия данни, трябва да включва следните елементи:

- обработването може да се извършва само при документирани инструкции от администратора;
- обработващият данни гарантира, че лицата, упълномощени да обработват личните данни, са се ангажирали с поверителността или са подчинени на съответното правно задължение за поверителност;
- обработващият данни трябва да предлага минимално ниво на сигурност, определено от администратора;
- администраторът трябва да съдейства при осигуряването на съответствие с ОРЗД.

Примери

Строителна фирма използва подизпълнител за конкретни строителни работи и му предоставя данните за контакт на клиентите, при които трябва да се извършат строителните работи. Подизпълнителят допълнително използва данните, за да изпрати на клиентите маркетингов материал. Подизпълнителят в този случай не се квалифицира само като „обработващ данни“ съгласно ОРЗД, тъй като той не само обработва лични данни от името на строителната компания, но ги обработва и допълнително за свои собствени цели. Подизпълнителят следователно действа като „администратор на данни“.

Вие сте дружество за търговия на дребно, което решава да съхранява резервна версия на вашата клиентска база данни на облачен сървър. За тази цел сключвате договор с доставчик на компютърни услуги „в облак“, известен със своите стандарти за защита на данните, който също така има и сертифицирана система за криптиране на данни. Доставчикът на компютърни услуги „в облак“ е вашият обработващ данни, тъй като съхранява личните данни на вашите клиенти на сървърите си и ще обработва личните данни от ваше име.

Позовавания

- член 28 и съображение (81) от ОРЗД.

5.2. Еднакви ли са задълженията, независимо от количеството данни, които моето/моята дружество/организация обработва?

Отговор

Общият регламент относно защитата на данните (ОРЗД) се основава на подход, съобразен с риска. С други думи, дружествата/организациите, които обработват лични данни, се насърчават да прилагат защитни мерки, **съответстващи на нивото на риска за техните дейности по обработка на данни**. Поради това задълженията на дружество, което обработва много данни, са по-обременителни, отколкото на дружество, което обработва малко данни.

Например вероятността за наемане на служител по защита на данните е по-голяма при дружества/организации, които обработват много данни, отколкото при дружества/организации, които обработват малко данни (в този случай това е свързано с понятието за обработка на лични данни в „голям мащаб“). Същевременно естеството на личните данни и въздействието на предвиденото обработване също играят роля. Обработването на малко данни, но които имат чувствителен характер,

напр. данни за състоянието на здравето, би изискало прилагането на по-строги мерки за спазване на ОРЗД.

Във всички случаи принципите за защита на данните трябва да се спазват и да на физическите лица трябва да се позволи да упражняват правата си.

Позоваване

- глава IV от ОРЗД

5.3. Какво означава защитата на данните „на етапа на проектирането“ и „по подразбиране“?

Отговор

Дружествата/организациите се насърчават да прилагат технически и организационни мерки на най-ранните етапи от проектирането на операциите по обработка така, че от самото начало да защитават принципите на неприкосновеност на личния живот и защита на данните („защита на данните на етапа на проектиране“). По подразбиране дружествата/организациите трябва да гарантират, че личните данни се обработват с най-голяма защита на неприкосновеността на личния живот (напр. следва да се обработват само необходимите данни, кратък период на съхранение, ограничен достъп) така, че личните данни по подразбиране да не са достъпни за неопределен брой лица („защита на данните по подразбиране“).

Примери

Защита на данните на етапа на проектирането

Използване на псевдонимизиране (замяна на лично идентифицируем материал с изкуствени идентификатори) и криптиране (кодиране на съобщения така, че да могат да ги прочетат само оторизираните лица).

Защита на данните по подразбиране

Социална медийна платформа трябва да се насърчи да зададе такива настройки на потребителските профили, които са най-благоприятни за неприкосновеността на личния живот, като например ограничи от самото начало достъпността до потребителските профили, за да не бъдат достъпни по подразбиране за неопределен брой лица.

Позовавания

- член 25 и съображение (78) от ОРЗД.

5.4. Какво представлява нарушение на сигурността на данните и какво следва да бъде направено в случай на нарушение на сигурността на данните?

Отговор

Нарушение на сигурността на данни възниква, когато данните, за които Вашето дружество/организация отговаря, са засегнати от инцидент със сигурността, в резултат на който се нарушава поверителността, наличието или целостта. Ако това се случи и има вероятност нарушението да представлява риск за правата и свободите на дадено лице, Вашето дружество/организация трябва да **уведоми надзорния орган без ненужно забавяне и най-късно до 72 часа, след като сте узнали за нарушението**. Ако Вашето дружество/организация е обработващ данни, то трябва да уведоми администратора на данни за всяко нарушение на сигурността на данните.

Ако нарушението на сигурността на данните представлява **висок риск за засегнатите лица**, всички те също трябва да бъдат информирани, освен ако не са въведени ефективни технически и организационни мерки за защита или други мерки, които гарантират, че вече няма вероятност рискът да се случи на практика.

За вас като организация е жизненоважно да приложите подходящи технически и организационни мерки, за да се избегнат възможни нарушения на сигурността на данните.

Примери

Организацията трябва да уведоми ОЗД и физическите лица

Данните на служителите на текстилно дружество са разкрити. Данните включват личните адреси, членове на семейството, месечната заплата и медицински бележки на всеки служител. В този случай текстилното дружество трябва да информира надзорния орган за нарушението. Тъй като личните данни включват чувствителни данни, като например данни за здравословното състояние, дружеството трябва да уведоми и служителите.

Болничен служител решава да копира данните на пациентите на компактдиск и да ги публикува онлайн. Болницата разбира за това няколко дни по-късно. Веднага след като болницата разбере, тя има 72 часа, за да информира надзорния орган, и тъй като личните данни съдържат чувствителна информация, като например дали даден пациент е болен от рак, дадена пациентка е бременна и т.н., тя трябва да информира и пациентите. В този случай би било под въпрос дали болницата е въвела подходящи технически и организационни мерки за защита. Ако тя действително е въвела подходящи мерки за защита (напр. криптиране на данните), би било малко вероятно рискът да се осъществи и тя би могла да бъде освободена от изискването за уведомяване на пациентите.

Дружеството трябва да уведоми клиентите, а те могат след това да уведомят ОЗД и физическите лица

Дружество, предлагащо услуги „в облак“, губи няколко твърди диска, които съдържат лични данни, принадлежащи на няколко от неговите клиенти. То трябва да уведоми тези клиенти, веднага щом узнае за нарушението. Неговите клиенти трябва да уведомят ОЗД и физическите лица в зависимост от данните, които са били обработени от обработващия данни.

Позовавания

- Насоки на работната група по член 29 относно известието за нарушение на сигурността на личните данни съгласно Регламент 2016/679 (WP 250);
- член 4, параграф 12 и членове 33 и 34 и съображения (85), (86), (87) и (88) от ОРЗД.

5.5. Кога е необходимо да се изготви оценка на въздействието върху защитата на данните (ОВЗД)?

Отговор

ОВЗД се изисква, когато има вероятност обработването да доведе до висок риск за правата и свободите на физическите лица. ОВЗД се изисква най-малко в следните три случая:

- системна и обширна оценка на личните аспекти на физическо лице, включително профилиране;
- обработване на чувствителни данни в голям мащаб;
- систематично мащабно наблюдение на обществените зони.

Националните органи за защита на данните в съгласие с Европейския комитет за защита на личните данни могат да предоставят списъци на случаи, при които може да се изисква ОВЗД. ОВЗД

трябва да се извърши преди обработването и трябва да се разглежда като жив инструмент, а не като еднократно действие. Когато съществуват остатъчни рискове, които не могат да бъдат смекчени от въведените мерки, трябва да се направи консултация с ОЗД преди началото на обработването.

Примери

Изисква се ОВЗД

Банка, която проверява клиентите си чрез база данни за кредитна справка; болница, която иска да въведе нова база данни за здравна информация със здравни данни за пациентите; автобусен превозвач, който е на път да монтира камери в автобусите, за да наблюдава поведението на шофьорите и пътниците.

Не се изисква ОВЗД

Общински лекар, който обработва лични данни на своите пациенти. В този случай, при условие че броят на пациентите е ограничен, няма нужда от ОВЗД, тъй като обработването от общинските лекари не се прави в голям мащаб.

Позовавания

• Насоки на работната група по член 29 относно оценката на въздействието върху защитата на данните (ОВЗД) и определяне дали обработването е „възможно да доведе до висок риск“ за целите на Регламент (ЕС) 2016/679 от 4 април 2017 г.;

• членове 35 и 36 и съображения (89) - (96) от ОРЗД.

5.6. Служители по защита на данните

5.6.1. Трябва ли моето/моята дружество/организация да има служител по защита на данните (СЗД)?

Отговор

Вашето дружество/организация трябва да назначи СЗД, независимо дали е администратор или обработващ данни, ако неговите **основни дейности** включват обработка на **чувствителни данни** в **голям мащаб** или основните ви дейности включват **мащабно, редовно и систематично наблюдение** на физическите лица. В тази връзка наблюдението на поведението на физическите лица включва всички форми на проследяване и профилиране в интернет, включително за целите на поведенческата реклама.

Публичните администрации винаги имат задължението да назначават СЗД (с изключение на съдилища при изпълнение на съдебните им функции).

СЗД може да бъде член на персонала на вашата организация или да бъде външно лице, назначено въз основа на договор за услуги. СЗД може да бъде физическо лице или организация.

Примери

Задължителен СЗД

СЗД е задължителен например когато Вашето дружество/организация:

• управлява болница, която обработва големи набори от чувствителни данни;

• е дружество за сигурност, което отговаря за наблюдението на търговски центрове и публични пространства;

• управлява малко дружество за набиране на висококвалифициран персонал, която изготвя профили на физически лица.

Незадължителен СЗД

СЗД не е задължителен, ако:

- вие сте лекар на местната общност и обработвате личните данни на вашите пациенти;
- имате малка юридическа кантора и обработвате лични данни на вашите клиенти.

Позовавания

- Насоки на работната група по член 29 относно служителите по защита на данните, 5 април 2017 г. (WP 243);
- членове 37, 38 и 39 и съображение (97) от ОРЗД.

5.6.2. Какви са отговорностите на служителя по защита на данните (СЗД)?

Отговор

СЗД подпомага администратора или обработващия данни по всички въпроси, свързани със защитата на личните данни. По-специално СЗД трябва:

- да информира и да дава съвети на администратора или на обработващия данни, както и на техните служители за задълженията им съгласно закона за защита на данните;
- да следи за спазването от страна на организацията на цялото законодателство във връзка със защитата на данните, включително при одити, дейности за повишаване на осведомеността, както и обучение на персонала, участващ в операциите по обработване;
- да дава съвети, когато е извършена ОВЗД, и да наблюдава нейното изпълнение;
- да действа като звено за контакт за искания от страна на физически лица относно обработката на личните им данни и упражняването на техните права;
- да си сътрудничи със ОЗД и да действа като звено за контакт за ОЗД по въпроси, свързани с обработването.

Организацията трябва да включва своевременно СЗД . СЗД не трябва да получава указания от администратора или обработващия данни за изпълнение на задачите си. СЗД докладва директно на най-високото ниво на управление на организацията.

Позоваване

- членове 37, 38 и 39 и съображение (97) от ОРЗД.

5.7. Какви правила се прилагат, ако моята организация прехвърля данни извън ЕС?

Отговор

В днешния глобализиран свят има голям брой трансгранични прехвърляния на лични данни, които понякога се съхраняват на сървъри в различни държави. **Предоставената защита от Общия регламент относно защитата на данните (ОРЗД) пътува с данните**, което означава, че правилата за защита на личните данни продължават да се прилагат, независимо от това къде се намират данните. Това важи и когато данните се прехвърлят на държава, която не е членка на ЕС (по-нататък „трета страна“).

ОРЗД предоставя различни инструменти за прехвърляне на данни от ЕС към трета страна:

- понякога с решение на Европейската комисия може да бъде обявено, че трета страна, предлага адекватно ниво на защита („решение за адекватно ниво на защита“), което означава, че можете да

прехвърляте данни на друго дружество в тази трета страна, без да е необходимо износителят на данни да предоставя допълнителни гаранции или данните да бъдат обект на допълнителни условия. С други думи, прехвърлянията към трета страна с адекватно ниво на защита ще бъдат сравними на предаването на данни в рамките на ЕС;

• при липса на решение за адекватно ниво на защита прехвърлянето може да се извърши чрез предоставяне на подходящи гаранции и при условие че са налице приложими права и ефективни правни средства за защита на физическите лица. Тези подходящи предпазни мерки включват, наред с другото:

– в случай на група предприятия или групи от дружества, които извършват съвместна икономическа дейност, дружествата могат да прехвърлят лични данни въз основа на т.нар. обвързващи корпоративни правила;

– договорни споразумения с получателя на личните данни, като се използват например стандартните договорни клаузи, одобрени от Европейската комисия;

– спазване на кодекс за поведение или механизъм за сертифициране, заедно с получаване на обвързващи и изпълними ангажименти от страна на получателя за прилагане на подходящи предпазни мерки за защита на прехвърлените данни;

• и накрая, ако се предвижда прехвърляне на лични данни на трета страна, която не е предмет на решение за адекватно ниво на защита, и ако липсват подходящи предпазни мерки, може да се извърши прехвърляне въз основа на редица изключения за конкретни ситуации, например когато дадено лице изрично се е съгласило с предложеното прехвърляне, след като му е била предоставена цялата необходима информация относно рисковете, свързани с прехвърлянето.

Пример

Вие сте френско дружество, което възнамерява да разшири услугите си в Южна Америка, особено в Аржентина, Уругвай и Бразилия. Първата стъпка би била да се провери дали тези трети страни подлежат на решение относно адекватно ниво на защита. В този случай както Аржентина, така и Уругвай са обявени за държави с адекватно ниво на защита. Ще можете да прехвърляте лични данни до тези две трети страни без допълнителни гаранции, докато за прехвърляния до Бразилия, която не е обект на решение относно адекватно ниво на защита, ще трябва да оформите прехвърлянията си, като предоставите подходящи предпазни мерки.

Позовавания

• глава V, членове 44−50 и съображения (101)−(116) от ОРЗД;

• последни работни документи на **работната група по член 29** относно международните прехвърляния:

– Работен документ относно решение за адекватно ниво на защита (актуализация на глава първа на WP 12), WP 254,

– Работен документ за създаване на таблица с елементите и принципите, които могат да бъдат намерени в Задължителните корпоративни правила, WP 256,

– Работен документ за създаване на таблица с елементите и принципите, които могат да бъдат намерени в Задължителните корпоративни правила за обработващия данни, WP 257;

• вижте също за справка Съобщението на Европейската комисия **„Обмен и защита на личните данни в глобализирания свят“**, 10 януари 2017 г.

5.8. Как мога да покажа, че моята организация е в съответствие с ОРЗД?

Отговор

Принципът на **отчетност** е крайъгълен камък на Общия регламент относно защитата на данните (ОРЗД). Според ОРЗД дружество/организация следва да носи отговорност за спазването на всички принципи за защита на данните и също така следва да отговаря за доказването на това съответствие. ОРЗД предоставя на дружествата/организациите набор от инструменти, които да подпомогнат демонстрирането на отчетност, някои от които трябва задължително да бъдат въведени.

Например в конкретни случаи установяването на СЗД или провеждането на оценки на въздействието върху защитата на данните (ОВЗД) може да бъде задължително. Администраторите на данни могат да изберат да използват други инструменти, като кодекси на поведение и механизми за сертифициране, за да покажат, че спазват принципите за защита на данните.

Можете да се придържате към **етичен кодекс**, изготвен от бизнес асоциация, одобрен от ОЗД. Кодекс на поведение може да придобие валидност в целия ЕС чрез акт за изпълнение на Комисията.

Можете да се придържате към **механизъм за сертифициране,** управляван от един от сертифициращите органи, които са получили акредитация от ОЗД или национален орган по акредитация, или и от двата, както е определено във всяка държава членка на ЕС.

И кодексът за поведение, и механизмът за сертифициране са инструменти, които се използват по избор и следователно от Вашето дружество/организация зависи да реши дали да се придържа към даден кодекс за поведение или да поиска сертифициране. При всички случаи Вашето дружество/организация трябва да следва и спазва ОРЗД, но придържането към такива инструменти може да бъде взето предвид в случай на принудителна мярка срещу вас за нарушение на ОРЗД.

Пример

Застрахователният орган чадър във държавата членка от ЕС, от която е Вашето дружество/организация, има одобрен от надзорния орган кодекс на поведение. Редица конкурентни застрахователни компании се придържат към кодекса. Въпреки че придържането е доброволно, придържането към кодекса помага при доказване на спазването на ОРЗД.

Позовавания

- членове 24, 40 - 43 и 83 и съображения (98), (99), (100), (148), (150) и (151) от ОРЗД.

6. РАЗГЛЕЖДАНЕ НА ИСКАНИЯ НА ГРАЖДАНИТЕ

6.1. Как да се справим с исканията на физически лица, които упражняват правата си за защита на данните?

Отговор

Физическите лица могат да се свържат с Вашето дружество/организация, за да упражнят своите права съгласно ОРЗД (права за достъп, коригиране, изтриване, преносимост и др.). Когато личните данни се обработват по електронен път, Вашето дружество/организация трябва да предостави средства за подаване на искания по електронен път. Вашето дружество/организация трябва да отговори на искането без ненужно забавяне и по принцип в рамките на **1 месец от получаването на искането.**

То може да помолите за допълнителна информация, за да потвърди самоличността на лицето, подало искането.

Ако Вашето дружество/организация отхвърли искането, то трябва да информира физическото лице за причините за това и за правото му да подаде жалба до органа по защита на личните данни и да потърси съдебна защита.

Разглеждането на исканията на физическите лица **трябва да се извършва безплатно.** Когато исканията са явно неоснователни или прекомерни, особено поради повтарящия се характер, можете да наложите разумна такса или да откажете да предприемете действия.

Пример

Лице, което е получил достъп до всичките си лични данни преди месец, отново внася същото искане за достъп до същите лични данни. Можете да прецените дали да го информирате, че отхвърляте искането му или да поискате разумна такса.

Позовавания

• членове 12 и 15 - 22 и съображения (59) и (63)--(71) от ОРЗД.

6.2. До какви лични данни и информация дадено физическо лице може да получи достъп при подаване на искане?

Отговор

Когато някой подаде искане за достъп до личните си данни, Вашето дружество/организация трябва:

• да потвърди дали обработва лични данни, отнасящи се до него, или не;

• да предостави копие на личните данни, които съхранява за него;

• да предостави информация за обработването (като например цели, категории лични данни, получатели и т.н.).

Вашето дружество/организация трябва да предостави на физическото лице копие от неговите лични данни безплатно. За всички допълнителни копия обаче може да се изиска разумна такса.

Упражняването на правото на достъп е тясно свързано с упражняването на правото на преносимост на данните − да се даде възможност на физическото лице да предаде данните си на друга организация.

Важно е в известието за поверителност на Вашето дружество/организация ясно да бъдат разграничени едното право от другото. Ето защо двете права трябва да бъдат посочени накратко поотделно.

Пример

Вашето дружество/организация предоставя онлайн услуга за социални мрежи, чрез която физическите лица могат да обменят съобщения и снимки. Потребител се свързва с вас, за да получи достъп до личните си данни и да провери кои лични данни, свързани с него, се обработват от Вашето дружество/организация. Вашето дружество/организация трябва да потвърди, че обработва лични данни, свързани с него, и да предостави копие (като например името, данните за контакти, съобщенията и разменените снимки). Вашето дружество/организация трябва също да му предостави информация за обработването − обикновено тя ще бъде включена в известието за поверителност на вашата услуга.

Позовавания

• член 15 и съображения (63) и (64) от ОРЗД.

6.3. Винаги ли трябва да изтриваме личните данни, ако дадено лице поиска това?

Отговор

Общият регламент относно защитата на данните (ОРЗД) дава право на **физическите лица**

да поискат данните им да бъдат изтрити, а организациите имат **задължението да го направят, освен** в следните случаи:

- личните данни, с които Вашето дружество/организация разполага, са необходими за упражняване на правото на свобода на изразяване;
- съществува правно задължение за съхраняване на данните;
- поради причини от обществен интерес (например обществено здраве, научни, статистически или исторически изследователски цели).

Ако Вашето дружество/организация е обработило незаконно данни, то трябва да ги изтрие. По отношение на физическо лице, данните, събрани докато то все още е било непълнолетно, следва да се заличат.

Що се отнася до „правото да бъдеш забравен“ онлайн, от организациите се очаква да предприемат разумни действия (напр. технически мерки), за да информират други уебсайтове, че дадено лице е поискало изтриването на личните му данни.

Данните също така могат да се съхраняват, ако са претърпели подходящ процес на анонимизиране.

Примери

Данните не трябва да се изтриват

Вашето дружество/организация ръководи онлайн вестник. Един от вашите журналисти публикува история за това как един политик е изпрал пари в офшорни банки. Политикът моли да премахнете историята, защото се обработват личните му данни. Доколкото личните данни се използват с цел упражняване на правото на свобода на изразяване, Вашето дружество/организация по принцип не е длъжно да изтрива тези данни. Това обаче ще зависи от действащото национално законодателство.

Данните трябва да се изтриват

Вашето дружество/организация управлява социална медийна платформа. Непълнолетен качва снимки; обаче няколко години по-късно той решава, че въпросните снимки потенциално увреждат перспективите му за кариера. Тъй като физическото лице е било непълнолетно по време на качването на снимките, Вашето дружество/организация е длъжно да изтрие въпросните снимки. Освен това, ако снимките са обработени на други уебсайтове, Вашето дружество/организация трябва да предприеме разумни стъпки, за да ги информирате, че е подадена заявка за изтриване на снимките.

Позовавания

- член 17 и съображения (65) и (66) от ОРЗД;
- Насоки на работната група по член 29 относно изпълнението на решението на Съда на Европейския съюз от 13 май 2014 г. по дело *Google Spain and Google*, C-131/12, ECLI:EU:C:2014:317[1] (WP 225).

6.4. Какво ще стане, ако някой възрази срещу обработването на личните му данни от страна на моето дружество?

Отговор

Физическите лица **имат право да възразят срещу обработването на лични данни,** ако посочат конкретни причини, които ги засягат. Ако възникне такава особена ситуация, тя трябва да бъде разгледана индивидуално и може да бъде засегната от променени обстоятелства, промени в качеството на интервенцията или нова ситуация на опасност.

Физическите лица могат да повдигнат възражение само в случаите, когато публична администрация обработва данните в контекста на нейните обществени задачи или когато дадено дружество обработва данните въз основа на законните си интереси. В такива случаи вече не можете да обработвате данните, освен ако не докажете, че трябва да ги обработвате по причини, които имат преимущество пред правата и свободите на лицето, или ако имате нужда от данните за установяване, упражняване или защита на правни искове.

Лицата също имат право да възразят по всяко време на обработката на личните им данни за целите на **директния маркетинг**. Съгласно Общия регламент относно защитата на данните под „директен маркетинг“ се разбира всяко действие от страна на дадено дружество да разпространява рекламни или маркетингови материали, насочени към конкретни лица. Трябва да информирате физическите лица в известието си за поверителност или най-късно по време на първата комуникация с физически лица, че ще използвате личните им данни за директен маркетинг и че те безплатно имат право да се противопоставят. Когато дадено лице възрази срещу обработването за целите на директния маркетинг, вече не можете да обработвате личните му данни за тези цели.

Пример

В застрахователния сектор много често личните данни са необходими за защита на правни искове в случай на мерки за борба с измамите или срещу прането на пари. В тези случаи застрахователните компании могат да откажат да се съобразят с възражението на дадено лице поради основания, които имат преимущество пред правата и свободите на лицето.

Позовавания

- член 21 и съображения (69) и (70) от ОРЗД;
- Становище 06/2014 на работната група по член 29 относно понятието за законни интереси на администратора на лични данни съгласно член 7 от Директива 95/46/ЕО.

6.5. Могат ли хората да поискат данните им да бъдат прехвърлени на друга организация?

Отговор

Да, **физическите лица имат право да получат** от вашето дружество/организация личните данни, които са ви предоставили, в структуриран, машинночитаем формат и да ги предават на друго дружество/организация (право на преносимост на данните). Правото може да се упражнява само когато личните данни са събрани в контекста на договор или въз основа на съгласие и тези данни се обработват с автоматични средства.

Пример

Пациент от частна клиника в Белгия се премества в друга клиника в Германия. Лицето иска от белгийската клиника, която има електронни файлове за него, да му предостави личните му данни в структуриран, машинночитаем формат, за да може да предаде данните на съответните здравни специалисти в Германия. Белгийската клиника трябва да му предостави личните данни в често използван отворен формат (например XML, JSON, CSV и т.н.). Когато избира формат на данните, организацията трябва да вземе под внимание как този формат би повлиял или възпрепятствал правото на физическото лице да използва повторно данните. Например предоставянето на физическо лице на PDF версии на неговото досие може да не е достатъчно, за да се гарантира, че личните данни лесно ще се използват повторно.

Позовавания

- член 20 и съображение (68) от ОРЗД;
- Насоки на работната група по член 29 относно преносимостта на данните.

6.6. Има ли ограничения за използването на автоматизирано вземане на решение?

Отговор

Да, **физическите лица не трябва да са обект на решение, което е основано единствено на автоматизирано обработване** (като например алгоритми) и което е правно обвързващо или ги засяга значително.

Може да се счита, че дадено решение има правни последици, когато се засягат законните права или правният статус на лицето (например правото на глас). Освен това обработването може значително да засегне дадено лице, ако влияе върху обстоятелствата, в които се намира лицето, неговото поведение или неговия избор (например автоматизираното обработване може да доведе до отказ на онлайн заявление за кредит).

Използването на автоматизирано обработване за вземане на решение се разрешава само в следните случаи:

- решението, основаващо се на алгоритъм, е необходимо (т.е. не трябва да има друг начин за постигане на същата цел) за сключването или за изпълнението на договор с физическото лице, чиито данни сте обработвали чрез алгоритъма (напр. заявление за онлайн заем);

- конкретна част от законодателството на ЕС или национален закон позволява използването на алгоритми и предвижда подходящи гаранции за защита на правата, свободите и законните интереси на физическите лица (например регламенти за избягване на данъчно облагане);

- физическото лице изрично е дало съгласието си за решение въз основа на алгоритъма.

Взетото решение обаче трябва да защитава правата, свободите и законния интерес на физическите лица чрез прилагане на подходящи предпазни мерки. Освен в случаите, когато вземането на такива решения се основава на закон, физическото лице трябва да бъде информирано най-малкото за i) логиката на процеса на вземане на решение; ii) правото му да получи човешка намеса; iii) потенциалните последици от обработката; и iv) правото му да оспори решението. Следователно Вашето дружество/организация трябва да предприеме необходимите процедурни мерки, за да позволи на лицето да изрази своята гледна точка и да оспори решението.

И накрая, трябва да обърнете специално внимание, ако вашият алгоритъм използва специални категории лични данни: автоматизираното вземане на решения е разрешено само при определени условия:

- ако физическото лице е дало изричното си съгласие и/или

- ако обработването е необходимо поради значими обществени интереси в съответствие със законодателството на ЕС или националното законодателство.

Освен това, ако лицето е дете, по принцип трябва да избягвате вземането на решения изцяло въз основа на автоматизирано обработване, което поражда правни последици или последици, които имат подобни съществено значение за децата, тъй като те представляват по-уязвима група от обществото.

Пример

Вашето дружество/организация е онлайн банка, която предлага заеми. Клиентите въвеждат данните си и алгоритъмът извежда резултати за това дали трябва да предложите на клиента заем или не, както и предложения лихвен процент. Вашето дружество/организация трябва да прегледа това решение, преди да го съобщи на бъдещия клиент, и трябва да го информира, че той може да изрази своето мнение и евентуално да оспори вашето решение, като се има предвид, че лицето има право да не бъде обект на решение, базирано на алгоритми.

Позовавания

• член 4, параграф 4 и член 22 и съображения (71) и (72) от ОРЗД;

• Насоки на работната група по член 29 относно автоматизираното вземане на индивидуални решения и профилиране за целите на Регламент (ЕС) 2016/679 (WP 251).

7. ИЗПЪЛНЕНИЕ И САНКЦИИ

7.1. Изпълнение

7.1.1. Каква е ролята на органа за защита на данните?

Отговор

Една от ролите на ОЗД е да **публикува експертни съвети** по въпросите на защитата на данните. Той информира широката общественост относно правата и задълженията, свързани със защитата на данните, и по-специално с Общия регламент относно защитата на данните (ОРЗД). Един уместен пример е задължението, наложено на ОЗД да изготвят и да публикуват списък на операциите по обработка, които изискват оценка на въздействието върху защитата на данните. Някои ОЗД вече са създали ръководства и други инструменти, които да помогнат на бизнеса да разбере задълженията си по ОРЗД, а на физическите лица да разберат правата си. Освен това работната група по член 29, която е групата на националните европейски органи за защита на данните (която ще бъде заменена от Европейския комитет за защита на личните данни), е изготвила редица документи за тълкуване на разпоредбите на закона за защита на данните. ОЗД обаче не може да дава съвети в отделни случаи или да замени компетентен адвокат.

Не е необходимо да уведомявате ОЗД, че обработвате данни. Въпреки това е необходима **предварителна консултация** с ОЗД, когато **ОВЗД** покаже, че обработването на данните би довело до **висок риск** и остават остатъчни рискове въпреки прилагането на няколко предпазни мерки. Също така **трябва да се свържете с ОЗД в случай на нарушение на сигурността на данните**. За някои конкретни видове обработване на данни националните законодателства все още могат да изискват от вас да получите разрешение от вашия ОЗД.

Пример

Притежавате магазин за продажба на домашни потреби. Обработвате клиентски данни, като адреси за доставка и данни за плащане, които се изискват съгласно естеството на вашата дейност. В този случай не е необходимо да уведомявате ОЗД.

Позовавания

• глава IV, глава VI;

• Насоки на работната група по член 29 относно ОРЗД, по-специално насоките относно ОЗВД и насоките относно уведомленията за нарушение на сигурността на данните

7.1.2. Какво представлява Европейският комитет за защита на личните данни (EDPB)?

Отговор

EDPB е орган на ЕС, който ще отговаря за прилагането на Общия регламент относно защитата на данните (ОРЗД) от 25 май 2018 г. Той е съставен от ръководителя на всеки ОЗД и на Европейския надзорен орган по защита на данните (EDPS) или техни представители. Европейската комисия участва в заседанията на EDPB без право на глас. Секретариатът на EDPB ще бъде осигурен от EDPS.

EDPB ще бъде в центъра на новата рамка за защита на данните в ЕС. Той ще помогне да се гарантира, че законът за защита на данните **се прилага съгласувано в целия ЕС** и ще работи за

осигуряване на **ефективно сътрудничество** между органите по защита на данните. Комитетът не само ще **издава насоки** за тълкуването на основните понятия на ОРЗД, но също така ще бъде призован **да се произнася с обвързващи решения по спорове** относно трансграничното обработване, като по този начин ще се осигури еднакво прилагане на правилата на ЕС, за да се избегне възможността един и същ случай да се разглежда различно от различните юрисдикции.

Позовавания

• членове 63−76 и съображения (135)−(140) от ОРЗД.

7.1.3. Какво ще стане, ако обработваме данни в различни държави на ЕС?

Отговор

Общият регламент относно защитата на данните (GDPR) се прилага в целия ЕС − един набор от правила за защита на данните за всички държави. Това улеснява вашето дружество и то не трябва да се съобразява с няколко различни закона. В някои области държавите − членки на ЕС, могат допълнително да уточнят прилагането на правилата на GDPR (напр. правила за заетост, сектора на общественото здравеопазване, правила за съгласуване на свободата на изразяване със защитата на данните). Също така GDPR въвежда така наречения механизъм за обслужване на „едно гише“, който осигурява сътрудничество между органите за защита на данните (ОЗД) в случай на трансгранично обработване.

Ако обработвате данни в **различни държави**, компетентният ОЗД − който ще бъде **водещият орган** в преговорите с други заинтересовани ОЗД в ЕС − е **ОЗД на държавата − членка на ЕС, в която се намира главният ви офис.** Това е централната ви администрация в ЕС, където се вземат решения относно целите и средствата за обработване на лични данни и където е правомощието за изпълнение на тези решения. Ако нямате централна администрация в ЕС, главният ви офис ще бъде мястото, където се извършва ефективното и реалното осъществяване на управленски дейности, които определят основните решения относно целите и средствата за обработване.

Ако обработвате данни, за да изпълнявате национално правно задължение, компетентен е само ОЗД на тази държава от ЕС.

Пример

Главното управление на текстилно предприятие (т.е. неговото седалище) се намира в Италия. То разполага с верига от магазини в съседни държави, като Малта, Гърция, Франция и Австрия. В тези съседни държави магазините от неговата верига създават бази данни, които обработват личните данни на клиентите за маркетингови цели. Решенията за това „как“, „кога“ и „защо“ да се осъществи контакт с посочените клиенти се вземат в централата в Италия. Така, в този случай решението за обработването на лични данни за маркетингови цели се счита за направено в Италия. Италианският ОЗД е водещият орган на вашето предприятие.

Позовавания

• Насоки на работната група по член 29 относно водещия надзорен орган и приложението към тях (Често задавани въпроси), 5 април 2017 г.;

• член 4, параграф 23, членове 55, 56, 60−70; съображения 124−140.

7.2. Санкции

7.2.1. Какво ще стане, ако не спазим правилата за защита на данните?

Отговор

Общият регламент относно защитата на данните (GDPR) предоставя различни инструменти на органите за защита на данните в случай на неспазване на правилата за защита на данните:

• вероятно нарушение − например може да бъде издадено **предупреждение**;

• нарушение: възможностите включват порицание, временна или окончателна забрана за обработването и глоба до 20 милиона евро или 4 % от общия годишен световен оборот на бизнеса.

Струва си да се отбележи, че в случай на нарушение ОЗД може да наложи парична глоба вместо или в допълнение към порицанието и/или забраната за обработване.

Органът трябва да гарантира, че глобите, наложени във всеки отделен случай, са **ефективни, пропорционални** и **възпиращи**. Той ще вземе предвид редица фактори, като естеството, тежестта и продължителността на нарушението, умишления или небрежния му характер, всяко действие, предприето за смекчаване на претърпените от физическите лица щети, степента на сътрудничество на организацията и т.н.

Пример

Дружество продава онлайн домашни потреби. Чрез този уебсайт потребителите могат да купуват кухненски уреди, маси, столове и други битови стоки, като въвеждат банкови данни. Уебсайтът претърпява кибернетична атака, в резултат на която атакуващият придобива достъп до личните данни. В този случай липсата на подходящи технически мерки от страна на дружеството изглежда е причината за загубата на данни.

В този случай надзорният орган ще вземе под внимание различни фактори, преди да вземе решение кое коригиращо средство да се използва. Фактори, като: колко сериозни са били пропуските в ИТ системата? Колко време ИТ инфраструктурата е била изложена на такъв риск? Провеждани ли са тестове в миналото, за да се предотврати подобна атака? На колко клиенти данните са били откраднати/разкрити? Какъв тип лични данни са били засегнати − имало ли е чувствителни данни? Всички тези и други съображения ще бъдат взети предвид от надзорния орган.

Позовавания

• членове 58, 60, 83, 84; съображения 129, 148, 150, 151;

• Насоки на работната група по член 29 относно прилагането и определянето на административни глоби за целите на Регламент 2016/679, 3 октомври 2017 г.

7.2.2. Може ли дружеството/организацията ми да носи отговорност за щети?

Отговор

Физическите лица могат да предявят иск за обезщетение, ако дадено дружество или организация наруши Общия регламент относно защитата на данните (ОРЗД) и те са понесли материални щети (например финансови загуби) или неимуществени щети (например загуба на репутация или психологически стрес). ОРЗД гарантира, че ще им бъде предоставено обезщетение, независимо от броя на организациите, участващи в обработването на техните данни. Обезщетение може да бъде предявено директно от организацията или пред компетентните национални съдилища. Производства се образуват пред съдилищата на държавата от ЕС, в която е установен администраторът или обработващият данни, или в която живее гражданинът, претендиращ за обезщетение (в която е неговото обичайно местопребиваване).

Позоваване

• член 82 и съображения (146) и (147) от ОРЗД.

ИНФОРМАЦИОННО-РАЗЯСНИТЕЛНА ДЕЙНОСТ НА ЕВРОПЕЙСКАТА КОМИСИЯ. ПРАВА НА ГРАЖДАНИТЕ.“

На 24 януари 2018 г. Европейската Комисия стартира онлайн инструмент с практическа насоченост, който да помага на гражданите да се възползват от новите правила за защита на данните и да упражняват правата си.

В настоящия брой публикуваме съдържанието на инструмента „Права на гражданите“. В него Европейската комисия уточнява, че публикуваните информация и насоки са *„само средство за ориентиране — само текстът на Общия регламент относно защитата на данните (ОРЗД) има правна сила. Следователно само ОРЗД може да създава права и задължения за физическите лица. Тези насоки не пораждат никакви права или очаквания, подлежащи на изпълнение. Обвързващото тълкуване на законодателството на ЕС е от изключителната компетентност на Съда на Европейския съюз. Гледните точки, изразени в настоящите насоки, не изключват позицията, която може да заеме Комисията пред Съда. Нито Европейската комисия, нито лице, действащо от името на Европейската комисия, носи отговорност за използването на следната информация. Тъй като тези насоки отразяват състоянието на техниката в момента на изготвянето им, те следва да се разглеждат като „жив инструмент“, отворен за усъвършенстване, и съдържанието им може да бъде предмет на изменения без предизвестие*.“

Този инструмент е достъпен онлайн ТУК.

ПРАВА НА ГРАЖАНИТЕ

Научете как са защитени личните ви данни, какви са правата ви, които ви помагат да си върнете контрола върху вашите лични данни и какво да направите при възникване на проблем.

1. <u>КАК СА ЗАЩИТЕНИ ЛИЧНИТЕ МИ ДАННИ?</u>

1.1. Как са защитени данните за моите религиозни убеждения/сексуална ориентация/здравословно състояние/политически възгледи?

Отговор

Следните специални категории лични данни се считат за „чувствителни“ и получават специална защита съгласно Общия регламент относно защитата на данните (ОРЗД):

- расов или етнически произход;
- политически възгледи;
- религиозни или философски убеждения;
- членство в професионална организация;
- обработване на генетични данни;
- биометрични данни с цел уникалната ви идентификация като физическо лице;
- здравословно състояние;
- сексуален живот или сексуална ориентация.

Общото правило е, че обработването на типовете данни, изброени по-горе, е **забранено**. Съгласно някои дерогации обаче на дружество/организация може да бъде позволено да обработва чувствителни лични данни, когато например:

- явно сте направили вашите чувствителни данни обществено достояние;
- сте дали изричното си съгласие;
- закон урежда специален вид обработване на данни за конкретна цел от обществен интерес или касаеща здравословното състояние;
- закон, включващ адекватни гаранции, предвижда обработването на чувствителни лични данни в области, като общественото здраве, заетостта и социалната закрила.

Пример

Националният статистически институт (държавна организация) организира публично преброяване на населението на всеки 5 години. Получавате препратка към проучване, което сте задължени да попълните. То съдържа полета, като например пол и расов или етнически произход. В такава хипотеза, тъй като проучването се основава на закон, който служи на цели от обществен интерес и съдържа гаранции за защита на Вашите чувствителни данни (например достъп до данните имат само упълномощени получатели, работещи по преброяването), Вашите чувствителни лични данни могат да бъдат обработени от Националния статистически институт.

Позовавания

- член 9 и съображения (51)—(56) от ОРЗД.

1.2. Може ли да се събират лични данни на деца?

Отговор

Налице е допълнителна защита за този тип лични данни, тъй като децата не познават достатъчно добре рисковете и последиците от споделянето на данни, както и своите права. Всяка информация, насочена специално към деца, трябва да се адаптира така, че да бъде **лесно достъпна, като се използват ясни и недвусмислени формулировки.**

За повечето онлайн услуги се изисква **съгласието на родителя или настойника**, за да се обработят личните данни на детето въз основа на съгласието до определена възраст. Това важи за сайтовете за социални контакти, както и за платформи за изтегляне на музика и купуване на онлайн игри.

Възрастовата граница за получаване на съгласието на родителите се определя от всяка държава членка на ЕС и може да варира между 13 и 16 години. Консултирайте се с Вашия **национален орган за защита на данните**.

Дружествата трябва да положат разумни усилия, като вземат предвид наличната технология, за да проверят дали даденото съгласие действително е в съответствие със закона. Това може да включва мерки за проверка на възрастта (така например задаване на въпрос, на който едно дете не би могло да отговори, или да се поиска непълнолетното лице да предостави имейла на родителя си, за да се даде възможност за писмено съгласие).

Пряко предлаганите на деца услуги за превенция и консултиране не изискват съгласието на родител, тъй като те имат за цел да защитят висшите интереси на детето.

Примери

Необходимо е съгласието на родител

Имате 12-годишна дъщеря. Тя би искала да се присъедини към популярна социална медийна мрежа и е помолена за съгласие за обработване на информацията за нейната религиозна принадлежност.

Вие трябва да дадете съгласието си, в случай че искате тя да се присъедини към тази социална мрежа.

Не е необходимо съгласието на родител

Вашият 17-годишен син възнамерява да участва в онлайн проучване за моделите на потребление на дрехи. Сайтът изисква съгласие за обработване на данните му. Тъй като е навършил 16 години, той може да даде своето съгласие, без да поиска вашето.

Позовавания

• член 8 и съображения (38) и (58) от ОРЗД.

1.3. Може ли работодателят ми да ме накара да дам съгласието си да използва личните ми данни?

Отговор

Взаимоотношението работодател—служител обикновено се счита за небалансирано взаимоотношение, при което работодателят има повече правомощия от служителя. Тъй като съгласието трябва да бъде дадено свободно и в контекста на небалансираното взаимоотношение, вашият работодател в повечето случаи не може да разчита на вашето съгласие да използва данните ви.

Възможно е да има ситуации, при които обработването на личните данни на служител въз основа на съгласието му да е законосъобразно — особено ако това е в интерес на служителя. Например ако дадено дружество отпуска обезщетения на служителя или членовете на семейството му (например отстъпки за услугите на дружеството), обработването на личните данни на служителя е разрешено и законно, ако е било дадено информирано предварително съгласие.

Пример

Невалидно съгласие

Вашият работодател вярва, че трябва да се подобри производителността на труда. За да направи това, той възнамерява да инсталира камери за видеонаблюдение в коридорите и на входа на хигиенно-санитарните помещения. Той ви моли да дадете съгласието си, за да може да наблюдава движението Ви и времето, прекарано извън офиса. Дори да дадете съгласието си, то ще се счита за невалидно и Вашият работодател не може да инсталира камера за видеонаблюдение въз основа на това съгласие.

Позовавания

• членове 7 и 88 и съображение (43) от ОРЗД;

• Насоки на работната група по член 29 относно съгласието съгласно Регламент (ЕС) 2016/679 (WP 259);

• Становище 2/2017 на работната група по член 29 относно обработването на данни на работното място (WP 249).

1.4. Как трябва да се поиска съгласието ми?

Отговор

Искането за съгласие трябва да бъде представено **ясно и кратко**, като се използва лесен за разбиране език, и да бъде **ясно отличимо** от останалата информация, като например общите условия. Искането трябва да уточнява **за какво ще се използват личните ви данни** и да съдържа данни за контакт с дружеството, което ще обработва данните. Съгласието трябва да бъде **свободно дадено и да бъде конкретно, информирано** и недвусмислено. „Информирано съгласие“ означава, че трябва да получите информация за обработването на Вашите лични данни, в това число най-малко:

• идентичността на организацията, обработваща данните;

• целите, за които се обработват данните;

• вида на данните, които ще бъдат обработени;

• възможността за оттегляне на съгласието (пример: чрез изпращане на имейл за оттегляне на съгласието);

• където е приложимо, фактът, че данните ще се използват само за автоматизирано вземане на решения, включително профилиране;

• информация относно това дали съгласието е свързано с международно предаване на Вашите данни, възможните рискове от предаването на данните към държави извън ЕС, ако по отношение на тези държави няма прието решение на Комисията относно адекватното ниво на защита и не са налице подходящи гаранции.

Примери

Съгласно закона не се изисква съгласие

Записвате се в музикално училище на курс по пиано. Формулярът за записване съдържа дълъг документ, написан с малък шрифт и в който се използват строго правни и технически термини; той представя възможността училището да предаде Вашите лични данни на търговците на дребно на музикални инструменти. Училището е в нарушение на закона, тъй като Вашето съгласие за получаване на маркетингов материал (потенциално от търговци на дребно на инструменти) не Ви е било поискано, както е предвидено в закона.

Откривате банкова сметка онлайн и искате да потвърдите заявката си. Показва се страница с две полета за отметка, които гласят „Приемам общите условия“ и „Съгласен съм с това, че решението за правото ми на кредитна карта ще се основава единствено на профилиране без човешка намеса.“ И двете полета за отметка са активирани (отметнати) по подразбиране. Трябва да деактивирате полето за отметка, ако не искате да сте субект на решение относно правото Ви на кредитна карта, изготвено единствено въз основа на профилиране. Дори и да не деактивирате полето за отметка, банката не би получила валидно съгласие, тъй като предварително маркираните полета не се считат за валидно съгласие съгласно ОРЗД.

Позовавания

• членове 6 и 7; съображения (42) и (43) от ОРЗД;

• Насоки на работната група по член 29 относно съгласието съгласно Регламент (ЕС) 2016/679 (WP 259).

1.5. Какво се случва, ако данните, които съм споделил, са изтеглени?

Отговор

Налице е нарушение на личните данни, когато има нарушение на сигурността, което води до случайно или незаконно унищожаване, загуба, промяна, неразрешено разкриване или достъп до обработени лични данни. Ако това се случи, организацията, която съхранява личните данни, трябва да уведоми надзорния орган без ненужно забавяне. Когато има вероятност нарушението на сигурността на личните данни да доведе до висок риск за вашите права и свободи и рискът не е бил смекчен, тогава вие, като физическо лице, също трябва да бъдете информирани.

Пример

Резервирали сте си такси чрез онлайн приложение. Дружество за таксиметрови услуги е претърпяло масово нарушение на сигурността на личните данни, а данните на водачите и потребителите са били откраднати. Изглежда, че не е била въведена специална мярка за сигурност, която да защитава

личните данни. Дружеството би трябвало да ви информира за нарушението. В този случай можете да подадете жалба срещу дружеството пред националния орган за защита на данните (ОЗД).

Позовавания

• членове 32, 33 и 34 и съображения (85) - (88) от ОРЗД.

2. МОИТЕ ПРАВА

2.1. Какви са правата ми?

Отговор

Имате право:

• да получите **информация** за обработването на Вашите лични данни;

• **да получите достъп** до съхраняваните за Вас лични данни;

• да поискате неправилните, неточните или непълните лични данни да бъдат **коригирани**;

• да поискате личните **данни да бъдат изтрити,** когато вече не са необходими или ако обработването им е незаконно;

• **да възразите** срещу обработването на вашите лични данни за целите на маркетинга или на основания, свързани с Вашата конкретна ситуация;

• да поискате **ограничаване** на обработването на личните Ви данни в конкретни случаи;

• да получавате личните си данни в пригоден за машинно четене формат и да ги изпращате на друг администратор („**преносимост на данните**“);

• да поискате решенията, основаващи се на **автоматизирано обработване**, които Ви засягат или значително ви засягат и са въз основа на вашите лични данни, да бъдат направени от физически лица, а не само от компютри. Вие също така имате право в този случай да изразите Вашата гледна точка и да оспорите решението.

За да упражните правата си, трябва да се свържете с дружеството или организацията, която обработва личните Ви данни (т.е. администратора). Ако дружеството/организацията има служител по защита на данните (СЗД),

можете да отправите искането си към този СЗД. Дружеството/организацията трябва да отговори на исканията Ви без ненужно забавяне и **най-късно до 1 месец**. Ако дружеството/организацията не възнамерява да изпълни искането Ви, то трябва да посочи причината. Може да бъдете помолени да предоставите информация, за да потвърдите самоличността си (например като щракнете върху връзка за потвърждение, като въведете потребителско име или парола), за да упражните правата си.

Тези права се прилагат **в целия ЕС**, независимо от това къде се обработват данните и къде е установено дружеството. Тези права също така се прилагат и когато купувате стоки и услуги от дружества извън ЕС, които извършват дейност в ЕС.

Позоваване

• глава III от ОРЗД.

2.2. Каква информация трябва да получа, когато предоставям данните си?

Отговор

Когато предоставяте личните си данни, трябва да получите, наред с останалото, информация за:

• **името** на дружеството или организацията, която обработва данните Ви (включително данните за контакт на СЗД, ако има такъв);

• **целите**, за които дружеството/организацията ще използва данните Ви;

• категориите на съответните лични данни;

• правното основание за обработване на личните Ви данни;

• **продължителността** от време, през което ще бъдат съхранявани данните Ви;

• **други дружества/организации**, които ще получат данните Ви;

• дали данните ще бъдат **прехвърлени извън ЕС;**

• Вашите **основни права** в областта на защитата на данни (напр. правото на достъп и прехвърляне на данни или да бъдат премахнати);

• **правото за подаване на жалба** до орган за защита на данните (ОЗД);

• **правото да оттеглите съгласието** си по всяко време;

• наличието на автоматизирано вземане на решения

• и съответната логика, включително последиците от това.

Информацията трябва да бъде представена по **сбит, прозрачен, разбираем начин** и формулирана ясно и недвусмислено.

Позовавания

• членове 12 и 13 и съображения (60) - (62) от ОРЗД;

• Насоки на работната група по член 29 относно прозрачността съгласно Регламент (ЕС) 2016/679 (WP 260).

2.3. Как мога да получа достъп до личните си данни, с които разполага дадено дружество/организация?

Отговор

Имате право да поискате и да получите от дружеството/организацията потвърждение дали притежава лични данни, които ви засягат.

Ако имат личните ви данни, вие имате **право на достъп до тези данни**, да **получите копие** и всякаква **подходяща допълнителна информация** (като например причината за обработване на личните ви данни, използваните категории лични данни и др.).

Това право на достъп трябва да е **лесно** и да е възможно на „разумни интервали“. Дружеството/организацията трябва да ви предостави **безплатно** копие на личните ви данни. Всяко допълнително копие може да бъде предмет на разумна такса. Когато заявката се подава по електронен път (например чрез електронна поща) и освен ако не сте поискали друго, информацията трябва да бъде предоставена в често използвана електронна форма.

Това право не е абсолютно: използването на правото на достъп до Вашите лични данни не следва да засяга правата и свободите на другите, включително търговската тайна или интелектуалната собственост.

Примери

Право на достъп

Заемате книги от библиотека. Можете да поискате от библиотеката да Ви предостави касаещите Ви лични данни, с които разполага. След това библиотеката трябва да Ви предостави цялата информация относно Вас, която съхранява. Например: кога за пръв път сте започнали да използвате услугите на библиотеката; кои книги сте вземали; дали сте имали просрочена книга и глоби, които може да са Ви били наложени.

Абонирали сте се за схема за карти за лоялност на търговска верига със супермаркети в различни части на града и държавата. Ако използвате правото си да поискате информация и да получите Вашата лична информация, съхранявана от схемата за карти за лоялност, трябва да получите информация относно това например колко често сте използвали картата; в кои супермаркети сте пазарували; всички отстъпки, които сте получили, и дали сте били набелязани като клиент чрез използване на техники за профилиране (и как); дали супермаркетът, който е част от многонационална верига от дружества, е разкрил данните Ви на свързано с него дружество, което продава парфюми и козметика.

Позовавания

- член 15 и съображения (63), (64) от ОРЗД.

2.4. Данните ми са неправилни: мога ли да ги коригирам?

Отговор

Ако смятате, че личните Ви данни може да са неверни, непълни или неточни, можете да помолите дружеството или организацията да ги коригира. Те трябва да направят това без ненужно забавяне (по принцип в рамките на 1 месец) или писмено да обосноват причината, поради която молбата не може да бъде уважена.

Пример

Кредитно бюро обработва информацията, предоставена му от бившия Ви хазяин, която гласи, че Вие дължите наем за три месеца. Наскоро сте спечелили правен спор и претенцията му за тримесечния наем е обявена за неоснователна. Можете да поискате от кредитното бюро да коригира данните, които разполага за вас, така че да не бъдете поставяни в неблагоприятно положение в бъдеще, когато се обработват искания за кредит.

Позовавания

- членове 12, 16, 19 и 23; съображение (65) от ОРЗД.

2.5. Мога ли да помоля дадено дружество/организация да ми изпрати личните ми данни, за да мога да ги използвам на друго място?

Отговор

Ако дадено дружество обработва вашите лични данни въз основа на ваше съгласие или договор, можете да го помолите да предаде вашите лични данни на вас.

Можете също така да поискате личните ви данни да бъдат предадени директно на друго дружество, чиито услуги искате да използвате, когато това е технически осъществимо.

Пример

Вие сте член на онлайн социална медийна мрежа. Решавате, че една нова конкурентна социална медийна мрежа е по-подходяща за Вашите цели и възрастова група. Можете да поискате от онлайн социалната медийна мрежа да пренесе личните Ви данни, включително снимките Ви, в новата социална медийна мрежа.

Позовавания

- член 20 и съображение (68) от ОРЗД;
- Насоки на работната група по член 29 относно правото на преносимост на данните, приети на 13 декември 2016 г., последно преработени и приети на 5 април 2017 г. (WP 242, рев. 01)

2.6. Мога ли да помоля дадено дружество/организация да спре обработването на личните ми данни?

Отговор

Имате **право да възразите** срещу обработването на личните Ви данни и да поискате от дружеството/организацията да прекрати обработването на Вашите лични данни, ако те се обработват с цел:

- **директен маркетинг;**
- за **научни/исторически изследвания** и **статистически данни;**
- за неин собствен **законен интерес** или при изпълняване на задача от **обществен интерес**/ при упражняване на официално правомощие.

Ако не сте съгласни с директния маркетинг, дружеството трябва да прекрати използването на личните Ви данни и да се съобрази с искането Ви, без да иска такса.

Дадено дружество/организация може обаче да продължи да обработва Вашите лични данни въпреки възраженията Ви, ако:

- в случай на обработване за целите на научни/исторически изследвания и статистически цели, обработването е необходимо за изпълнението на задача, осъществявана по причини от обществен интерес;
- в случай на обработване въз основа на законни интереси или изпълнение на задача от обществен интерес/упражняване на официални правомощия, тя може да докаже, че има убедителни законови основания, които имат преимущество над вашите интереси, права и свободи. Ето защо е необходимо балансирано изпълнение.

Дружеството трябва да ви информира за правото Ви на възражение, когато се свърже с Вас за първи път.

Пример

Купили сте два билета от онлайн дружество за продажба на билети, за да гледате любимата си група на живо. След това сте засипани с реклами за концерти и събития, които не ви интересуват. Информирате онлайн дружеството за продажба на билети, че не желаете да получавате допълнителни рекламни материали. Дружеството трябва да прекрати обработването на личните Ви данни за директен маркетинг и скоро след това да спрете да получавате имейли от него. За това то не трябва да Ви налага такса.

Позовавания

- членове 7, 12 и 21 и съображения (69) и (70) от ОРЗД.

2.7. Мога ли да помоля дадено дружество да изтрие личните ми данни?

Отговор

Да, можете да поискате личните Ви данни да бъдат изтрити, когато например данните, които дружеството съхранява за Вас, вече не са необходими или когато данните Ви са били използвани незаконно. Лични данни, предоставени, когато сте били дете, могат да бъдат изтрити във всеки един момент.

Това право се прилага и **онлайн** и често се нарича **„правото да бъдеш забравен“**. При конкретни обстоятелства можете да поискате от дружествата, които са направили личните Ви данни достъпни онлайн, да ги изтрият. Тези дружества също така са задължени да предприемат разумни

стъпки, с които да информират другите дружества (администратори), които обработват личните данни, че субектът на данни е поискал изтриване на всички връзки или копия от тези лични данни.

Трябва да се има предвид, че това право не е абсолютно право, което означава, че и други права, като например свободата на изразяване на мнение и правото на научни изследвания, също са гарантирани.

Примери

Данните трябва да бъдат изтрити

Присъединили сте се към сайт за социални контакти. След известно време решавате да напуснете сайта за социални контакти. Имате право да поискате от дружеството да изтрие Вашите лични данни.

Данните не могат да бъдат изтрити веднага

Нова банка предлага добри сделки за жилищни кредити. Купувате нова къща и решавате да преминете към новата банка. Искате от „старата“ банка да закрие всичките ви сметки и да изтрие всичките Ви лични данни. Старата банка обаче е подчинена на закон, който задължава банките да съхраняват всички данни за клиентите за период от 10 години. Старата банка не може просто така да изтрие личните Ви данни. В този случай може да поискате ограничаване на обработването на личните Ви данни. След това банката може само да съхранява данните Ви за срока, изискван по закон, и не може да извършва други операции с тях.

Данните трябва да бъдат изтрити

При онлайн търсене с Вашето име и фамилия резултатите показват връзка към статия във вестник. Информацията във вестника датира от няколко години и е свързана с проблем (търг за недвижими имоти, свързан с процедура за събиране на вземания), който е решен отдавна и сега не е от значение. Ако не сте обществено лице и вашият интерес за премахване на статията има превес над интереса на широката общественост да има достъп до информацията, тогава търсачката е длъжна да премахне връзките към уебстраниците, които съдържат Вашето име и фамилия.

Позовавания

- членове 12, 17 и 23; съображения (65) и (66) от ОРЗД;
- Насоки на работната група по член 29 относно изпълнението на решението на Съда на Европейския съюз от 13 май 2014 г., *Google Spain and Google*, C-131/12, ECLI:EU:C:2014:317 (WP 225)

2.8. Кога трябва да упражня правото си на ограничаване на обработването на личните ми данни?

Отговор

Общо погледнато, в случаите, когато не е ясно дали личните данни ще трябва да бъдат изтрити и кога точно ще се случи това, можете да упражните правото си на ограничаване на обработването. Това право може да бъде упражнявано когато:

- точността на въпросните данни е оспорена;
- не искате данните да бъдат изтрити;
- данните вече не са необходими за първоначалната цел, но не могат да бъдат изтрити поради правни основания;
- решението относно Вашето възражение за обработването е висящо.

„Ограничение“ означава, че Вашите лични данни могат — с изключение на съхранението — да бъдат обработвани само с Вашето съгласие за установяване, упражняване или защита на правни искове, за защита на правата на друго физическо или юридическо лице или по причини от обществен интерес на ЕС или на държава членка от ЕС. Трябва да бъдете информирани преди премахването на ограничението.

Пример

Нова банка на вътрешния пазар предлага добри сделки за жилищни кредити. Купувате нова къща и решавате да смените банката. Искате от „старата“ банка да закрие всичките Ви сметки и да изтрие всичките Ви лични данни. Старата банка обаче е подчинена на закон, който задължава банките да съхраняват всички данни за клиентите за период от 10 години. Старата банка е задължена по закон да съхранява данните Ви, но вие все пак можете да поискате ограничаване на обработването на данните, за да сте сигурни, че те няма да се използват „случайно“ за нежелани цели.

Позовавания

- член 18 и съображение (73) от ОРЗД.

2.9. Мога ли да бъда обект на автоматизирано вземане на индивидуални решения, включително профилиране?

Отговор

Профилирането се извършва, когато се оценяват аспекти на личния ви живот, за да се направят прогнози за вас, дори и да не се вземат решения. Например ако дадено дружество или организация направи оценка на вашите характеристики (възраст, пол, височина) или ви класифицира в категория, това означава, че сте профилирани.

Вземане на решения единствено по автоматизиран път е налице когато се вземат решения за Вас чрез технологични средства и без човешко участие. Те могат да бъдат взети дори без профилиране.

Законът за защита на личните данни определя, че имате **право да не сте субект на решение, основано единствено на автоматични средства**, ако решението има правни последици за Вас или Ви засяга значително. Дадено решение има правни последици, когато Вашите законни права са засегнати (като например вашето право на глас). Освен това обработването може значително да Ви засегне, ако влияе върху обстоятелствата, поведението или избора Ви. Например автоматизираното обработване може да доведе до отказ на Ваше онлайн искане за кредит.

Профилирането и автоматизираното вземане на решения са често срещана практика в редица сектори, като банковото дело и финансите, данъчното облагане и здравеопазването. То може да е по-ефективно, но да е по-малко прозрачно и да ограничава избора ви.

Макар че като общо правило може да не сте обект на решение, основано единствено на автоматизирано обработване, този вид вземане на решения може по изключение да бъде разрешено, ако даден закон позволява използването на алгоритми и предвижда подходящи гаранции.

Също така изцяло автоматизирани решения са разрешени, когато:

- решението е необходимо (а именно, не трябва да има друг начин за постигане на същата цел), за да се сключи или да се изпълни договор с вас;
- дали сте изричното си съгласие.

В тези два случая взетото решение трябва да гарантира вашите права и свободи чрез прилагане на подходящи гаранции. Дружеството или организацията трябва най-малкото да ви информира за правото ви да получите човешка намеса и да изпълни необходимите процедурни механизми; освен това дружеството или организацията трябва да ви позволи да изразите своята гледна точка и да ви информира, че можете да оспорвате решението.

Решенията, базирани на алгоритми, не могат да използват специални категории данни, освен ако не сте дали съгласието си или обработването не е позволено в съответствие с правото на ЕС или с националното право (вж. по-горе).

Пример

Използвате онлайн банка за заем. От вас се иска да въведете данните си, а алгоритъмът на банката ще ви каже дали банката ще ви отпусне заем, или — не, и ще ви посочи предложения лихвен процент. Трябва да бъдете информирани, че можете: да изразявате мнението си, да оспорвате решението и да поискате решението, направено чрез алгоритъма да бъде прегледано от човек.

Позовавания

- членове 21 и 22 и съображения (71) и (72) от ОРЗД;
- Насоки на работната група по член 29 относно автоматизираното вземане на индивидуални решения и профилиране за целите на Регламент (ЕС) 2016/679 (WP 251).

3. ПРАВНА ЗАЩИТА

3.1. Какво трябва да направя, ако смятам, че правата ми за защита на личните данни са нарушени?

Отговор

Ако смятате, че Вашите права за защита на личните данни са нарушени, пред вас се откриват три възможности:

- **Подаване на жалба до вашия национален орган за защита на данните (ОДЗ).**

Органът извършва разследване и ви информира за напредъка или резултата от жалбата ви в рамките на 3 месеца.

- **Предприемане на правно действие срещу дружеството или организацията**

Подайте иск в съда срещу дружество/организация, ако смятате, че е нарушило правата Ви за защита на данните. Това не Ви спира да подадете жалба до националния ОЗД, ако желаете.

- **Предприемане на правно действие срещу ОЗД**

Ако смятате, че ОЗД не е разгледал жалбата Ви по подходящ начин, ако не сте удовлетворени от отговора му или ако не Ви информира за напредъка или резултата в рамките на 3 месеца от деня на подаване на жалбата, можете да предявите иск срещу ОЗД направо пред съда.

Понякога дружеството, срещу което е подадена жалбата, обработва данни в различни държави членки на Европейския съюз. В този конкретен случай компетентният ОЗД обработва жалбата в сътрудничество с ОЗД, базирани в другите държави членки на ЕС. Тази система, наречена механизъм „обслужване на едно гише“, гарантира, че жалбите се обработват по-ефективно. Например той може да помогне жалбата ви да се свърже с подобни жалби, подадени в други държави членки на ЕС. ОЗД, в който сте подали жалбата, е вашето основно звено за контакт.

Пример

Обичате да тичате. Купили сте си часовник, който изчислява сърдечния пулс и скоростта на километър, проследява маршрута ви и събира други подходящи данни. Качили сте всичките си данни на уебсайт. Разбирате, че вашите данни са били объркани с данните на друг. Можете да подадете жалба до ОЗД срещу уебсайта.

Позовавания

- членове 60, 77, 78, 79 и 80 и съображения (141), (143) и (145) от ОРЗД.

3.2. Кои са органите за защита на данните (ОЗД) и как да се свържа с тях?

Отговор

ОЗД са независими публични органи, които следят и упражняват надзор чрез правомощия за разследване и коригиране на прилагането на закона за защита на данните. Те предоставят експертни съвети по въпросите за защита на данните и обработват жалбите, които може да са нарушили закона.

Свържете се с вашия национален орган за защита на данните

Позовавания

- членове 55, 57 и 58 от ОРЗД.

3.3. Може ли неправителствена организация (НПО) да предявява искове от мое име?

Отговор

Имате право да упълномощите една НПО да подаде жалба от Ваше име, когато са изпълнени следните три условия:

1. НПО е учредена в съответствие със закона;

2. НПО преследва цел от обществен интерес (напр. подобряване на живота на гражданите в областта на защитата на потребителите);

3. НПО е активна в областта на защитата на данните.

Жалбата може да бъде подадена както пред съответния **орган за защита на данните**, така и при необходимост пред съдебен орган. В някои държави членки от ЕС националното законодателство допуска НПО да подаде жалба, без да сте я упълномощили за това.

Позовавания

- член 80 и съображение (142) от ОРЗД.

3.4. Мога ли да предявя иск за обезщетение?

Отговор

Можете да предявите иск обезщетение, ако дадено дружество или организация не са спазили закона за защита на данните и сте претърпели материални щети (напр. финансови загуби) или неимуществени вреди (напр. страдание или загуба на репутация). Можете да предявите иск пред съответното дружество или организация или пред националните съдилища. Можете да предявите иск за обезщетение пред съдилищата в държавата членка на ЕС, където се намира администраторът или обработващият данните. Като алтернатива такова производство може да бъде образувано пред съдилищата на държавата членка от ЕС, в която обичайно пребивавате.

Пример

Правите поръчка на уебсайт. Сайтът претърпява кибератака, защото няма адекватни мерки за сигурност. Данните на кредитната Ви карта са преместени на друг уебсайт и са използвани за закупуване на продукти, които никога не сте поръчвали. Можете да предявите иск за обезщетение от уебсайта за финансовите щети, тъй като той е нарушил закона за защита на данните, като не е осигурил адекватна защита при обработването на данните.

Позовавания

- член 82 и съображения (146) и (147) от ОРЗД.

НАСОКИ НА РАБОТНА ГРУПА ПО ЧЛ. 29 ОТ ДИРЕКТИВА 95/46/ЕО ОТНОСНО ПРИЛАГАНЕТО НА ОБЩИЯ РЕГЛАМЕНТ ЗА ЗАЩИТА НА ДАННИТЕ

Работната група по член 29 от Директива 95/46/ЕО, която обединява всички национални органи по защита на данните, включително Европейския надзорен орган по защита на данните, играе основна роля в подготовката за прилагането на Общия регламент, като издава насоки за дружествата и другите заинтересовани страни. От 25 май 2018 г. неин приемник става създаденият с регламента Европейски комитет по защита на данните. Европейският комитет по защита на данните ще бъде орган на ЕС със статут на юридическо лице, който ще гарантира последователното прилагане на регламента. Той ще включва ръководителите на всички органи за защита на данните и Европейския надзорен орган по защита на данните, или техните представители.

Към момента Работната група по чл. 29 е приела следните насоки с оглед началото на прилагането на Общия регламент:

- Насоки за длъжностните лица по защита на данните („ДЛЗД“);

- Насоки относно оценката на въздействието върху защитата на данни (ОВЗД) и определяне дали съществува вероятност обработването „да породи висок риск” за целите на Регламент 2016/679;

- Насоки относно правото на преносимост на данните;

- Насоки относно прилагането и определянето на административните наказания „глоба” или „имуществена санкция” за целите на Регламент (ЕС) 2016/679;

- Насоки за определяне на водещ надзорен орган на администратор или обработващ лични данни;

- Насоки относно автоматизираното вземане на индивидуални решения и профилиране за целите на Регламент 2016/679;

- Насоки относно уведомяването за нарушение на сигурността на личните данни по Регламент 2016/679;

- Насоки относно прозрачността по Регламент 2016/679;

- Насоки относно съгласието по Регламент 2016/679.

От голямо значение е фактът, че тези насоки са предмет на обществена консултация преди финализирането им. В този процес е изключително важно мненията на заинтересованите страни да бъдат възможно най-точни и конкретни, което спомага за насочване вниманието към специфичните секторни характеристики. Крайната отговорност за тези насоки е на Работната група по член 29 и на бъдещия Европейски комитет по защита на данните, и органите за защита на данните ще се обръщат към тях при прилагането на регламента. Възможно е насоките да се изменят в светлината на последни развития и практики. За тази цел е от съществено значение органите за защита на данните да насърчават диалог с всички заинтересовани страни.

Важно е да се напомни, че когато става въпрос за тълкуването и прилагането на регламента, компетентни за окончателното тълкуване на регламента ще са съдилищата на национално и европейско равнище.

В настоящия брой публикуваме следните насоки на Работната група по чл. 29:

- Насоки за длъжностните лица по защита на данните („ДЛЗД“);

- Насоки относно оценката на въздействието върху защитата на данни (ОВЗД) и определяне дали съществува вероятност обработването „да породи висок риск” за целите на Регламент 2016/679;

- Насоки относно правото на преносимост на данните;

- Насоки относно прилагането и определянето на административните наказания „глоба” или „имуществена санкция” за целите на Регламент (ЕС) 2016/679;

- Насоки за определяне на водещ надзорен орган на администратор или обработващ лични данни.

НАСОКИ НА РАБОТНА ГРУПА ПО ЧЛ. 29 ОТ ДИРЕКТИВА 95/46/ЕО ОТНОСНО ДЛЪЖНОСТНИТЕ ЛИЦА ПО ЗАЩИТА НА ДАННИТЕ (ДЗЛД)

1. Въведение

Общият регламент относно защитата на данните („ОРЗД“)[1], който предстои да влезе в сила на 25 май 2018 г., предвижда модернизирана и основана на отчетност рамка за съблюдаване на защитата на данните в Европа. Длъжностните лица по защита на данните („ДЛЗД“) ще играят основна роля по отношение на тази нова рамка за много организации, като оказват съдействие за спазването на разпоредбите на ОРЗД.

Според ОРЗД някои администратори и обработващи лични данни са задължени да определят ДЛЗД[2]. Такъв е случаят с всички публични органи и структури (независимо какви данни обработват), както и за други организации, чиято основна дейност включва систематично и мащабно наблюдение на физически лица или които обработват мащабно специални категории лични данни.

Дори когато според ОРЗД не се изисква изрично назначаването на ДЛЗД, организациите понякога може да го приемат за полезно и доброволно да определят ДЛЗД. Работната група за защита на личните данни по член 29 („Работна група по член 29“) насърчава тези доброволни усилия.

Концепцията за ДЛЗД не е нова. Макар че според Директива 95/46/ЕО[3] от нито една организация не се изисква да назначава ДЛЗД, все пак в различни държави членки с течение на времето се е развила практиката за назначаване на ДЛЗД.

Преди приемането на ОРЗД Работната група по член 29 застъпваше тезата, че ДЛЗД са основният фактор за отчетност и че с назначаването на ДЛЗД може да се способства за спазването и, още повече, да се превърне в конкурентно предимство за предприятията[4]. Освен това, за да се способства за спазването чрез прилагането на инструменти за отчетност (като улесняване на оценките на въздействието върху защитата на данните и провеждането или подпомагането на одити), ДЛЗД служат за посредници между съответните заинтересовани страни (например надзорни органи, субекти на данните и стопански единици в рамките на дадена организация).

ДЛЗД не са лично отговорни в случай на неспазване на ОРЗД. В ОРЗД ясно се казва, че администраторът или обработващият лични данни е този, който е длъжен да гарантира и да е в състояние на докаже, че обработването се извършва в съответствие с предвидените в него разпоредби (член 24, параграф 1). Спазването на разпоредбите за защита на данните е отговорност на администратора на данни или на обработващия лични данни.

Администраторът на данни или обработващият лични данни също изпълняват важна роля за осигуряване на ефективното изпълнение на задачите на ДЛЗД. Назначаването на ДЛЗД е първата стъпка, но на ДЛЗД трябва в достатъчна степен да се даде независимост и да се осигурят ресурси, за да могат те да изпълняват ефективно своите задачи.

В ОРЗД се отчита, че ДЛЗД представляват важен фактор в новата система за управление на данните, и се определят условията за тяхното назначаване, длъжност и задачи. С настоящите насоки се цели да бъдат пояснени съответните разпоредби в ОРЗД, за да се помогне на администраторите и

1 Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. 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), (ОВ L 119, 4.5.2016 г.). ОРЗД е от значение за ЕИП и ще се прилага след включването му в Споразумението за ЕИП.

2 Назначаването на ДЛЗД е задължително също така за компетентни органи по член 32 от Директива (ЕС) 2016/680 на Европейския парламент и на Съвета от 27 април 2016 г. 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 −131), както и националното законодателство за прилагане. Макар че настоящите насоки са насочени към ДЛЗД съгласно ОРЗД, насоките са релевантни също така за ДЛЗД съгласно Директива 2016/680 с оглед на сходните им разпоредби.

3 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 L 281, 23.11.1995 г., стр. 31).

4 Вж. http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150617_appendix_core_issues_plenary_en.pdf

обработващите лични данни да спазват законодателството, но също така да се окаже съдействие на ДЛЗД при изпълнението на техните функции. В насоките са дадени също така препоръки относно най-добри практики, които са базирани на натрупания опит в някои държави − членки на ЕС. Работната група по член 29 ще следи прилагането на тези насоки и ако е целесъобразно, може да ги допълва с още подробности.

2. Определяне на ДЛЗД

2.1. Задължително определяне

Според член 37, параграф 1 от ОРЗД определянето на ДЛЗД се изисква в три конкретни случая[5]:

а) когато обработването се извършва от публичен орган или структура[6];

б) когато основните дейности на администратора или обработващия лични данни се състоят в операции по обработване, които поради своето естество, обхват и/или цели изискват редовно и систематично мащабно наблюдение на субектите на данни; или

в) когато основните дейности на администратора или обработващия лични данни се състоят в мащабно обработване на специалните категории данни[7] или[8] на лични данни, свързани с присъди и нарушения[9] .

В следващите подраздели Работната група по член 29 предлага насоки по отношение на критериите и използваната терминология в член 37, параграф 1.

Освен ако е очевидно, че дадена организация не е задължена да определя ДЛЗД, Работната група по член 29 препоръчва администраторите и обработващите лични данни да документират направения вътрешен анализ с оглед на вземането на решение дали да бъде назначено ДЛЗД или не, за да бъдат в състояние да докажат, че съответните фактори са взети предвид по надлежен начин[10]. Този анализ представлява част от документацията според принципа на отчетност. Той може да бъде изискан от надзорния орган и следва да се актуализира при нужда, например ако администраторите или обработващите лични данни започнат осъществяването на нови дейности или предоставянето на нови услуги, които е възможно да попадат в случаите, посочени в член 37, параграф 1.

Когато дадена организация доброволно определя ДЛЗД, изискванията по членове 37−39 ще се прилагат за неговото определяне, длъжност и задачи по същия начин, както ако определянето е било задължително.

Нищо не пречи на организация, която не е задължена по закон да определя ДЛЗД и не желае да определя ДЛЗД на доброволна база, все пак да наеме персонал или външни консултанти, които да изпълняват задачи, свързани със защитата на личните данни. В този случай е важно да се гарантира, че няма да има объркване по отношение на званието, статута, длъжността и задачите. Поради това във всички съобщения в рамките на дружеството, както и с органите за защита на данните, субектите на данни и обществеността като цяло, трябва да се пояснява, че длъжността на въпросното физическо лице или консултант не е длъжностно лице по защита на данните (ДЛЗД)[11].

5 Следва да се има предвид, че според член 37, параграф 4 определянето на ДЛЗД може да се изисква и в други случаи според правото на Съюза или правото на държава членка.

6 Освен когато става въпрос за съдилища при изпълнение на съдебните им функции. Вж. член 32 от Директива (ЕС) 2016/680.

7 В съответствие с член 9 те включват лични данни, разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения или членство в синдикални организации, както и обработването на генетични данни, биометрични данни за целите единствено на идентифицирането на физическо лице, данни за здравословното състояние или данни за сексуалния живот или сексуалната ориентация на физическото лице.

8 В член 37, параграф 1, буква в) е използван съюзът „и”. Вж. раздел 2.1.5 по-долу за обяснение на използването на „или” вместо „и”.

9 член 10.

10 Вж. член 24, параграф 1.

11 Това е от значение също така за ръководителите на служби за защита на информацията или други специалисти в областта на неприкосновеността на личния живот, каквито понастоящем вече се наемат в някои дружества, които е възможно не винаги да отговарят на критериите на ОРЗД, например по отношение на наличните ресурси или гаранции за независимост, и ако не ги изпълняват, тогава те не може да бъдат считани за ДЛЗД, нито наричани така.

ДЛЗД се определя, независимо дали задължително или на доброволна база, за всички операции по обработването, които се извършват от администратора или обработващия лични данни.

2.1.1 „Публичен орган или структура“

В ОРЗД не е дадено определение на *„публичен орган или структура*“. Работната група по член 29 счита, че това понятие следва да бъде определено съгласно националното право. Съответно публичните органи и структури включват национални, регионални и местни органи, но според приложимите национални закони понятието обикновено включва така също редица други органи, уредени от публичното право[12]. В такива случаи определянето на ДЛЗД е задължително.

Обществена задача може да се изпълнява и обществени правомощия да се упражняват[13] не само от публични органи или структури, но също така от други физически или юридически лица, уредени от публичното или частното право, в сектори като услуги за обществен транспорт, водоснабдяване и енергоснабдяване, пътна инфраструктура, обществени медии, социално жилищно настаняване или дисциплинарни органи за регулираните професии в съответствие с националната нормативна уредба на всяка държава членка.

В тези случаи субектите на данни може да са поставени в много сходна ситуация на тази, в която данните им се обработват от публичен орган или структура. По-специално някои данни може да се обработват със сходна цел и физическите лица често в много малка степен могат или изобщо не могат да избират дали и как да се обработват техните данни и следователно може да се нуждаят от допълнителната защита, която може да бъде осигурена с определянето на ДЛЗД.

Макар че в такива случаи не е задължително, Работната група по член 29 препоръчва като добра практика частните организации, които изпълняват обществени задачи или упражняват обществени правомощия, да определят ДЛЗД. Дейността на подобно ДЛЗД обхваща всички извършвани операции по обработването, включително онези, които не са свързани с изпълнението на обществената задача или на официалните задължения (например управлението на база данни на служителите).

2.1.2 „Основни дейности“

Член 37, параграф 1, букви б) и в) от ОРЗД се отнасят до *„основните дейности на администратора или обработващия лични данни“*. В съображение 97 е посочено, че основните дейности на администратора се отнасят до неговите *„първични дейности, а не до обработването на лични данни като вторични дейности“*. „Основните дейности“ може да се считат за ключовите операции, които са необходими за постигането на целите на администратора или обработващия лични данни.

Въпреки това не следва да се счита, че „основните дейности“ изключват дейностите, при които обработването на данни представлява неразривна част от дейността на администратора или обработващия лични данни. Например основната дейност на една болница е предоставянето на здравно обслужване. Болницата обаче не може да предоставя здравно обслужване безопасно и ефективно, без да обработва данни за здравословното състояние, като например здравни досиета на пациенти. Следователно обработването на тези данни следва да се счита за една от основните дейности на всяка болница и съответно болниците трябва да определят ДЛЗД.

Като друг пример може да се посочи частно охранително дружество, което осъществява наблюдение върху няколко частни търговски обекта и обществени места. Основната дейност на дружеството е наблюдение, което от своя страна е неразривно свързано с обработването на лични данни. Следователно това дружество също трябва да определи ДЛЗД.

12 Вж. например определението на „орган от обществения сектор” и „орган, управляван от публичното право” 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).

13 Член 6, параграф 1, буква д).

От друга страна, всички организации извършват определени дейности, например плащане на служителите си или осъществяване на стандартни дейности по поддръжка на ИТ. Това са примери за спомагателни функции, които са необходими за основната дейност или основното направление на стопанската дейност на организацията. Въпреки че тези дейности са необходими или дори съществено важни, те обикновено са считани за спомагателни функции, а не за основна дейност.

2.1.3 „Мащабно“

Според член 37, параграф 1, букви б) и в) се изисква обработването на лични данни да се извършва мащабно, за да се предприеме определяне на ДЛЗД. В ОРЗД не е определено какво се приема за мащабно обработване, макар че в съображение 91 са дадени известни насоки[14].

Всъщност не е възможно да се посочи точен брой по отношение както на обема обработвани данни, така и на броя на засегнатите физически лица, който да бъде приложим във всички ситуации. В тази връзка обаче не се изключва възможността с течение на времето да се наложи стандартна практика за по-конкретно и/или количествено определяне на това какво представлява *„мащабно“* при някои видове общи дейности по обработване. Работната група по член 29 планира също да се включи в този процес, като споделя и разпространява примери за съответни прагове, при които се налага определяне на ДЛЗД.

Във всички случаи Работната група по член 29 препоръчва, когато се установява дали се извършва мащабно обработване, да се вземат предвид по-специално следните фактори:

• брой на засегнатите субекти на данните или като конкретен брой, или като дял от съответното население;

• обем на данните и/или диапазон от различни елементи на данните, които се обработват;

• продължителност или постоянство на дейността по обработване на данните;

• географски обхват на дейността по обработване.

Примерите за мащабно обработване включват

• обработване на пациентски данни в обичайните условия на осъществяване на дейността на болница;

• обработване на данни за пътувания на физически лица, използващи системата на обществен транспорт на даден град (например проследяване чрез карти за пътуване);

• обработване в реално време на данни за определяне на географското местоположение на клиенти на международна верига за бързо хранене за статистически цели от страна на обработващ лични данни, който е специализиран в предоставянето на тези услуги;

• обработване на клиентски данни от застрахователно дружество или банка в обичайните условия на осъществяване на дейността;

• обработване на лични данни от търсачка с цел поведенческа реклама;

• обработване на данни (съдържание, трафик, местоположение) от доставчици на телефонни или интернет услуги.

Примерите, които не представляват мащабно обработване, включват:

• обработване на пациентски данни от отделен лекар;

14 Според съображението се включват по-специално „широкомащабни операции по обработване, 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”. От друга страна, в съображението изрично е посочено, че „обработването на лични данни не следва да се счита за широкомащабно, ако засяга лични данни на пациенти или клиенти на отделен лекар, друг здравен работник или адвокат”. Важно е да се има предвид, че, докато в съображението са дадени примери за крайности в мащаба (обработване от отделен лекар спрямо обработване на данни на цяла държава или цяла Европа); между тези крайни случаи се простира огромна междинна зона. Освен това следва да се отчете, че това съображение се отнася до оценките на въздействието върху защитата на данните. Това предполага, че някои елементи може да са специфични за този контекст и да не са непременно приложими към определянето на ДЛЗД точно по същия начин.

• обработване на лични данни от отделен адвокат във връзка с присъди и нарушения.

2.1.4 „Редовно и систематично [...] наблюдение“

Понятието за редовно и систематично наблюдение на субектите на данните не е определено в ОРЗД, но концепцията за *„наблюдението на поведението на такива субекти на данни“* се споменава в съображение 24[15] и ясно включва всички форми на проследяване и профилиране в интернет, включително с цел поведенческа реклама.

Понятието за наблюдение обаче не е ограничено до онлайн средата и онлайн проследяването следва да се счита само за един от примерите за наблюдение на поведението на субектите на данните[16].

Според тълкуването на Работната група по член 29 „редовно“ означава едно или повече от следните:

• текущо или възникващо на определени интервали за определен период;

• многократно или повтарящо се на определени интервали;

• случващо се постоянно или периодично.

Според тълкуването на Работната група по член 29 „систематично“ означава едно или повече от следните:

• възникващо по някаква система;

• предварително уредено, организирано или методично;

• случващо се в рамките на общ план за събиране на данни;

• осъществявано в рамките на стратегия.

Примери за дейности, които може да представляват редовно и систематично наблюдение на субектите на данните: експлоатация на далекосъобщителна мрежа; предоставяне на далекосъобщителни услуги; пренасочване на електронни съобщения; основани на данни маркетингови дейности; профилиране и оценяване за целите на оценка на риска (например за целите на определяне на кредитоспособността, изчисляване на застрахователни премии, предотвратяване на измами, откриване на случаи на изпиране на пари); проследяване на местоположението, например чрез мобилни приложения; програми за лоялност; поведенческа реклама; наблюдение на данни за благосъстоянието, тонуса и здравословното състояние чрез носими устройства; вътрешна система за видеонаблюдение; свързани устройства, например интелигентни измервателни устройства, интелигентни автомобили, автоматизация на дома и т.н.

2.1.5 Сп*ециални категории данни и данни, свързани с присъди и нарушени*

Член 37, параграф 1, буква в) се отнася до обработването на специални категории данни съгласно член 9 и лични данни, свързани с присъди и нарушения, посочени в член 10. Въпреки че в разпоредбата е използван съюзът „и“, няма причина, основана на политиката, поради която двата критерия да трябва да се прилагат едновременно. По тази причина следва да се счита, че съюзът е „или“.

2.2. ДЛЗД на обработващ лични данни

По отношение на определянето на ДЛЗД член 37 се прилага както за администратори[17], така и за обработващи лични данни[18]. В зависимост от това кой отговаря на критериите за задължително

15 „С цел да се определи дали дадена дейност по обработване може да се смята за наблюдение на поведението на субектите на данни, следва да се установи дали физическите лица се следят в интернет, включително да се установи евентуално последващо използване на техники за обработване на лични данни, които се състоят в профилиране на дадено физическо лице, по-специално с цел да се вземат отнасящи се до него решения или да се анализират или предвиждат неговите лични предпочитания, поведение и начин на мислене.”

16 Следва да се вземе предвид, че съображение 24 е насочено към извънтериториалното прилагане на ОРЗД. Освен това има разлика също така между формулировката „наблюдението на тяхното поведение” (член 3, параграф 2, буква б) и „редовно и систематично [...] наблюдение на субектите на данни” (член 37, параграф 1, буква б), която съответно може да се счита, че представлява различно понятие.

17 Администраторът е определен в член 4, параграф 7 като лице или орган, който определя целите и средствата на обработването на лични данни.

18 Обработващият лични данни е определен в член 4, параграф 8 като лице или орган, което/който обработва данни от името на администратора.

определяне, в някои случаи само администраторът или само обработващият лични данни, а в други случаи и администраторът, и неговият обработващ лични данни е длъжен да назначи ДЛЗД (които тогава следва да си сътрудничат).

Важно е да се подчертае, че дори администраторът да отговаря на критериите за задължително определяне, от неговия обработващ лични данни не се изисква непременно да назначава ДЛЗД. Макар че това може да е добра практика.

Примери:

• Малко семейно предприятие, което се занимава с разпространение на домакински уреди в един град, използва услугите на обработващ лични данни, чиято основна дейност се състои в предоставянето на аналитични услуги на уебсайтове и съдействие за целева реклама и маркетинг. Дейностите на семейното предприятие и неговите клиенти не са свързани с „мащабно“обработване на данни, като се имат предвид малкият брой клиенти и относително ограничените дейности. Взети заедно обаче, дейностите на обработващия лични данни, който има много клиенти като това малко предприятие, представляват мащабно обработване. Следователно обработващият лични данни трябва да определи ДЛЗД съгласно член 37, параграф 1, буква б). В същото време самото семейно предприятие не е задължено да определя ДЛЗД.

• Средно предприятие за производство на плочки възлага дейността на службата си по трудова медицина на външен обработващ лични данни, който има голям брой подобни клиенти. Обработващият лични данни следва да определи ДЛЗД съгласно член 37, параграф 1, буква в), при условие че обработването е мащабно. Производителят обаче не е непременно задължен да определи ДЛЗД.

ДЛЗД, което е определено от обработващ лични данни, следи също така дейностите, които организацията на обработващия лични данни осъществява самостоятелно в качеството си на администратор на данни (например човешки ресурси, ИТ, логистика).

2.3. Определяне на едно ДЛЗД за различни организации

Според член 37, параграф 2 група предприятия има право да определи едно ДЛЗД, при условие че *„от всяко предприятие има лесен достъп“* до него. Понятието за достъпност се отнася до задачите на ДЛЗД като точка за контакт по отношение на субектите на данните[19], надзорния орган[20], но също така вътрешно в организацията, като се има предвид, че една от задачите на ДЛЗД е *„да информира и съветва администратора или обработващия лични данни и служителите, които извършват обработване, за техните задължения по силата на настоящия регламент“*[21].

За да се гарантира достъпът до ДЛЗД, независимо дали вътрешен или външен достъп, важно е да се осигури наличието на неговите данни за контакт в съответствие с изискванията на ОРЗД[22].

Въпросното лице, при нужда с помощта на екип, трябва да има възможност ефективно да общува със субектите на данните[23] и да си сътрудничи[24] със съответните надзорни органи. Това означава също така, че тази комуникация трябва да се осъществява на езика или езиците, използван/и от съответните надзорни органи или субекти на данните. Наличието на ДЛЗД (независимо дали присъства физически в същото помещение като служителите, или чрез гореща линия или други сигурни средства за комуникация) е от съществена важност, за да се гарантира, че субектите на данни ще могат да се свържат с ДЛЗД.

19 член 38, параграф 4: „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”

20 член 39, параграф 1, буква 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”

21 член 39, параграф 1, буква а).

22 Вж. също раздел 2.6 по-долу.

23 член 12, параграф 1: „Администраторът предприема необходимите мерки за предоставяне на всякаква информация по членове 13 и 14 и на всякаква комуникация по членове 15—22 и член 34, която се отнася до обработването, на субекта на данните в кратка, прозрачна, разбираема и лесно достъпна форма, на ясен и прост език, особено що се отнася до всяка информация, конкретно насочена към деца”

24 Член 39, параграф 1, буква г): „да си сътрудничи с надзорния орган”.

В съответствие с член 37, параграф 3 едно ДЛЗД може да бъде определено за няколко публични органа или структури, като се отчита организационната им структура и размер. По отношение на ресурсите и комуникацията се прилагат същите условия. Като се има предвид, че ДЛЗД отговаря за разнообразни задачи, администраторът или обработващият лични данни трябва да гарантира, че едно ДЛЗД, при нужда с помощта на екип, може да ги изпълнява ефективно, въпреки че е определено за няколко публични органа или структури.

2.4. Достъпност и местоположение на ДЛЗД

В раздел 4 от ОРЗД е предвидено, че ДЛЗД следва реално да бъде достъпно.

За да се гарантира достъпността на ДЛЗД, Работната група по член 29 препоръчва ДЛЗД да се намира в рамките на Европейския съюз, независимо дали администраторът или обработващият лични данни е установен в Европейския съюз или не.

Не може обаче да се изключи в някои ситуации, когато администраторът или обработващият лични данни няма място на установяване в Европейския съюз[25], че ДЛЗД може да е в състояние да осъществява своите дейности по-ефективно, ако се намира извън ЕС.

2.5. Опит и умения на ДЛЗД

В член 37, параграф 5 се казва, че ДЛЗД *„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 член 39“*. Според съображение 97 необходимото ниво на експертни познания следва да се определя по-специално в съответствие с извършваните операции по обработване на данни и защитата, която е необходима за личните данни, обработвани от администратора или обработващия лични данни.

• Ниво на опит

Изискваното ниво на опит не е строго определено, но то трябва да е съизмеримо с чувствителността, сложността и обема на данните, които обработва дадена организация. Например когато дадена дейност по обработване на данни е особено сложна или когато се касае за голям обем от чувствителни данни, за ДЛЗД може да са нужни повече опит и подкрепа. Налице е също така разлика в зависимост от това дали организацията системно прехвърля лични данни извън Европейския съюз или дали подобни прехвърляния са редки. Следователно ДЛЗД трябва да се избира внимателно, предвид възникващите в рамките на организацията въпроси във връзка със защитата на данните.

• Професионални качества

Въпреки че в член 37, параграф 5 не са изрично определени професионалните качества, които следва да се имат предвид при определянето на ДЛЗД, важен фактор е ДЛЗД да има опит в сферата на националните и европейските закони и практики в областта на защитата на данните и да разбира в дълбочина ОРЗД. Полезно би било също така надзорните органи да насърчават подходящото и редовно обучение на ДЛЗД.

От полза е да притежава познания за стопанския сектор и организацията на администратора. ДЛЗД следва също така добре да познава извършваните операции по обработване, както и информационните системи и нуждите на администратора, свързани със сигурността и защитата на данните.

В случай на публичен орган или структура, ДЛЗД следва да е добре запознато също така с административните правила и процедури на организацията.

25 Вж. член 3 от ОРЗД относно териториалния обхват.

• ***Способност да изпълнява своите задачи***

Способността за изпълняване на задачите, възлагани на ДЛЗД, следва да се тълкува както по отношение на неговите лични качества и знания, така също и във връзка с позицията му в рамките на организацията. Личните качества следва да включват например почтеност и висока професионална етика; първостепенната задача на ДЛЗД следва да бъде осигуряването на възможност за спазване на ОРЗД. ДЛЗД изпълнява ключова роля за насърчаване на културата на защита на данните в рамките на организацията и спомага за прилагането на съществено важните елементи на ОРЗД като принципите на обработване на данните[26], правата на субектите на данните[27], защита на данните чрез проектното решение и по подразбиране[28], записи на дейностите по обработване[29], сигурност на обработването[30], както и уведомяване и съобщаване за нарушения на сигурността на данните[31].

• ***ДЛЗД въз основа на договор за услуги***

Функциите на ДЛЗД може да се упражняват също така въз основа на договор за услуги, сключен с физическо лице или организация, извън организацията на администратора/обработващия лични данни. В последния случай е съществено важно всеки член на организацията, който изпълнява функциите на ДЛЗД, да отговаря на всички приложими изисквания от раздел 4 от ОРЗД (например съществено важно е никой да не е в конфликт на интереси). Също толкова важно е всеки един член да бъде защитен по разпоредбите на ОРЗД (например да няма несправедливо прекратяване на договор за услуги за дейностите като ДЛЗД, но също така да няма несправедливо уволняване на никой отделен член на организацията при изпълняване на задачите на ДЛЗД). В същото време отделните умения и силни страни може да се съчетаят, така че различните физически лица, работещи в екип, да могат по-ефективно да обслужват своите клиенти.

Предвид правната яснота и добрата организация и с оглед на избягването на конфликт на интереси сред членовете на екипа, се препоръчва да е налице ясно разпределение на задачите в рамките на екипа на ДЛЗД, като отделно лице бъде натоварено с ролята на основно лице за контакт и „отговорник“ за всеки клиент. По принцип би било от полза също така тези точки да бъдат включени в договора за услуги.

2.6. Публикуване и съобщаване на данните за контакт с ДЛЗД

Според член 37, параграф 7 от ОРЗД се изисква администраторът или обработващият лични данни:

• да публикува данните за контакт с ДЛЗД; както и

• да съобщи данните за контакт с ДЛЗД на съответните надзорни органи.

Целта на тези изисквания е да се гарантира, че субектите на данни (както в рамките на организацията, така и извън нея) и надзорните органи ще могат лесно и пряко да се свързват с ДЛЗД, без да се налага да осъществява контакт с друга част на организацията. Поверителността е също толкова важна: например служителите може да не са склонни да се оплачат на ДЛЗД, ако не е гарантирана поверителността на техните съобщения.

ДЛЗД е длъжно да спазва секретността или поверителността на изпълняваните от него задачи в съответствие с правото на Съюза или правото на държава членка (член 38, параграф 5).

Данните за контакт с ДЛЗД следва да включват информация, позволяваща на субектите на данните и на надзорните органи лесно да осъществяват връзка с ДЛЗД (пощенски адрес, специален

26 Глава II.
27 Глава III.
28 член 25.
29 член 30.
30 член 32.
31 членове 33 и 34

телефонен номер и/или специален адрес на ел. поща). По целесъобразност, за целите на комуникацията с обществеността може да бъдат осигурени и други средства за комуникация, като например специална гореща линия или специален формуляр за контакт с ДЛЗД на уебсайта на организацията.

Според член 37, параграф 7 не се изисква публикуваните данни за контакт да включват името на ДЛЗД. Въпреки че това може да е добра практика, администраторът или обработващият лични данни и ДЛЗД решават дали това е необходимо или полезно с оглед на конкретните обстоятелства[32].

Съобщаването на името на ДЛЗД на надзорния орган обаче е съществено важно, за да може ДЛЗД да служи като точка за контакт между организацията и надзорния орган (член 39, параграф 1, буква д).

Работната група по член 29 препоръчва така също като добра практика организацията да уведомява служителите си за името и данните за контакт с ДЛЗД. Например името и данните за контакт с ДЛЗД може да са публикувани вътрешно в интранета на организацията, в указател на вътрешните телефони и организационните диаграми.

3. Длъжност на ДЛЗД

3.1. Ангажираност на ДЛЗД с всички въпроси, свързани със защитата на личните данни

В член 38 от ОРЗД се казва, че администраторът и обработващият лични данни гарантират, че ДЛЗД „*участва по подходящ начин и своевременно във всички въпроси, свързани със защитата на личните данни*“.

Съществено важно е ДЛЗД или неговият екип да се включват на възможно най-ранен етап във всички въпроси, касаещи защитата на данните. Що се отнася до оценките на въздействието върху защитата на данните, в ОРЗД изрично се предвижда ранното включване на ДЛЗД и се посочва, че администраторът следва да се съветва с ДЛЗД, когато прави такива оценки на въздействието[33]. Като се гарантира информирането на ДЛЗД и консултирането с него от самото начало, ще се улесни спазването на ОРЗД, ще се насърчи възприемането на подход за неприкосновеност на личния живот чрез проектното решение и съответно следва да се включи като стандартна процедура в управлението на организацията. Освен това е важно ДЛЗД да се приема като партньор за обсъждане в рамките на организацията и да се включва в съответните работни групи, които се занимават с дейностите по обработване на данни в рамките на организацията.

Следователно организацията трябва да гарантира например, че:

• редовно ДЛЗД се кани да участва на заседанията на висшето и средното ръководство;

• присъствието му е препоръчително, когато се вземат решения, имащи отражение върху защитата на данните. Всяка релевантна информация трябва своевременно да се предоставя на ДЛЗД, за да може ДЛЗД да даде подходящ съвет;

• на становището на ДЛЗД трябва винаги да се отдава необходимото значение. Работната група по член 29 препоръчва като добра практика в случай на несъгласие да се документират причините, поради които съветът на ДЛЗД не е последван;

• когато се установи нарушение на сигурността на данните или друг инцидент, незабавно трябва да се направи консултация с ДЛЗД.

Когато е целесъобразно, администраторът или обработващият би могъл да разработи насоки или програми за защита на данните, в които да се предвидят случаите, когато трябва да се направи консултация с ДЛЗД.

32 Следва да се отбележи, че според член 33, параграф 3, буква б), където е описана информацията, която трябва да бъде предоставена на надзорния орган и на субектите на данни в случай на нарушение на сигурността на личните данни, за разлика от член 37, параграф 7, изрично се изисква да се съобщи и името (а не само данните за контакт) на ДЛЗД.

33 член 35, параграф 2.

3.2. Необходими ресурси

Според член 38, параграф 2 от ОРЗД се изисква организациите да подпомагат своите ДЛЗД, като „*осигуряват ресурсите, необходими за изпълнението на техните задачи, и достъп до личните данни и операциите по обработване, а така също поддържат техните експертни знания*“. По-специално следва да се имат предвид следните аспекти:

• активно подпомагане на функциите на ДЛЗД от страна на висшето ръководство (като например на ниво управителен съвет);

• достатъчно време за изпълнението на задълженията на ДЛЗД. Това е особено важно, когато е назначено вътрешно ДЛЗД на непълно работно време или когато външно ДЛЗД изпълнява функции по защита на данните в допълнение към други задължения. В противен случай противоречието между приоритетите би могло да доведе до пренебрегване на задълженията на ДЛЗД. Съществено важно е да се предвиди достатъчно време за задачите на ДЛЗД. Добра практика е да се определи процент от времето за функциите на ДЛЗД, когато те не се изпълняват на база пълен работен ден. Добра практика е също така определянето на необходимото време за изпълнение на функциите, определянето на подходящото ниво на приоритет за задълженията на ДЛЗД и изготвянето на работен план от ДЛЗД (или от организацията);

• подходящо подпомагане от гледна точка на финансовите ресурси, инфраструктурата (помещения, съоръжения, оборудване) и персонала, когато е целесъобразно;

• официално съобщаване за определянето на ДЛЗД пред целия персонал, за да се гарантира, че в организацията се знае за наличието и функциите му;

• необходим достъп до други отдели, като човешки ресурси, правни, ИТ, по сигурността и т.н., за да могат ДЛЗД да получават съществено важно подпомагане, ресурси и информация от въпросните други отдели;

• продължаващо обучение. ДЛЗД трябва да имат възможност да са в крак с новостите в областта на защитата на данните. Целта трябва да е непрекъснато да се повишава нивото на опит на ДЛЗД и те следва да се насърчават да участват в курсове за обучение по защита на данните и други форми на професионално развитие, като участие на форуми и семинари, посветени на неприкосновеността на личния живот, т.н.;

• предвид големината и структурата на организацията, може е наложително да се сформира екип на ДЛЗД (ДЛЗД и неговия персонал). В такива случаи ясно трябва да се определи вътрешната структура на екипа и задачите и отговорностите на всеки от неговите членове. Аналогично, когато функциите на ДЛЗД се изпълняват от външен доставчик на услуги, екип от физически лица, работещи за съответното предприятие, може ефективно да изпълнява задачите на ДЛЗД като екип, отговорност за който носи определеното лице за контакт и „отговорник“ за клиента.

Обикновено колкото по-сложни и по-чувствителни са операциите по обработване, толкова повече ресурси трябва да бъдат предоставени на ДЛЗД. Функциите по защита на данните трябва да бъдат ефективни и достатъчно добре ресурсно обезпечени с оглед на извършваното обработване на данни.

3.3. Указания и изпълнение на техните „*задължения и задачи независимо*“

В член 38, параграф 3 са предвидени някои основни положения, които спомагат да се осигурят гаранции за това, че ДЛЗД са в състояние да изпълняват своите задачи с достатъчна степен на независимост в рамките на тяхната организация. По-специално администраторите/обработващите лични данни са длъжни да гарантират, че ДЛЗД „*не получава никакви указания във връзка с изпълнението на своите задачи*“. В съображение 97 е добавено, че ДЛЗД „*независимо от това дали са служители на администратора, следва да бъдат в състояние да изпълняват своите задължения и задачи независимо*“.

Това означава, че при изпълнението на своите задачи по член 39 ДЛЗД не бива да получават указания как да решат въпроса, например какъв резултат трябва да бъде постигнат, как да провеждат разследване по жалба или дали да се консултират с надзорния орган. Освен това те не бива да получават указания да възприемат определена гледна точка по даден въпрос, свързан със законодателството в областта на защитата на данните, например конкретно тълкуване на закона.

Независимостта на ДЛЗД обаче не означава, че те разполагат с правомощия за вземане на решения извън задачите им по член 39.

Администраторът или обработващият лични данни продължава да носи отговорност за спазването на законодателството в областта на личните данни, което трябва да бъде в състояние да докаже[34]. Ако администраторът или обработващият лични данни взема решения, които са несъвместими с ОРЗД и съвета на ДЛЗД, на ДЛЗД трябва да бъде дадена възможност ясно да изрази неговото различно становище пред най-висшето ръководно ниво и пред лицата, които вземат решенията. В това отношение в член 38, параграф 3 е предвидено, че ДЛЗД *„се отчита пряко пред най-висшето ръководно ниво на администратора или обработващия лични данни“*. Благодарение на това пряко отчитане се гарантира, че висшето ръководство (например съвета на директорите) е запознато със съвета и препоръките на ДЛЗД в рамките на неговите задачи да уведомява и съветва администратора или обработващия лични данни. Друг пример за пряко отчитане е изготвянето на годишен отчет за дейността на ДЛЗД, който се представя на най- висшето ръководно ниво.

3.4. Освобождаване от длъжност или санкциониране за изпълнението на задачите на ДЛЗД

Според член 38, параграф 3 се изисква ДЛЗД да „*не може да бъде освобождавано от длъжност, нито санкционирано от администратора или обработващия лични данни за изпълнението на своите задачи*“.

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.

34 член 5, параграф 2.

3.5. Конфликт на интереси

Според член 38, параграф 6 се допуска ДЛЗД „*да изпълнява и други задачи и задължения*“. Изисква се обаче организацията да гарантира, че „*тези задачи и задължения да не водят до конфликт на интереси*“.

Отсъствието на конфликт на интереси е тясно свързано с изискването да се действа независимо. Въпреки че се допуска ДЛЗД да изпълняват и други функции, те може да бъдат натоварени с други задачи и задължения, само ако те не пораждат конфликт на интереси. Това означава по- специално, че ДЛЗД не може да заема длъжност в рамките на организацията, която ще го задължава да определя целите и средствата за обработването на лични данни. Поради специфичната организационна структура във всяка организация, този аспект трябва да се разглежда на база конкретен случай.

Длъжностите в рамките на организацията, които влизат в противоречие, по общо правило може да включват длъжности във висшето ръководство (като главен изпълнителен директор, главен оперативен директор, главен финансов директор, главен медицински директор, ръководител на маркетингов отдел, ръководител на отдел „Човешки ресурси“ или ръководител на ИТ отдел), но също така и други функции по-надолу в организационната структура, ако въпросните длъжности или функции са свързани с определяне на целите и средствата за обработване на данните. Освен това конфликт на интереси може да възникне също така например, ако външно ДЛЗД бъде поканено да представлява администратора или обработващия лични данни пред съдилищата по дела, касаещи теми за защитата на данните.

В зависимост от дейностите, големината и структурата на организацията, може да е добра практика администраторите и обработващите лични данни:

• да идентифицират длъжностите, които биха били несъвместими с функциите на ДЛЗД;

• да разработят вътрешни правила в тази връзка, за да се избягва възникването на конфликти на интереси;

• да включат по-общо обяснение на понятието „конфликт на интереси“;

• да декларират, че тяхното ДЛЗД не е в конфликт на интереси, що се отнася до изпълнението на неговите функции на ДЛЗД, като средство за повишаване на осведомеността по отношение на това изискване;

• да предвидят гаранции във вътрешните правила на организацията и да осигурят достатъчната точност и детайлност на съобщението за свободната длъжност на ДЛЗД или на договора за услуги, за да се избегне конфликт на интереси. В този контекст следва да се има предвид също така, че конфликтите на интереси може да съществуват под различни форми, в зависимост от това дали ДЛЗД е нает като вътрешен служител или на външна база.

4. Задачи на ДЛЗД

4.1. Наблюдение на спазването на ОРЗД

Според член 39, параграф 1, буква б) ДЛЗД са натоварени, наред с други задължения, със задължението да наблюдават спазването на ОРЗД. В съображение 97 е уточнено допълнително, че *„администраторът или обработващият лични данни следва да бъде подпомаган при наблюдението на вътрешното спазване на настоящия регламент“* от ДЛЗД.

В рамките на тези задължения за наблюдаване на спазването ДЛЗД има право по-специално:

• да събира информация за определяне на дейностите по обработване;

• да анализира и проверява изпълнението на дейностите по обработване;

• да информира, съветва и отправя препоръки към администратора или обработващия лични данни.

Наблюдаване на спазването не означава, че ДЛЗД носи лична отговорност в случай на неспазване. В ОРЗД ясно се казва, че администраторът, а не ДЛЗД, е този, който е длъжен 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“* (член 24, параграф 1). Спазването на изискванията за защита на данните е корпоративна отговорност на администратора на данни, а не на ДЛЗД.

4.2. Роля на ДЛЗД в оценката на въздействието върху защитата на данните

Според член 35, параграф 1 извършването на оценка на въздействието върху защитата на данните („ОВЗД“) е задача на администратора, а не на ДЛЗД. Все пак ДЛЗД може да изиграе много важна и полезна роля, като подпомага администратора. Въз основа на принципа на защита на данните чрез проектното решение, с член 35, параграф 2 изрично се изисква администраторът на данните да *„иска становището“* на ДЛЗД, когато прави ОВЗД. От друга страна, съгласно член 39, параграф 1, буква в) ДЛЗД е натоварено със задължението *„да предоставя съвети по отношение на ОВЗД и да наблюдава извършването на оценката съгласно член 35“*.

Работната група по член 29 препоръчва администраторът да иска становището на ДЛЗД по следните въпроси, наред с други[35]:

• дали да извърши ОВЗД или не;

• каква методика да използва при извършването на ОВЗД;

• дали да извърши ОВЗД вътрешно или да я възложи на външен изпълнител;

• какви гаранции (включително технически и организационни мерки) да приложи, за да намали до минимум всички рискове за правата и интересите на субектите на данните;

• дали оценката на въздействието върху защитата на данните е направена правилно и дали заключенията от нея (дали да се продължи с обработването и какви гаранции да се приложат) показват спазване на ОРЗД.

Ако администраторът не е съгласен със становището на ДЛЗД, документацията на ОВЗД изрично следва да обосновава в писмен вид защо становището не е взето предвид[36].

Работната група по член 29 препоръчва също така администраторът ясно да очертае, например в договора с ДЛЗД, но също така в информацията, която се предоставя на служителите, ръководството (и други заинтересовани страни, ако е уместно), точните задачи на ДЛЗД и техния обхват, по-специално по отношение на извършването на ОВЗД.

4.3. Сътрудничество с надзорния орган и действие като точка за контакт

Според член 39, параграф 1, букви г) и д) ДЛЗД следва „*да си сътрудничи с надзорния орган*“ и „*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*“.

35 В член 39, параграф 1 са посочени задачите на ДЛЗД и се указва, че ДЛЗД следва да изпълнява „най- малко” следните задачи. Следователно нищо не пречи на администратора да възложи на ДЛЗД други задачи, различни от изрично посочените в член 39, параграф 1, или да прецизира тези задачи по-подробно.

36 В член 24, параграф 1 е посочено, 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”.

Тези задачи се отнасят до ролята на ДЛЗД като „лице, оказващо съдействие“, спомената във въведението към настоящите насоки. ДЛЗД действа като точка за контакт, за да се улесни достъпът на надзорния орган до документите и информацията по изпълнението на предвидените в член 57 задачи, както и за упражняването на неговите разследващи, коригиращи, разрешителни и консултативни правомощия, посочени в член 58. Както вече беше посочено, ДЛЗД е обвързано със спазване на секретност или поверителност по отношение на изпълняваните от него задачи в съответствие с правото на Съюза или правото на държава членка (член 38, параграф 5). Все пак задължението за секретност/поверителност не забранява на ДЛЗД да осъществява контакт и да иска становището на надзорния орган. В член 39, параграф 1, буква д) е предвидено, че ДЛЗД може да се консултира с надзорния орган по целесъобразност по всякакви други въпроси.

4.4. Подход, основан на риска

С член 39, параграф 2 се изисква ДЛЗД „*надлежно да отчита рисковете, свързани с операциите по обработване, и да се съобразява с естеството, обхвата, контекста и целите на обработката*“.

С този член се напомня един общ принцип на здравия разум, който може да е релевантен за много аспекти от ежедневната работа на ДЛЗД. По същество с него се изисква ДЛЗД да определят приоритетите в техните дейности и да съсредоточават усилията си върху въпросите, които представляват най-голям риск за защитата на данните. Това не означава, че те следва да пренебрегват наблюдението на спазването на операциите по обработване на данни, които са със сравнително по-ниско ниво на риск, а по-скоро означава, че те следва да се съсредоточават най- вече върху областите с по-висок риск.

Този селективен и прагматичен подход следва да помогне на ДЛЗД да съветват администратора каква методика да използва когато извършва ОВЗД, в кои области трябва да се направи вътрешен или външен одит на защитата на данните, какви дейности по вътрешно обучение да се осигурят за персонала или ръководството, отговорно за дейностите по обработване на данни, както и на кои операции по обработване да отдели повече от времето си и от ресурсите.

4.5. Функции на ДЛЗД по отношение на воденето на регистър

Според член 30, параграфи 1 и 2 администраторът или обработващият лични данни, а не ДЛЗД, следва да „*поддържа регистър на дейностите по обработване, за които отговаря*“ или да „*поддържа регистър на всички категории дейности по обработването, извършени от името на администратор*“.

На практика ДЛЗД често създават описи и водят регистър на операциите по обработване въз основа на информация, която им се предоставя от различни отдели в тяхната организация, отговарящи за обработването на лични данни. Тази практика е установена съгласно множество действащи национални закони и според правилата за защита на данните, приложими за институциите и органите на ЕС[37].

В член 39, параграф 1 е посочен списък със задачите, с които ДЛЗД трябва да бъде натоварено като минимум. Следователно нищо не пречи на администратора или на обработващия лични данни да възложи на ДЛЗД задачата да води регистър на операциите по обработване, за които отговаря администраторът или обработващият лични данни. Този регистър следва да се счита за един от инструментите, даващи възможност на ДЛЗД да изпълнява неговите задачи по наблюдаване на спазването, информиране и съветване на администратора или обработващия лични данни.

Във всички случаи регистърът, който се изисква да се води в съответствие с член 30, следва да се счита също така за инструмент, позволяващ на администратора и на надзорния орган,

37 член 24, параграф 1, буква г) от Регламент (ЕО) № 45/2001.

при поискване, да придобият представа за всички дейности по обработване на лични данни, които се извършват в дадена организация. Следователно това е предварително условие за спазването и, като такова, представлява ефективна мярка за отчетност.

5. ПРИЛОЖЕНИЕ – НАСОКИ ЗА ДЛЗД: КАКВО ТРЯБВА ДА ЗНАЕТЕ

Целта на настоящото приложение е да се отговори по прост и лесен за четене начин на някои основни въпроси, които може да възникнат в организациите по отношение на новите изисквания съгласно Общия регламент относно защитата на данните (ОРЗД) за назначаването на ДЛЗД.

Определяне на ДЛЗД

1. Кои организации трябва да назначават ДЛЗД?

Определянето на ДЛЗД е задължение:

• ако обработването се извършва от публичен орган или структура (независимо какви данни се обработват);

• ако основните дейности на администратора или обработващия лични данни се състоят в операции по обработване, които изискват редовно и систематично мащабно наблюдение на субектите на данни;

• ако основните дейности на администратора или обработващия лични данни се състоят в мащабно обработване на специални категории данни или лични данни, свързани с присъди или нарушения.

Следва да се има предвид, че според правото на Съюза или на държава членка определянето на ДЛЗД може де се изисква и в други случаи. В заключение трябва да се отбележи, че дори определянето на ДЛЗД да не е задължително, понякога организациите може да сметнат за полезно доброволно да определят ДЛЗД. Работната група за защита на личните данни по член 29 („Работната група по член 29“) насърчава тези доброволни усилия. Когато дадена организация доброволно определя ДЛЗД, по отношение на неговото назначение, длъжност и задачи ще се прилагат същите изисквания, както ако определянето е било задължително.

Източник: член 37, параграф 1 от ОРЗД

2. Какво се разбира под „основни дейности“?

За „основни дейности“ може да се считат ключовите операции за постигане на целите на администратора или на обработващия лични данни. Те включват и всички дейности, при които обработването на данни представлява неразривна част от дейността на администратора или на обработващия лични данни. Например обработването на данни за здравословното състояние като здравни досиета на пациенти следва да се счита за една от основните дейности на всяка болница и следователно болниците трябва да определят ДЛЗД.

От друга страна, всички организации извършват определени спомагателни дейности, например плащане на служителите си или осъществяване на стандартни дейности по поддръжка на ИТ. Това са примери за спомагателни функции, които са необходими за основната дейност или основното направление на стопанската дейност на организацията. Въпреки че тези дейности са необходими или дори съществено важни, те обикновено са считани за спомагателни функции, а не за основна дейност.

Източник: член 37, параграф 1, букви б) и в) от ОРЗД

3. Какво се разбира под „мащабно обработване“?

В ОРЗД не е дадено определение на това какво представлява мащабно обработване. Работната група по член 29 препоръчва, когато се установява дали се извършва мащабно обработване, да се вземат предвид по-специално следните фактори:

• брой на засегнатите субекти на данните или като конкретен брой, или като дял от съответното население;

• обем на данните и/или диапазон от различни елементи на данните, които се обработват;

• продължителност или постоянство на дейността по обработване на данните;

• географски обхват на дейността по обработване.

Примерите за мащабно обработване включват:

• обработване на пациентски данни в обичайните условия на осъществяване на дейността на болница;

• обработване на данни за пътувания на физически лица, използващи системата за обществен транспорт на даден град (например проследяване чрез карти за пътуване);

• обработване в реално време на данни за определяне на географското местоположение на клиенти на международна верига за бързо хранене за статистически цели от страна на обработващ лични данни, който е специализиран в тези дейности;

• обработване на клиентски данни от застрахователно дружество или банка в обичайните условия на осъществяване на дейността;

• обработване на лични данни от търсачка с цел поведенческа реклама;

• обработване на данни (съдържание, трафик, местоположение) от доставчици на телефонни или интернет услуги.

Примерите, които не представляват мащабно обработване, включват:

• обработване на пациентски данни от отделен лекар;

• обработване на лични данни от отделен адвокат във връзка с присъди и нарушения.

Източник: член 37, параграф 1, букви б) и в) от ОРЗД.

4. Какво означава „редовно и систематично [...] наблюдение“?

Понятието „редовно и систематично наблюдение“ на субектите на данните не е определено в ОРЗД, но ясно включва всички форми на проследяване и профилиране в интернет, включително с цел поведенческа реклама. Все пак понятието „наблюдение“ не е ограничено до онлайн средата.

Примери за дейности, които може да представляват редовно и систематично наблюдение на субектите на данните: експлоатация на далекосъобщителна мрежа; предоставяне на далекосъобщителни услуги; пренасочване на електронни съобщения; основани на данни маркетингови дейности; профилиране и оценяване за целите на оценка на риска (например за определяне на кредитоспособността, изчисляване на застрахователни премии, предотвратяване на измами, откриване на случаи на изпиране на пари); проследяване на местоположението, например чрез мобилни приложения; програми за лоялност; поведенческа реклама; наблюдение на данни за благосъстоянието, тонуса и здравословното състояние чрез носими устройства; вътрешна система за видеонаблюдение; свързани устройства, например интелигентни измервателни устройства, интелигентни автомобили, автоматизация на дома и т.н.

Според тълкуването на Работната група по член 29 „редовно“ означава едно или повече от следните:

• текущо или възникващо на определени интервали за определен период;

• многократно или повтарящо се на определени интервали;

• случващо се постоянно или периодично.

Според тълкуването на Работната група по член 29 „систематично“ означава едно или повече от следните:

• възникващо по някаква система;
• предварително уредено, организирано или методично;
• случващо се в рамките на общ план за събиране на данни;
• осъществявано в рамките на стратегия.

Източник: член 37, параграф 1, буква б) от ОРЗД

5. Могат ли организациите да назначават съвместно ДЛЗД? Ако отговорът е „да“, при какви условия?

Да. Група предприятия може да определи едно ДЛЗД, при условие че *„от всяко предприятие има лесен достъп“* до въпросното лице. Понятието за достъпност се отнася до задачите на ДЛЗД като точка за контакт по отношение на субектите на данните, надзорния орган и също така вътрешно в рамките на организацията. За да се гарантира достъпът до ДЛЗД, независимо дали вътрешен или външен достъп, важно е да се осигури наличието на неговите данни за контакт. ДЛЗД, при нужда с помощта на екип, трябва да бъде в състояние ефективно да общува със субектите на данни и да си сътрудничи със съответните надзорни органи. Това означава, че въпросната комуникация трябва да се осъществява на езика или езиците, използван/и от съответните надзорни органи и субектите на данни. Наличието на ДЛЗД (независимо дали присъства физически в същото помещение като служителите, чрез гореща линия или други сигурни средства за комуникация) е от съществена важност, за да се гарантира, че субектите на данни ще бъдат в състояние да се свържат с ДЛЗД.

Едно ДЛЗД може да бъде определено за различни публични органи или структури, като се отчита организационната им структура и размер. По отношение на ресурсите и комуникацията важат същите съображения. Като се има предвид, че ДЛЗД отговаря за разнообразни задачи, администраторът или обработващият лични данни трябва да гарантира, че едно ДЛЗД, при нужда с помощта на екип, може да ги изпълнява ефективно, въпреки че е определено за няколко публични органа или структури.

Източник: член 37, параграфи 2 и 3 от ОРЗД

6. Къде следва да се намира ДЛЗД?

За да се гарантира достъпността на ДЛЗД, Работната група по член 29 препоръчва ДЛЗД да се намира в рамките на Европейския съюз, независимо дали администраторът или обработващият лични данни е установен в Европейския съюз или не. Не може обаче да се изключи в някои ситуации, когато администраторът или обработващият лични данни няма място на установяване в Европейския съюз, че ДЛЗД няма да е в състояние да осъществява своите дейности по-ефективно, ако се намира извън ЕС.

7. Възможно ли е да се назначи външно ДЛЗД?

Да. ДЛЗД може да бъде член на персонала на администратора или обработващия лични данни (вътрешно ДЛЗД) или да изпълнява задачите въз основа на договор за услуги. Това означава, че ДЛЗД може да бъде външно лице и в такъв случай неговите функции може да се упражняват на база на договор за услуги, сключен с физическо лице или организация.

Когато функциите на ДЛЗД се изпълняват от външен доставчик на услуги, екип от физически лица, работещи за съответното предприятие, може ефективно да изпълнява задачите на ДЛЗД като екип, отговорност за който носи определеното лице за контакт и „отговорник“ за клиента. В този случай е съществено важно всеки член на външната организация, който изпълнява функциите на ДЛЗД, да отговаря на всички приложими изисквания по ОРЗД.

В насоките се препоръчва, с оглед на правната яснота и добрата организация и за избягване на конфликти на интереси сред членовете на екипа, в договора за услуги да се предвиди ясно разпределение на задачите в рамките на външния екип на ДЛЗД и за всеки клиент да бъде определено по едно физическо лице като основно лице за контакт и „отговорник“.

Източник: член 37, параграф 6 от ОРЗД

8. Какви професионални качества трябва да притежава ДЛЗД?

ДЛЗД се определя въз основа на неговите професионални качества и по-специално въз основа на експертните му познания в сферата на законодателството и практиките в областта на защитата на данните и способността му да изпълнява своите задачи.

Необходимото ниво на експертни знания следва да се определя в съответствие с извършваните операции по обработване на данни и защитата, която е необходима за обработваните лични данни. Например когато дадена дейност по обработване на данни е особено сложна или когато се касае за голям обем от чувствителни данни, ДЛЗД може да има нужда от повече опит и подкрепа.

Съответните умения и опит включват:

• опит с национални и европейски закони и практики в областта на защитата на данните, в това число разбиране на ОРЗД в дълбочина;

• разбиране на извършваните операции по обработване;

• разбиране на информационните технологии и сигурността на данните;

• познания за стопанския сектор и органспособност за насърчаване на културата на защита на данните в рамките на организацията.

Източник: член 37, параграф 5 от ОРЗД

Длъжност на ДЛЗД

9. Какви ресурси следва предостави администраторът или обработващият лични данни на ДЛЗД?

ДЛЗД трябва да разполага с нужните ресурси, за да може да извършва своите задачи.

В зависимост от естеството на операциите по обработване и от дейностите и големината на организацията, на ДЛЗД трябва да бъдат предоставени следните ресурси:

• активно подпомагане на функциите на ДЛЗД от страна на висшето ръководство;

• достатъчно време за изпълнението на задачите на ДЛЗД;

• подходящо подпомагане от гледна точка на финансови ресурси, инфраструктура (помещения, съоръжения, оборудване) и персонал, когато е целесъобразно;

• официално съобщаване на определянето на ДЛЗД пред целия персонал;

• достъп до други отдели в рамките на организацията, за да могат ДЛЗД да получават съществено важно подпомагане, ресурси или информация от въпросните други отдели;

• продължаващо обучение.

Източник: член 38, параграф 2 от ОРЗД.

10. Какви гаранции дават възможност на ДЛЗД да изпълнява задачите си по независим начин? Какво означава „конфликт на интереси“?

Предвидени са няколко гаранции, с които се дава възможност на ДЛЗД да действа независимо:

• не се дават указания от страна на администраторите или обработващите лични данни по отношение на изпълнението на задачите на ДЛЗД;

• не се допуска освобождаване от длъжност от страна на администратора във връзка с изпълнението на задачите на ДЛЗД;

• не се допуска конфликт на интереси с евентуални други задачи и задължения.

Другите задачи и задължения на ДЛЗД не трябва да водят до конфликт на интереси. Първо, това означава, че ДЛЗД не може да заема длъжност в рамките на организацията, която ще го задължава да определя целите и средствата за обработването на лични данни. Поради специфичната организационна структура във всяка организация, този аспект трябва да се разглежда на база конкретен случай.

Длъжностите в рамките на организацията, които влизат в противоречие, по общо правило може да включват длъжности във висшето ръководство (като главен изпълнителен директор, главен оперативен директор, главен финансов директор, главен медицински директор, ръководител на маркетингов отдел, ръководител на отдел „Човешки ресурси“ или ръководител на ИТ отдел), но също така и други функции по-надолу в организационната структура, ако въпросните длъжности или функции са свързани с определяне на целите и средствата за обработване на данните. Освен това конфликт на интереси може да възникне също така например, ако външно ДЛЗД бъде поканено да представлява администратора или обработващия лични данни пред съдилищата по дела, касаещи теми по защита на данните.

Източник: член 38, параграфи 3 и 6 от ОРЗД

Задачи на ДЛЗД

11. Какво означава „наблюдение на спазването“?

В рамките на задълженията за наблюдение на спазването ДЛЗД може по-специално:

• да събира информация за определяне на дейностите по обработване;

• да анализира и проверява спазването на дейностите по обработване;

• да информира, съветва и отправя препоръки към администратора или обработващия лични данни.

Източник: член 39, параграф 1, буква б) от ОРЗД

12. Носи ли ДЛЗД лична отговорност в случай на неспазване на изискванията за защита на данните?

Не. ДЛЗД не носят лична отговорност в случай на неспазване на изискванията за защита на данните. Администраторът или обработващият лични данни е този, който е длъжен да гарантира и да бъде в състояние да докаже, че обработването се извършва в съответствие с този регламент. Спазването на разпоредбите за защита на данните е отговорност на администратора или обработващия лични данни.

13. Каква е ролята на ДЛЗД във връзка с оценките на въздействието върху защитата на данните и регистрите на дейностите по обработване?

Що се отнася до оценката на въздействието върху защитата на данните, администраторът или обработващият лични данни следва да иска становището на ДЛЗД по следните въпроси, наред с други:

• дали да извърши ОВЗД или не;

• каква методика да използва при извършването на ОВЗД;

• дали да извърши ОВЗД вътрешно или да я възложи на външен изпълнител;

• какви гаранции (включително технически и организационни мерки) да приложи, за да намали до минимум всички рискове за правата и интересите на субектите на данните;

• дали оценката на въздействието върху защитата на данните е извършена правилно и дали заключенията от нея (дали да се продължи с обработването и какви гаранции да се приложат) съответстват на изискванията за защита на данните.

Що се отнася до регистрите на дейностите по обработване, администраторът или обработващият лични данни, а не ДЛЗД, е този, който е длъжен да поддържа регистри на операциите по обработване. Нищо обаче не пречи на администратора или обработващия лични данни да възложи на ДЛЗД задачата да води регистри на операциите по обработване, за които отговаря администраторът или обработващият лични данни. Тези регистри следва да се считат за един от инструментите, даващи възможност на ДЛЗД да изпълнява неговите задачи по наблюдение на спазването, информиране и съветване на администратора или обработващия лични данни.

Източник: член 39, параграф 1, буква в) и член 30 от ОРЗД.

НАСОКИ НА РАБОТНА ГРУПА ПО ЧЛ. 29 ОТ ДИРЕКТИВА 95/46/ЕО ОТНОСНО ОЦЕНКАТА НА ВЪЗДЕЙСТВИЕТО ВЪРХУ ЗАЩИТАТА НА ДАННИ (ОВЗД) И ОПРЕДЕЛЯНЕ ДАЛИ СЪЩЕСТВУВА ВЕРОЯТНОСТ ОБРАБОТВАНЕТО ДА ПОРОДИ "ВИСОК РИСК" ЗА ЦЕЛИТЕ НА РЕГЛАМЕНТ 2016/679

I.Въведение

Регламент 2016/679[1] (ОРЗД) ще се прилага от 25 май 2018 г. С член 35 от ОРЗД се въвежда понятието за оценка на въздействието върху защитата на данните (ОВЗД)[2], което се съдържа и в Директива 2016/680[3].

ОВЗД представлява процес, чиято цел е да опише обработването, да оцени неговата необходимост и пропорционалност и да спомогне за управлението на рисковете за правата и свободите на физическите лица, произтичащи от обработването на лични данни[4], като ги оцени и определи мерки за справяне с тези рискове. ОВЗД представляват важен инструмент за отчетност, тъй като помагат на администраторите на лични данни не само да спазят изискванията на ОРЗД, но и да демонстрират, че са предприети подходящи мерки за гарантиране на спазването на Регламента

1 Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. 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/EG (Общ регламент относно защитата на данните).

2 Изразът „оценка на въздействието върху неприкосновеността на личния живот" (ОВНЛЖ) често се използва в други видове контекст за обозначаване на същото понятие.

3 В член 27 от Директива (ЕС) 2016/680 на Европейския парламент и на Съвета от 27 април 2016 г. 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 също се посочва, че е необходима оценка на въздействието върху неприкосновеността на личния живот, тъй като съществува вероятност обработването „да породи висок риск за правата и свободите на физическите лица".

4 ОРЗД не съдържа официално определение на понятието ОВЗД, но

- минималното му съдържание е посочено в член 35, параграф 7, както следва:

а) системен опис на предвидените операции по обработване и целите на обработването, включително, ако е приложимо, преследвания от администратора законен интерес;

б) оценка на необходимостта и пропорционалността на операциите по обработване по отношение на целите;

в) оценка на рисковете за правата и свободите на субектите на данни, посочени в параграф 1; и

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.";

- значението и ролята му са пояснени в съображение 84, както следва: „За да се подобри спазването на настоящия регламент, когато има вероятност операциите по обработването да доведат до висок риск за правата и свободите на физическите лица, администраторът следва да отговаря за изготвянето на оценка на въздействието върху защитата на личните данни, за да се оценят по-специално произходът, естеството, спецификата и степента на този риск".

(вж. също така член 24[5]). С други думи **ОВЗД е процес за осигуряване и доказване на спазването на изискванията.**

Съгласно ОРЗД неспазването на изискванията за ОВЗД може да доведе до налагане на глоби от компетентния надзорен орган. Ако не бъде извършена ОВЗД, когато обработването подлежи на ОВЗД (член 35, параграфи 1, 3 и 4), ако ОВЗД бъде извършена неправилно (член 35, параграфи 2, 7 и 9) или ако не бъде проведена консултация с компетентния надзорен орган, когато това се изисква (член 36, параграф 3, буква д), това може да доведе до налагането на административна глоба в размер до 10 милиона евро или, в случай на предприятие, до 2 % от общия му годишен световен оборот за предходната финансова година, която от двете суми е по-висока.

II. Приложно поле на насоките

В настоящите насоки се вземат предвид:

- Изявлението на работната група за защита на личните данни по член 29 (РГ29), 14/EN WP 218[6];
- Насоките на РГ29 относно длъжностните лица по защита на данните, 16/EN WP 243[7];
- Становището на РГ29 относно ограничаването в рамките на целта, 13/EN WP 203[8];
- международни стандарти[9].

В съответствие с основания на анализ на риска подход, залегнал в ОРЗД, извършването на ОВЗД не е задължително за всяка операция по обработване. ОВЗД се изисква само когато съществува вероятност обработването *„да породи висок риск за правата и свободите на физическите лица“* (член 35, параграф 1). За да се гарантира последователно тълкуване на обстоятелствата, при които е задължително да се извърши ОВЗД (член 35, параграф 3), целта на настоящите насоки на първо място е да се поясни това понятие и да се осигурят критерии за списъците, които трябва да бъдат приети от органите по защита на данните (ОЗД) съгласно член 35, параграф 4.

Съгласно член 70, параграф 1, буква д) Европейският комитет по защита на данните (ЕКЗД) ще може да издава насоки, препоръки и най-добри практики с цел насърчаване на съгласуваното прилагане на ОРЗД. Целта на настоящия документ е да се създаде основа за такава бъдеща работа на ЕКЗД и в тази връзка да се пояснят съответните разпоредби от ОРЗД, за да се помогне на администраторите да спазят правните разпоредби и да се осигури правна сигурност за администраторите, които следва да извършват ОВЗД.

Настоящите насоки също така целят да насърчат разработването на:

- общ списък на операциите по обработване в Европейския съюз, за които е задължително да се извърши ОВЗД (член 35, параграф 4);
- общ списък на операциите по обработване в ЕС, за които не е задължително да се извърши ОВЗД (член 35, параграф 5);
- общи критерии относно методологията за извършване на ОВЗД (член 35, параграф 5);
- общи критерии за уточняване в кои случаи следва да се провежда консултация с надзорния орган (член 36, параграф 1);
- препоръки, когато е възможно, в които се доразвива опитът, придобит от държавите членки на ЕС.

---

5 Вж. също така съображение 84: „Резултатите от оценката следва да бъдат взети предвид, когато се определят съответните мерки, за да се докаже, че обработването на лични данни отговаря на изискванията на настоящия регламент“.

6 Изявление на РГ29 относно ролята на основания на анализ на риска подход към правните рамки за защита на данните, 14/EN WP 218, прието на 30 май 2014 г. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf?wb48617274=72C54532

7 Насоки на РГ29 относно длъжностните лица по защита на данните, 16/EN WP 243, приети на 13 декември 2016 г. http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf?wb48617274=CD63BD9A

8 Становище 03/2013 на РГ 29 относно ограничаването в рамките на целта, 13/EN WP 203, прието на 2 април 2013 г. http://ec.europa.eu/iustice/data-protection/article-29/documentation/opinion- recommendation/files/2013/wp203 en.pdf

9 Например ISO 31000:2009, Управление на риска. Принципи и указания, Международна организация по стандартизация (ISO); ISO/IEC 29134 (проект), Информационни технологии. Техники за сигурност. Оценка на въздействието върху неприкосновеността на личния живот. Указания, Международна организация по стандартизация (ISO)..

III. ОВЗД: обяснение на Регламента

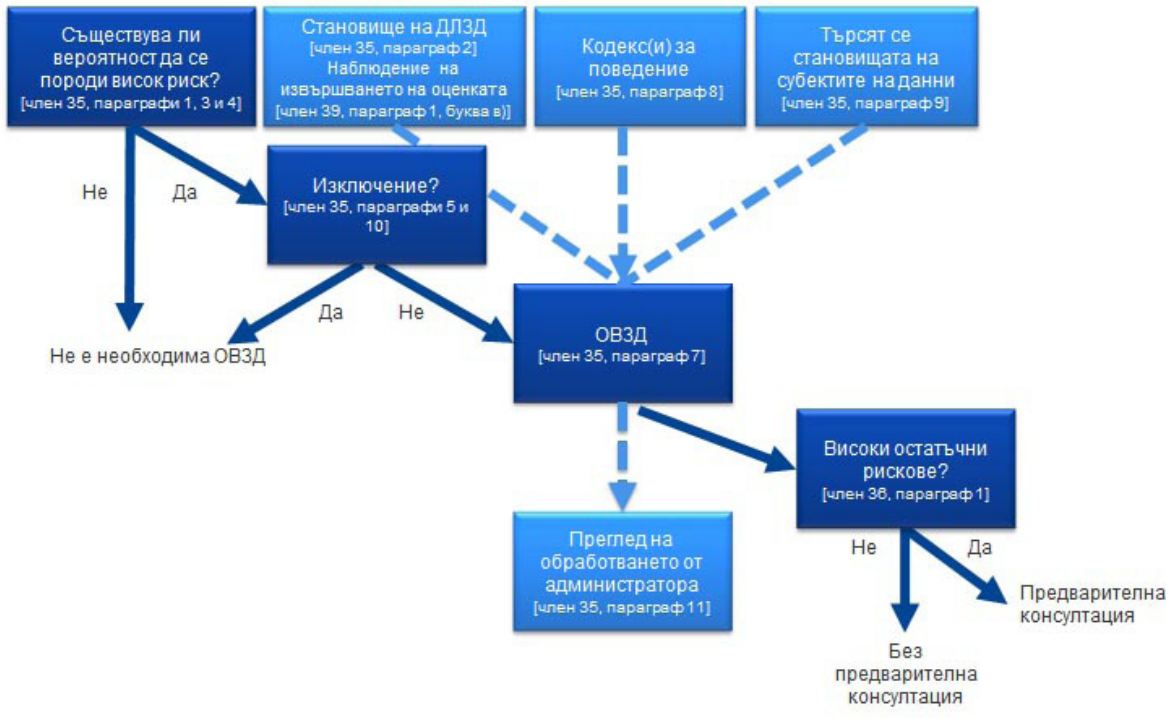
Съгласно ОРЗД администраторите са длъжни да въведат подходящи мерки, за да гарантират и да бъдат в състояние да докажат, че спазват ОРЗД, като вземат предвид, наред с другото, „рисковете с различна вероятност и тежест за правата и свободите на физическите лица“ (член 24, параграф 1). Задължението на администраторите да извършват ОВЗД при определени обстоятелства следва да се разбира в контекста на общото им задължение да управляват по подходящ начин рисковете[10], породени от обработването на лични данни.

„Риск“ означава сценарий, описващ дадено събитие и неговите последици, оценени от гледна точка на тяхната тежест и вероятност. От друга страна „управление на риска“ може да се определи като координирани дейности за ръководенето и контролирането на дадена организация във връзка с риска.

В член 35 се посочва вероятността от висок риск „за правата и свободите на физическите лица“. Както се посочва в изготвеното от Работната група за защита на личните данни по член 29 изявление относно ролята на основания на анализ на риска подход към правните рамки за защита на данните, посочването на „правата и свободите“ на субектите на данни е свързано най-вече с правата за защитата на личните данни и неприкосновеността на личния живот, но може да включва и други основни права, като например свободата на словото, свободата на мисълта, свободата на движение, забраната за дискриминация, правото на свобода и свободата на съвестта и религията.

В съответствие с основания на анализ на риска подход, залегнал в ОРЗД, извършването на ОВЗД не е задължително за всяка операция по обработване. Вместо това ОВЗД се изисква само когато съществува вероятност определен вид обработване „да породи висок риск за правата и свободите на физическите лица“ (член 35, параграф 1). При все това самият факт, че не са налице условията, при които извършването на ОВЗД е задължително, не намалява общото задължение на администраторите да въведат мерки, за да управляват по подходящ начин рисковете за правата и свободите на субектите на данни. На практика това означава, че администраторите трябва непрекъснато да оценяват рисковете, които се пораждат от техните дейности по обработване, за да идентифицират кога съществува вероятност определен вид обработване „да породи висок риск за правата и свободите на физическите лица“.

Следната фигура илюстрира основните принципи, свързани с ОВЗД в ОРЗД:



10 Трябва да се подчертае, че с цел управление на рисковете за правата и свободите на физическите лица тези рискове трябва редовно да се идентифицират, анализират, преценяват, оценяват, третират (например като се ограничават...) и преразглеждат. Администраторите не могат да избегнат своята отговорност, като сключват застрахователни полици за покритие на рисковете.

А. Към какво е насочена ОВЗД? Една-единствена операция по обработване или набор от сходни операции по обработване.

ОВЗД може да е свързана с една-единствена операция по обработване на данни. При все това член 35, параграф 1 гласи, че *„в една оценка може да бъде разгледан набор от сходни операции по обработване, които представляват сходни високи рискове“* В съображение 92 се добавя, че *„при определени обстоятелства може да бъде разумно и рентабилно предметът на дадена оценка на въздействието върху защитата на данните да обхваща повече от един проект, например когато обществени органи или структури възнамеряват да създадат общо приложение или платформа за обработване на данни или когато няколко администратори планират внедряването на общо приложение или среда за обработване на данните в цял промишлен сектор или сегмент или за широко използвана хоризонтална дейност“*.

Би могла да се използва една-единствена ОВЗД за оценяване на множество операции по обработване, които са сходни по своето естество, обхват, контекст, цел и рискове. В действителност ОВЗД целят систематичното проучване на нови ситуации, които биха могли да доведат до високи рискове за правата и свободите на физическите лица, и не е нужно да се извършва ОВЗД в случаите (т.е. операции по обработване, извършвани в определен контекст и за конкретна цел), които вече са проучени. Такъв може да бъде случаят, когато се използва сходна технология за събирането на един и същ вид данни за едни и същи цели. Например група от общински органи, всеки от които създава сходна система за видеонаблюдение, би могла да извърши една-единствена ОВЗД, която обхваща обработването от отделните администратори, или железопътен оператор (един-единствен администратор) би могъл да обхване видеонаблюдението на всички свои железопътни гари с една ОВЗД. Това може да бъде приложимо и към сходни операции по обработване, извършвани от различни администратори. В такива случаи следва да бъде споделена референтна ОВЗД или да бъде направена публично достъпна, като описаните в ОВЗД мерки трябва да бъдат изпълнени и трябва да бъде представена обосновка за извършването само на една-единствена ОВЗД.

Когато операцията по обработване включва съвместни администратори, те трябва да определят прецизно своите задължения. В тяхната ОВЗД следва да се посочва коя страна отговаря за различните мерки за третиране на рисковете и за защита на правата и свободите на субектите на данни. Всеки администратор следва да посочи своите потребности и да споделя полезна информация, без да разкрива тайни (например защита на търговски тайни, интелектуална собственост, поверителна търговска информация) или да оповестява слабости.

ОВЗД също така може да бъде полезна за оценяване на въздействието върху защитата на данните на даден технологичен продукт, например хардуер или софтуер, когато има вероятност той да се използва от различни администратори за извършване на различни операции по обработване. Естествено администраторът, който въвежда продукта, продължава да носи отговорност за извършването на своя ОВЗД по отношение на конкретното изпълнение, но при нейното извършване той може да използва като основа изготвена от доставчика на продукта ОВЗД, ако е целесъобразно. Като пример могат да бъдат посочени отношенията между производителите на интелигентни измервателни уреди и дружествата за комунални услуги. Всеки доставчик на продукт или обработващ лични данни следва да споделя полезна информация, без да разкрива тайни или да създава рискове за сигурността, като оповестява слабости.

Б. Кои операции по обработване подлежат на ОВЗД? Освен изключенията, всяка операция, при която съществува вероятност „да породи висок риск‘.

В настоящия раздел се описва кога ОВЗД е задължителна и кога не е необходимо да се извършва ОВЗД.

Освен ако операцията по обработване не отговаря на едно от изключенията (Ш.Б.а), трябва да се извърши ОВЗД, когато съществува вероятност операцията по обработване *„да породи висок риск*“ (Ш.Б.б).

а) Кога задължително се извършва ОВЗД? Когато съществува вероятност обработването *„да породи висок риск*“.

Съгласно ОРЗД не се изисква да се извършва ОВЗД за всяка операция по обработване, която може да породи рискове за правата и свободите на физическите лица. Извършването на ОВЗД е задължително само когато съществува вероятност обработването *„да породи висок риск за правата и свободите на физическите лица*“ (член 35, параграф 1, както е илюстрирано в член 35, параграф 3 и допълнено от член 35, параграф 4). Това е от особено значение, когато се въвежда нова технология за обработване на данни[11].

В случаите, когато не е ясно дали се изисква ОВЗД, РГ29 препоръчва все пак да се извърши ОВЗД, тъй като тя представлява полезен инструмент, който помага на администраторите да спазват законодателството в областта на защитата на данните.

Въпреки че ОВЗД може да се изисква и при други обстоятелства, в член 35, параграф 3 се посочват някои примери кога съществува вероятност операцията по обработване „да породи висок риск“:

- „а) систематична и подробна оценка на личните аспекти по отношение на физически лица, която се базира на автоматично обработване, включително профилиране, и служи за основа на решения, които имат правни последици за физическото лице или по подобен начин сериозно засягат физическото лице[12];

- б) мащабно обработване на специални категории данни, посочени в член 9, параграф 1 или на лични данни за присъди и нарушения по член 10[13]; или

- в) систематично мащабно наблюдение на публично достъпна зона“

Както става ясно от израза „по-специално“ в уводното изречение на член 35, параграф 3 от ОРЗД, посоченият списък не е изчерпателен. Възможно е да съществуват „високорискови“ операции по обработване, които да не са включени в този списък, но да пораждат сходен „висок риск“. Такива операции по обработване също следва да подлежат на ОВЗД. Поради тази причина в някои случаи изложените по-долу критерии са нещо повече от просто обяснение на това, което следва да се разбира от трите примера, дадени в член 35, параграф 3 от ОРЗД.

С оглед да се представи по-конкретен набор от операции по обработване, при които трябва да се извърши ОВЗД поради присъщия за тях висок риск, като се вземат предвид конкретните елементи на член 35, параграф 1 и член 35, параграф 3, букви а)−в), списъкът, който следва да бъде приет на национално равнище съгласно член 35, параграф 4, и съображения 71, 75 и 91, както и други препратки в ОРЗД към операции по обработване, които *„има вероятност да доведат до висок риск*“[14], следва да се вземат под внимание следните девет критерия.

1. Оценка или точкуване, включително профилиране и прогнозиране, по-специално от *„аспекти, имащи отношение към резултатите в работата на субекта на данни, икономическото състояние, здравето, личните предпочитания или интереси, благонадеждността или поведението,*

11 Вж. съображения 89, 91 и член 35, параграфи 1 и 3 за допълнителни примери.

12 Вж. съображение 75: „по-специално анализиране или прогнозиране на аспекти, отнасящи се до представянето на работното място, икономическото положение, здравето, личните предпочитания или интереси, надеждността или поведението, местонахождението или движенията в пространството, с цел създаване или използване на лични профили“.

13 Вж. съображение 75: „когато се обработват лични данни, които разкриват расов или етнически произход, политически възгледи, религиозни или философски убеждения, членство в професионална организация, и обработването на генетични данни, данни за здравословното състояние или данни за сексуалния живот или за присъди и нарушения или свързани с тях мерки за сигурност“.

14 Вж. например съображения 75, 76, 92, 116.

местоположението или движенията“ (съображения 71 и 91). Примерите за това биха могли да включват финансови институции, които извършват справки за своите клиенти в референтна база данни за кредити, в база данни за борба срещу изпирането на пари или финансирането на тероризма или в база данни за борба с измамите, биотехнологични компании, които предлагат генетични тестове директно на клиенти, за да оценят и прогнозират рисковете от заболявания/здравните рискове, или компании, които създават поведенчески или маркетингови профили въз основа на използването на техния уебсайт или навигацията в него.

2. Автоматизирано вземане на решения с правни последици или подобни сериозни последици: обработване с цел вземане на засягащи субектите на данни решения, които имат „*правни последици за физическото лице“ или „по подобен начин сериозно засягат физическото лице*“ (член 35, параграф 3, буква а). Например обработването може да доведе до изключване или дискриминация на физически лица. Обработването с незначителни последици или без последици за физическите лица не отговаря на този конкретен критерий. Допълнителни обяснения за тези понятия ще бъдат дадени в предстоящите Насоки на РГ29 относно профилирането.

3. Систематично наблюдение: обработване, което се използва за наблюдение, мониторинг или контрол на субектите на данни, включително данни, които се събират чрез мрежи, или „*систематично мащабно наблюдение на публично достъпна зона*“ (член 35, параграф 3, буква в))[15]. Този вид наблюдение е включен като критерий, защото е възможно да се събират лични данни при обстоятелства, когато субектите на данни може да не осъзнават кой събира техните данни и как ще бъдат използвани. Освен това за физическите лица може да е невъзможно да избегнат подлагането на такова обработване в публична (или публично достъпна) зона.

4. Чувствителни данни или данни от изключително лично естество: това включва специални категории лични данни, определени в член 9 (например информация относно политическите възгледи на физическите лица), както и лични данни, свързани с присъди и нарушения по смисъла на член 10. Пример за това биха били обществени болници, които съхраняват медицинските досиета на пациентите, или частни детективи, които съхраняват данните на нарушителите. Отвъд тези разпоредби на ОРЗД, за някои категории данни може да се счита, че увеличават евентуалния риск за правата и свободите на физическите лица. Тези лични данни се считат за чувствителни (по начина, по който се възприема обикновено този термин), защото са свързани с домашни и лични занимания (като например електронни съобщения, чиято поверителност следва да бъде защитена) или защото засягат упражняването на основно право (като например данни за местонахождението, събирането на които поставя под въпрос свободата на движение), или защото нарушенията във връзка с тях очевидно биха довели до сериозно въздействие върху ежедневието на субекта на данни (като например финансови данни, които могат да се използват за измами при плащания). В тази връзка може да е от значение дали данните вече са обявени публично от съответното физическо лице или от трети страни. Фактът, че личните данни са публично достъпни, може да се разгледа като фактор в оценката, ако се е очаквало данните да се използват допълнително за определени цели. Този критерий също така може да включва данни, като например лични документи, електронни писма, дневници, бележки от електронни четци, които позволяват водене на бележки, и изключително личната информация, записвана от приложения, в които се отбелязват събития от живота.

5. Мащабно обработване на данни: в ОРЗД не се определя какво означава мащабно, въпреки че съображение 91 съдържа известни насоки. Във всеки случай РГ29 препоръчва да се проучат

15 Съгласно тълкуването на РГ29“систематично“ е наблюдението, което отговаря на един или повече от следните критерии (вж. Насоки на РГ29 относно длъжностните лица по защита на данните, 16/EN WP 243):
- извършва се в съответствие с дадена система;
- предварително установено е, организирано е или е методично;
- извършва се като част от общ план за събиране на данни;
- извършва се като част от стратегия.

Съгласно тълкуването на РГ29 „публично достъпна зона“ е всяко място, достъпно за гражданите, например площад, търговски център, улица, пазар, железопътна гара или обществена библиотека.

по-специално следните фактори, когато се определя дали извършваното обработване е мащабно[16]:

а. броят на засегнатите субекти на данни като конкретна цифра или като дял от съответното население;

б. обемът на данните и/или обхватът на различните видове данни, които се обработват;

в. продължителността или непрекъснатостта на дейността по обработване на данните;

г. географският обхват на дейността по обработване.

6. Търсене на съвпадение или съчетаване на набори от данни, например с произход от две или повече операции по обработване на данни, извършени за различни цели и/или от различни администратори, по начин, който надхвърля разумните очаквания на субекта на данни[17].

7. Данни относно уязвими субекти на данни (съображение 75): обработването на този вид данни е включено като критерий поради увеличената неравнопоставеност на правомощията между субектите на данни и администратора, което означава, че физическите лица може да не са в състояние лесно да се съгласят или да възразят срещу обработването на техните данни, или да упражнят своите права. Уязвимите субекти на данни могат да включват деца (може да се счита, че те не са в състояние съзнателно и мотивирано да възразят срещу или да се съгласят с обработването на техните данни), служители, по-уязвими сегменти от населението, които се нуждаят от специална защита (психично болни лица, търсещи убежище лица или възрастни лица, пациенти и др.) и субекти на данни във всички случаи, при които може да се установи неравнопоставеност в отношенията с оглед на положението на субекта на данни и това на администратора.

8. Иновативно използване или прилагане на нови технологични или организационни решения, като например съчетаване на използването на пръстови отпечатъци и разпознаване на лица с цел подобряване на контрола на физическия достъп и др. В ОРЗД ясно се посочва (член 35, параграф 1 и съображения 89 и 91), че използването на нова технология, определена „*в съответствие с постигнатото ниво на технически познания*“ (съображение 91), може да доведе до необходимост от извършване на ОВЗД. Причината за това е, че използването на такава технология може да включва нови форми на събиране и използване на данни, което евентуално води до висок риск за правата и свободите на физическите лица. В действителност личните и социалните последици от внедряването на нова технология може да не са известни. ОВЗД ще помогне на администратора да разбере и да третира тези рискове. Например някои приложения, свързани с „интернет на предметите“, биха могли да окажат значително въздействие върху ежедневния живот на физическите лица и неговата неприкосновеност; и поради това изискват ОВЗД.

9. Когато операциите по обработването сами по себе си „*възпрепятстват субектите на данни да упражняват дадено право или да използват някоя услуга или договор*“ (член 22 и съображение 91). Това включва операции по обработване, чиято цел е да се позволи, измени или откаже достъпът на субектите на данни до услуга или сключването на договор. Пример за това са банки, които извършват справки за своите клиенти в референтна база данни за кредити, за да решат дали да им предложат кредит.

В повечето случаи администраторът може да заключи, че ако обработването отговаря на два критерия, ще се изисква извършването на ОВЗД. Като цяло РГ29 счита, че на колкото повече критерии отговаря обработването, толкова по-вероятно е да поражда висок риск за правата и свободите на субектите на данни, поради което ще изисква ОВЗД независимо от мерките, които администраторът планира да въведе.

При все това в някои случаи **администраторът може да заключи, че обработване, което отговаря само на един от тези критерии, изисква ОВЗД.**

Следните примери илюстрират как следва да се използват критериите, за да се оцени дали конкретна операция по обработване изисква ОВЗД:

16 Вж. Насоки на РГ29 относно длъжностните лица по защита на данните, 16/EN WP 243.

17 Вж. обяснението в становището на РГ29 относно ограничаването в рамките на целта, 13/EN WP 203, стр. 24.

Примери за обработване	Евентуално приложими критерии	Има ли вероятност да се изисква ОВЗД?
Болница, която обработва генетичните и здравните данни на своите пациенти (информационна система на болницата).	- Чувствителни данни или данни от изключително лично естество. - Данни относно уязвими субекти на данни. - Мащабно обработване на данни.	ДА
Използване на система от камери за наблюдение на поведението на шофьорите на магистралите. Администраторът предвижда да използва интелигентна система за видеоанализ за идентифициране на отделни автомобили и автоматично разпознаване на регистрационни номера.	- Систематично наблюдение. - Иновативно използване или прилагане на технологични или организационни решения.	
Дружество, което осъществява систематично наблюдение на дейностите на своите служители, включително наблюдение на работните станции на служителите, дейността им в интернет и др	- Систематично наблюдение. - Данни относно уязвими субекти на данни.	
Събиране на публични данни от социални мрежи с цел изготвяне на профили.	- Оценка или точкуване. - Мащабно обработване на данни. - Търсене на съвпадение или съчетаване на набори от данни. - Чувствителни данни или данни от изключително лично естество.	
Институция, която създава база данни за кредитен рейтинг или за борба с измамите на национално равнище.	- Оценка или точкуване. - Автоматизирано вземане на решения с правни последици или подобни сериозни последици. - Възпрепятства субект на данни да упражнява дадено право или да използва някоя услуга или договор. - Чувствителни данни или данни от изключително лично естество.	
Съхранение с цел архивиране на псевдонимизирани чувствителни лични данни относно уязвими субекти на данни, които са участвали в научноизследователски проекти или клинични изпитвания.	- Чувствителни данни. - Данни относно уязвими субекти на данни. - Възпрепятства субекти на данни да упражняват дадено право или да използват някоя услуга или договор.	

Примери за обработване	Евентуално приложими критерии	Има ли вероятност да се изисква ОВЗД?
Обработване на „лични данни на пациенти или клиенти на отделен лекар, друг здравен работник или адвокат" (съображение 91).	- Чувствителни данни или данни от изключително лично естество. - Данни относно уязвими субекти на данни.	**НЕ**
Онлайн списание, което използва списък с адресати, за да изпраща общо резюме с информация на своите абонати.	- Мащабно обработване на данни.	
Уебсайт за електронна търговия, на който се показват реклами за части за стари модели автомобили, което включва ограничено профилиране въз основа на разглежданите или закупените артикули на самия уебсайт.	- Оценка или точкуване.	

От друга страна, дадена операция по обработване може да отговаря на горепосочените случаи и все пак администраторът да заключи, че не „съществува вероятност да породи висок риск". В такива случаи администраторът следва да обоснове и документира причините, поради които не извършва ОВЗД, и да включи/отбележи възгледите на длъжностното лице по защита на данните.

Освен това като част от принципа на отчетност всеки администратор „*поддържа регистър на дейностите по обработване, за които отговаря*", включително, наред с другото, целите на обработването, описание на категориите данни и получателите на данните, както и „*когато е възможно, общо описание на техническите и организационни мерки за сигурност, посочени в член 32, параграф 1*" (член 30, параграф 1), и трябва да оцени дали съществува вероятност да се породи висок риск, дори ако в крайна сметка реши да не извърши ОВЗД.

Забележка: надзорните органи са длъжни да съставят, оповестят публично и да съобщят списък на операциите по обработване, за които се изисква ОВЗД, на Европейския комитет по защита на данните (ЕКЗД) (член 35, параграф 4)[18]. Горепосочените критерии могат да помогнат на надзорните органи да съставят този списък, като по целесъобразност с времето ще се добавя по- конкретно съдържание. Например обработването на всички видове биометрични данни или данни на деца също би могло да се счита за подходящо за съставянето на списък в съответствие с член 35, параграф 4.

б) Кога не се изисква ОВЗД? Когато не съществува вероятност обработването „*да породи висок риск*" или вече съществува сходна ОВЗД, или обработването е било разрешено преди май 2018 г., или за него има правно основание, или е включено в списъка с операции по обработване, за които не се изисква ОВЗД.

РГ29 счита, че не се изисква ОВЗД в следните случаи:

- **когато не съществува вероятност обработването *„да породи висок риск за правата и свободите на физическите лица"*** (член 35, параграф 1);

18 В този контекст „компетентният надзорен орган прилага посочения в член 63 механизъм за съгласуваност, ако тези списъци включват дейности за обработване, свързани с предлагането на стоки или услуги на субекти на данни или с наблюдението на тяхното поведение в няколко държави членки или могат съществено да засегнат свободното движение на лични данни в рамките на Съюза" (член 35, параграф 6).

- **когато естеството, обхватът, контекстът и целите на обработването са много сходни с тези на обработването, за което е извършена ОВЗД.** В тези случаи могат да се използват резултатите от ОВЗД за сходни операции по обработване (член 35, параграф 1[19]);

- когато операциите по обработване са били проверени от надзорен орган преди май 2018 г. при конкретни условия, които не са се променили[20] (вж. Ш.В);

- **когато операция по обработване** съгласно член 6, параграф 1, буква в) или д) **има правно основание** в правото на Съюза или в правото на държавата членка, когато това право регулира конкретната операция по обработване **и когато вече е извършена ОВЗД** като част от установяването на това правно основание (член 35, параграф 10)[21], освен ако държавата членка не сметне за необходимо да извърши ОВЗД преди започването на дейностите за обработване;

- **когато обработването е включено в незадължителния списък (съставен от надзорния орган) с операции по обработване,** за които не се изисква ОВЗД (член 35, параграф 5). Този списък може да включва дейности по обработване, които отговарят на условията, посочени от този орган, по-специално чрез насоки, конкретни решения или разрешения, правила за спазване и други (например във Франция − разрешения, изключения, опростени правила, набори от правила за спазване...). В тези случаи и съгласно повторната оценка от компетентния надзорен орган не се изисква ОВЗД, но само ако обработването попада изцяло в обхвата на съответната процедура, посочена в списъка, и продължава да отговаря напълно на всички съответни изисквания на ОРЗД.

В. Как се процедира при вече съществуващи операции по обработване? При определени обстоятелства се изисква ОВЗД.

Изискването за извършване на ОВЗД се прилага към съществуващи операции по обработване, при които съществува вероятност да породят висок риск за правата и свободите на физическите лица и по отношение на които е настъпила промяна в рисковете, като се вземат предвид естеството, обхватът, контекстът и целите на обработването.

ОВЗД не е необходима за операции по обработване, които са били проверени от надзорен орган или от длъжностното лице по защита на данните в съответствие с член 20 от Директива 95/46/ЕО и които се извършват по начин, който не се е променил след предишната проверка. В действителност „*приетите от Комисията решения и разрешенията на надзорните органи въз основа на Директива 95/46/ЕО остават в сила, докато не бъдат изменени, заменени или отменени*“ (*съображение 171*).

От друга страна това означава, че на ОВЗД следва да подлежи всяко обработване на данни, чиито условия за изпълнение (обхват, цел, събрани лични данни, самоличност на администраторите или получателите, срок на задържане на данните, технически и организационни мерки и др.) са се променили след предишната проверка, извършена от надзорния орган или от длъжностното лице по защита на данните, и при което съществува вероятност да породи висок риск.

Освен това би могла да се изисква ОВЗД след промяна в рисковете, породени от операциите по обработване[22], например защото започва да се използва нова технология или защото личните данни се използват за различна цел. Операциите по обработване на данни могат да се развият бързо и могат да възникнат нови слабости. Поради това следва да се отбележи, че преразглеждането на

19 „В една оценка може да бъде разгледан набор от сходни операции по обработване, които представляват сходни високи рискове“.

20 „Приетите от Комисията решения и разрешенията на надзорните органи въз основа на Директива 95/46/ЕО остават в сила, докато не бъдат изменени, заменени или отменени“ (съображение 171).

21 Когато ОВЗД се извършва на етапа на изготвяне на законодателството, което включва правното основание за обработване, съществува вероятност да се наложи преразглеждане на оценката преди започването на операциите, тъй като приетото законодателство може да се различава от предложението по начин, който оказва въздействие върху въпросите относно неприкосновеността на личния живот и защитата на данните. Освен това към момента на приемане на законодателството е възможно да не са налични достатъчни технически подробности по отношение на действителното обработване, дори ако се придружава от ОВЗД. В такива случаи може все пак да е необходимо да се извърши конкретна ОВЗД преди осъществяването на действителните дейности по обработване.

22 От гледна точка на контекста, събраните данни, целите, функциите, обработените лични данни, получателите, комбинациите от данни, рисковете (помощни елементи, източници на риск, потенциални въздействия, заплахи и др.), мерките за сигурност и международното предаване на данни.

ОВЗД не само е от полза за постигането на постоянни подобрения, но е от решаващо значение за поддържането на същото равнище на защита на данните в условията на променяща се с времето среда. ОВЗД може да стане необходима и поради промяна в организационния или обществения контекст за дейността по обработване, например защото последиците от определени автоматизирани решения са станали по-сериозни или защото нови категории субекти на данни са станали уязвими на дискриминация. Всеки от тези примери би могъл да представлява елемент, който води до промяна на риска, произтичащ от съответната дейност по обработване.

От друга страна някои промени също така биха могли да понижат риска. Например дадена операция по обработване може да се развие по такъв начин, че решенията вече да не са автоматизирани или, в случай на дейност по наблюдение, то вече да не е систематично. В такъв случай преразглеждането на извършения анализ на риска може да покаже, че вече не се изисква извършване на ОВЗД.

Съгласно добрата практика **ОВЗД следва постоянно да се преразглежда и да подлежи на редовна повторна оценка.** Поради това дори ако към 25 май 2018 г. не се изисква ОВЗД, в подходящ момент администраторът ще трябва да извърши такава ОВЗД като част от общите си задължения за отчетност.

Г. Как следва да бъде извършена ОВЗД?

а) В кой момент следва да бъде извършена ОВЗД? Преди да бъде извършено обработването.

ОВЗД следва да бъде извършена „преди да бъде извършено обработването“ (член 35, параграфи 1 и 10, съображения 90 и 93)[23]. Това съответства на принципите за защита на данните на етапа на проектирането и по подразбиране (член 25 и съображение 78). ОВЗД следва да се разглежда като инструмент, който подпомага вземането на решения относно обработването.

Извършването на ОВЗД следва да започне на възможно най-ранен етап от проектирането на операцията по обработване, дори ако някои от операциите по обработване все още не са известни. Актуализирането на ОВЗД през целия жизнен цикъл на проекта ще гарантира, че се отчитат защитата на данните и неприкосновеността на личния живот, което ще стимулира създаването на решения, с които се насърчава спазването. Освен това е възможно да бъде необходимо да се повторят отделните стъпки от оценката с напредването на процеса по разработване, защото подборът на определени технически или организационни мерки може да окаже въздействие върху тежестта и вероятността на рисковете, породени от обработването.

Фактът, че може да се наложи актуализиране на ОВЗД след реалното започване на обработването, не е основателна причина да се отложи или да не се извърши ОВЗД. ОВЗД е текущ процес, особено когато операцията по обработване е динамична и подлежи на текущи промени. **Извършването на ОВЗД е постоянен процес, а не еднократно действие.**

б) Кой е длъжен да извърши ОВЗД? Администраторът, заедно с длъжностното лице по защита на данните и обработващите лични данни.

Администраторът носи отговорност да гарантира, че се извършва ОВЗД (член 35, параграф 2). ОВЗД може да бъде извършена от друго лице в рамките на организацията или извън нея, но администраторът продължава да носи крайната отговорност за тази задача.

Администраторът също така трябва да поиска становището на длъжностното лице по защита на данните (ДЛЗД), когато такова е определено (член 35, параграф 2), като това становище и взетите от администратора решения следва да се документират в ОВЗД. ДЛЗД също така следва да наблюдава извършването на ОВЗД (член 39, параграф 1, буква в). Насоките на РГ29 относно длъжностните лица по защита на данните, 16/EN WP 243, съдържат допълнителни указания.

23 Освен когато става въпрос за вече съществуващо обработване, което е било проверено преди това от надзорния орган, като в този случай ОВЗД следва да бъде извършена преди осъществяването на значителни промени.

Ако обработването се извършва изцяло или частично от обработващ лични данни, **обработващият лични данни следва да подпомага администратора при извършването на ОВЗД** и да предостави цялата необходима информация (в съответствие с член 28, параграф 3, буква е).

Администраторът трябва да „*се обръща към субектите на данните или техните представители за становище*“ (член 35, параграф 9), „*когато е целесъобразно*“. РГ29 счита, че:

- тези становища биха могли да се потърсят по редица начини в зависимост от контекста (например общо проучване, свързано с целта и средствата на операцията по обработване, отправяне на въпрос към представителите на персонала или обичайните анкети, които се изпращат на бъдещите клиенти на администратора), за да се гарантира, че администраторът разполага със законно основание да обработва личните данни, с които е свързано търсенето на такива становища. Въпреки това следва да се отбележи, че съгласието за обработване на данните очевидно не представлява начин да се потърсят становищата на субектите на данни;

- ако окончателното решение на администратора се различава от становищата на субектите на данни, неговите причини да обработи данните или не следва да бъдат документирани;

- администраторът също така следва да документира своята обосновка да не потърси становищата на субектите на данни, ако реши, че това не е целесъобразно, например ако това би изложило на риск поверителността на бизнес плановете на дружеството или би било непропорционално или непрактично.

На последно място, добра практика представлява определянето и документирането на други специфични роли и отговорности в зависимост от вътрешната политика, процеси и правила, например:

- когато конкретни звена на дружеството могат да предлагат извършването на ОВЗД, тези звена следва впоследствие да предоставят данни за ОВЗД и да участват в процеса по валидиране на ОВЗД;

- по целесъобразност се препоръчва да се поиска становището на независими експерти от различни области[24] (адвокати, ИТ експерти, експерти по сигурността, социолози, експерти по етични стандарти и др.);

- ролите и отговорностите на обработващите лични данни трябва да бъдат определени в договор; и ОВЗД трябва да бъде извършена с помощта на обработващия лични данни, като отчита естеството на обработване и информацията, до която е осигурен достъп на обработващия лични данни (член 28, параграф 3, буква е);

- главният служител по сигурността на информацията (ГССИ), ако е назначен такъв, и ДЛЗД биха могли да предложат на администратора да извърши ОВЗД по отношение на конкретна операция по обработване и следва да помогнат на заинтересовани страни с методологията, да подпомогнат оценяването на качеството на оценката на риска и на въпроса дали остатъчният риск е приемлив, както и да се стремят към развиване на специфични познания за контекста, в който работи администраторът;

- главният служител по сигурността на информацията (ГССИ), ако е назначен такъв, и/или ИТ отделът следва да съдействат на администратора и биха могли да предложат извършването на ОВЗД по отношение на конкретна операция по обработване в зависимост от свързаните със сигурността или оперативните потребности.

в) Каква е методологията за извършване на ОВЗД? Различни методологии, но общи критерии.

В ОРЗД се определят минималните характеристики на ОВЗД (член 35, параграф 7 и съображения 84 и 90):

- *„опис на предвидените операции по обработване и целите на обработването „;*
- *„оценка на необходимостта и пропорционалността на операциите по обработване“;*
- *„оценка на рисковете за правата и свободите на субектите на данни“;*

24 Recommendations for a privacy impact assessment framework for the European Union (Препоръки за рамка на Европейския съюз за оценка на въздействието върху неприкосновеността на личния живот), документ D3: http://www.piafproiect.eu/ref/PIAF D3 final.pdf.

- *мерките, предвидени за:*
  - *„справяне с рисковете“;*
  - „демонстриране на спазването на настоящия регламент“.

Следната фигура илюстрира общия повтарящ се процес за извършване на ОВЗД[25]:

Спазването на кодекс за поведение (член 40) трябва да се вземе предвид (член 35, параграф 8), когато се оценява въздействието на дадена операция по обработване на данни. Това може да бъде от полза, за да се демонстрира, че са избрани или въведени подходящи мерки, при условие че кодексът за поведение е подходящ за операцията по обработване. Под внимание следва да се вземат и сертификатите, печатите и маркировките с цел да се демонстрира спазването на ОРЗД при операциите по обработване от страна на администраторите и обработващите лични данни (член 42), както и задължителните фирмени правила (ЗФП).

Всички съответни изисквания, определени в ОРЗД, осигуряват широка и обща рамка за планиране и извършване на ОВЗД. Практическото извършване на ОВЗД ще зависи от изискванията, определени в ОРЗД, които могат да бъдат допълнени от по-подробни практически насоки. Поради това извършването на ОВЗД е с променлив мащаб. Това означава, че дори администратор на малък обем данни може да планира и извърши ОВЗД, която е подходяща за неговите операции по обработване.

В съображение 90 от ОРЗД се описват редица елементи на ОВЗД, които се припокриват с добре определени елементи от управлението на риска (например ISO 31000[26]). От гледна точка на

25 Следва да се подчертае, че описаният тук процес се повтаря: на практика съществува вероятност всеки от етапите да се повтори многократно преди приключването на ОВЗД.

26 Процедури за управление на риска: комуникация и консултация, установяване на контекста, управление на риска, третиране на риска, наблюдение и преглед (вж. терминологията и определенията, както и съдържанието в предварителния преглед на ISO 31000: https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:en

управлението на риска ОВЗД е насочена към „управление на рисковете“ за правата и свободите на физическите лица, като се използват следните процеси:

- установяване на контекста: *„като се вземат предвид естеството, обхватът, контекстът и целите на обработването и източниците на риска“;*

- оценка на рисковете: *„за да се оценят конкретната вероятност и тежестта на високия риск“;*

- третиране на рисковете: *„ограничаване на този риск“* и *„с които се осигурява защитата на личните данни“* и *„се доказва съответствието с настоящия регламент“.*

Забележка: ОВЗД съгласно ОРЗД представлява инструмент за управление на рисковете за правата на субектите на данни и поради това отразява тяхната гледна точка, какъвто е случаят в определени области (например сигурност на обществото). От друга страна управлението на риска в други области (например информационната сигурност) е насочено към организацията.

ОРЗД осигурява гъвкавост на администраторите да определят конкретната структура и форма на ОВЗД, за да може тя да съответства на съществуващите работни практики. В рамките на ЕС и по света са установени редица различни процеси, при които се отчитат елементите, описани в съображение 90. При все това независимо от формата ОВЗД трябва да представлява действителна оценка на рисковете, която позволява на администраторите да въведат мерки за справяне с тях.

Биха могли да се използват различни методологии (вж. приложение 1 за примери за методологии за оценка на въздействието върху защитата на данни и неприкосновеността на личния живот), които да подпомогнат изпълнението на основните изисквания, определени в ОРЗД. За да се позволи съществуването на тези различни подходи и същевременно да се позволи на администраторите да спазват ОРЗД, са определени общи критерии (вж. приложение 2). Те пояснява основните изисквания на Регламента, но осигуряват достатъчно широк обхват за различни форми на изпълнение. Тези критерии могат да се използват, за да се демонстрира, че дадена методология за ОВЗД отговаря на стандартите, изисквани съгласно ОРЗД. **Администраторът сам избира методология, но тази методология следва да бъде в съответствие с критериите, посочени в приложение 2.**

РГ29 насърчава разработването на специфични за отделните сектори рамки за ОВЗД. Причината за това е, че тези рамки могат да се основават на специфични знания в отделните сектори, което означава, че ОВЗД може да бъде насочена към специфичните особености на конкретен вид операция по обработване (например конкретни видове данни, корпоративни активи, потенциални въздействия, заплахи, мерки). Това означава, че ОВЗД може да бъде насочена към въпроси, които възникват в конкретен икономически сектор или при използването на конкретни технологии или извършването на конкретни видове операции по обработване.

На последно място, при необходимост *„администраторът прави преглед, за да прецени дали обработването е в съответствие с оценката на въздействието върху защитата на данни, най-малкото когато има промяна в риска, с който са свързани операциите по обработване“ (член 35, параграф 11[27]).*

г) Има ли задължение за публикуване на ОВЗД? Не, но публикуването на резюме би могло да повиши доверието, а пълната ОВЗД трябва да бъде съобщена на надзорния орган в случай на предварителна консултация или ако бъде поискана от ОЗД.

ОРЗД не включва правно изискване за публикуването на ОВЗД, администраторът сам решава дали да направи това. При все това администраторите следва да обмислят публикуването най- малкото на части от оценката, например на резюме или на заключението от своята ОВЗД.

27 В член 35, параграф 10 изрично се изключва единствено прилагането на член 35, параграфи 1– 7.

Целта на този процес е да се подпомогне изграждането на доверие в извършваните от администратора операции по обработване и да се демонстрира отчетност и прозрачност. Особено добра практика е да се публикува ОВЗД, когато гражданите са засегнати от операцията по обработване. Такъв би могъл да бъде случаят по-специално когато публичен орган извършва ОВЗД.

Не е нужно публикуваната ОВЗД да съдържа цялата оценка, особено когато в ОВЗД се представя специфична информация, свързана с рисковете за сигурността на администратора, или когато по този начин биха могли да се разкрият търговски тайни или търговска информация с чувствителен характер. В тези обстоятелства публикуваната версия би могла да се състои просто от резюме на основните констатации на ОВЗД или дори само от изявление, че е извършена ОВЗД.

Освен това, когато ОВЗД покаже високи остатъчни рискове, администраторът ще бъде задължен да се консултира предварително с надзорния орган по отношение на обработването (член 36, параграф 1). Като част от тази процедура трябва да се предостави пълната версия на ОВЗД (член 36, параграф 3, буква д). Надзорният орган може да предостави становище[28], без да разкрива тайни или да оповестява слабости по отношение на сигурността, съгласно приложимите в съответната държава членка принципи относно публичния достъп до официални документи.

Д. Кога се осъществява консултация с надзорния орган? Когато остатъчните рискове са високи.

Както е обяснено по-горе:

- ОВЗД се изисква, когато съществува вероятност обработването „*да породи висок риск за правата и свободите на физическите лица*“ (член 35, параграф 1, вж. Ш.Б.а). Например се счита, че съществува вероятност мащабното обработване на здравни данни да породи висок риск и при него се изисква ОВЗД;

- в такъв случай администраторът носи отговорност за оценка на рисковете за правата и свободите на субектите на данни и да определи мерки[29], предвидени за намаляване на тези рискове до приемливо равнище и за демонстриране на спазването на ОРЗД (член 35, параграф 7, вж. Ш.В.в). Пример за това би било при съхранението на лични данни на преносими компютри да се прилагат подходящи технически и организационни мерки за сигурност (пълно криптиране на диска, надеждно управление на ключове, подходящ контрол на достъпа, резервни копия на сигурно място и др.) в допълнение към съществуващите политики (известие, съгласие, право на достъп, право на възражение и др.).

Ако в примера с преносимите компютри по-горе е било счетено, че администраторът е намалил рисковете в достатъчна степен, и след отчитане на член 36, параграф 1 и съображения 84 и 94 обработването може да започне без консултация с надзорния орган. Администраторът трябва да се консултира с надзорния орган именно в случаите, когато администраторът не може да намали идентифицираните рискове в достатъчна степен (т.е. остатъчните рискове продължават да бъдат високи).Примерите за неприемливо висок остатъчен риск включват случаи, в които за субектите на данни могат да настъпят значителни или дори необратими последици, които те не могат да преодолеят (например незаконен достъп до данни, който води до заплаха за живота на субектите на данни, съкращение, финансов риск), и/или когато изглежда очевидно, че рискът ще се материализира (например при невъзможност да се намали броят на лицата, които осъществяват достъп до данните, в резултат на начините на споделяне, използване или разпространение или когато не се отстрани известна слабост).

28 Даването на писмено становище на администратора е необходимо само когато надзорният орган е на мнение, че планираното обработване не е в съответствие с разпоредбите, посочени в член 36, параграф 2.

29 Включително като взема предвид съществуващите насоки от ЕКЗД и надзорните органи и като взема предвид достиженията на техническия прогрес и разходите за прилагане, както е определено в член 35, параграф 1.

Консултация с надзорния орган се изисква всеки път, когато администраторът не може да установи достатъчни мерки за намаляване на рисковете до приемливо равнище (т.е. остатъчните рискове продължават да бъдат високи)[30].

Освен това администраторът ще трябва да се консултира с надзорния орган всеки път, когато правото на държавите членки изисква от администраторите да се консултират с надзорния орган и/или да получават предварително разрешение от него 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 (член 36, параграф 5).

Следва обаче да се посочи, че независимо дали се изисква консултация с надзорния орган въз основа на равнището на остатъчния риск или не, продължават да важат задълженията да се поддържа документация за ОВЗД и своевременно да се актуализира ОВЗД.

IV. Заключения и препоръки

ОВЗД представляват полезен начин за администраторите да прилагат системи за обработване на данни, които са в съответствие с ОВЗД, и могат да бъдат задължителни за някои видове операции по обработване. Те са с променлив мащаб и могат да приемат различна форма, но в ОРЗД се определят основните изисквания за ефективна ОВЗД. Администраторите следва да гледат на извършването на ОВЗД като на полезна и положителна дейност, която подпомага спазването на законовите разпоредби.

В член 24, параграф 1 се определя основната отговорност на администратора от гледна точка на спазването на ОРЗД: *“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.“*

ОВЗД представлява ключова част от спазването на Регламента, когато се планира или се извършва обработване с висок риск. Това означава, че администраторите следва да използват критериите, определени в настоящия документ, за да определят дали трябва да се извърши ОВЗД или не. Съгласно вътрешната политика на администратора този списък би могъл да се разшири отвъд правните изисквания на ОРЗД. Това следва да доведе до повишено доверие и увереност от страна на субектите на данни и другите администратори на данни.

Когато се планира обработване с вероятност от висок риск, администраторът трябва:

- да избере методология за ОВЗД (в приложение 1 са дадени примери), която отговаря на критериите в приложение 2, или да определи и изпълнява систематичен процес за ОВЗД, който:
  - отговаря на критериите в приложение 2;
  - е интегриран в съществуващите процеси във връзка с планирането, разработването, промените, риска и оперативния преглед в съответствие с вътрешните процеси, контекста и културата;
  - включва съответните заинтересовани страни и ясно определя техните отговорности (администратор, ГССИ, субекти на данни или техни представители, бизнес, техническо обслужване, обработващи лични данни, служител по сигурността на информацията и др.);
- да предостави доклада от ОВЗД на компетентния надзорен орган, когато е длъжен;
- да се консултира с надзорния орган, когато не успее да определи достатъчни мерки за ограничаване на високите рискове;
- да извършва периодичен преглед на ОВЗД и на обработването, което се оценява чрез нея, най-малкото когато настъпи промяна на риска, породен от операцията по обработване;
- да документира взетите решения.

30 Забележка: „псевдонимизирането и криптирането на лични данни“ (както и свеждането до минимум на данните, механизмите за надзор и др.) не представляват непременно подходящи мерки. Това са само примери. Подходящите мерки зависят от конкретния контекст и рисковете във връзка с операциите по обработване.

Приложение 1 − Примери за съществуващи рамки за ОВЗД в ЕС

В ОРЗД не се уточнява какъв процес за ОВЗД трябва да се следва, а вместо това на администраторите се позволява да въведат рамка, която допълва съществуващите им работни практики, при условие че в нея се отчитат елементите, описани в член 35, параграф 7. Тази рамка може да бъде съобразена със специфичните нужди на администратора или да е обща за съответния сектор. Публикуваните преди това рамки, разработени от ОЗД в ЕС, и рамките на специфични сектори в ЕС включват (но не са ограничени до):

Примери за общи рамки в ЕС:

- Германия: стандартен модел за защита на данните, V.1.0 − пробна версия, 2016 г. [31]

https://www.datenschutzzentrum.de/uploads/SDM-Methodology_V1_EN1.pdf

- Испания: *Quia para una Evaluation de Impacto en la Protection de Datos Personales (EIPD),* Agencia espanola de protection de datos (AGPD), 2014 г.

https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf

- *Франция:* Оценка на въздействието върху неприкосновеността на личния живот (ОВНЛЖ), Commission nationale de l'informatique et des liberies (CNIL), 2015 г.

https://www.cnil.fr/fr/node/15798

- Обединено кралство: *Кодекс на практиката за провеждане на оценка на въздействието върху неприкосновеността на личния живот,* Служба на комисаря по информацията (ICO), 2014 г.

https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

Примери за специфични за отделните сектори рамки в ЕС:

- Рамка за оценка на въздействието върху защитата на данни и неприкосновеността на личния живот за приложения, използващи радиочестотна идентификация[32].

http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp180_annex_en.pdf

- Модел за оценка на въздействието върху защитата на данните за интелигентни електроенергийни мрежи и интелигентни измервателни системи[33].

http://ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf

Освен това ще бъде изготвен международен стандарт, който също ще осигурява насоки за методологиите, използвани при извършването на ОВЗД (ISO/IEC 29134[34]).

31 Единодушно приет и утвърден (Бавария гласува „въздържал се“) с 92 гласа. Конференция на независимите органи за защита на данните на федерално и провинциално ниво в Кюлунгсборн на 9− 10 ноември 2016 г.

32 Вж. също:

- Препоръка на Комисията от 12 май 2009 г. относно спазването на принципите за неприкосновеност на личния живот и защита на данните в приложения, използващи радиочестотна идентификация.
https://ec.europa.eu/digital-single-market/en/news/commission-recommendation-12-may-2009-implementation-privacy-and-data-protection-principles

- Становище 9/2011 относно преработеното предложение на индустрията за Рамка за оценка на въздействието на приложения с радиочестотна идентификация върху неприкосновеността на личния живот и защитата на данните. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp180_bg.pdf

33 Вж. също така Становище 07/2013 относно модела за оценка на въздействието върху защитата на данните за интелигентни електроенергийни мрежи и интелигентни измервателни системи („модела за ОВЗД“), изготвен от Експертна група 2 на Работната група на Комисията за интелигентни електроенергийни мрежи. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp209 bg.pdf

34 ISO/IEC 29134 (проект), Информационни технологии. Техники за сигурност. Оценка на въздействието върху неприкосновеността на личния живот. Указания, Международна организация по стандартизация (ISO).

Приложение 2 – Критерии за приемлива ОВЗД

РГ29 предлага следните критерии, които администраторите могат да използват, за да оценят дали ОВЗД или методология за извършване на ОВЗД е достатъчно всеобхватна, така че да отговаря на ОРЗД:

□ осигурен е системен опис на обработването (член 35, параграф 7, буква а):

□ вземат се предвид естеството, обхватът, контекстът и целите на обработването (съображение 90);

□ поддържа се регистър на личните данни, получателите и срока, за който ще се съхраняват личните данни;

□ осигурено е функционално описание на операцията по обработване;

□ определени са елементите, свързани с личните данни (хардуер, софтуер, мрежи, лица, хартиен носител или канали за предаване на хартиен носител);

□ взема се предвид спазването на одобрени кодекси за поведение (член 35, параграф 8);

□ оценяват се необходимостта и пропорционалността (член 35, параграф 7, буква б)):

□ определени са мерки за спазване на Регламента (член 35, параграф 7, буква г) и съображение 90), като се вземат предвид:

□ мерки, допринасящи за пропорционалността и необходимостта на обработването въз основа на:

□ конкретна, изрично указана и легитимна цел или цели (член 5, параграф 1, буква б);

□ законосъобразност на обработването (член 6);

□ подходящи, свързани със и ограничени до необходимото данни (член 5, параграф 1, буква в);

□ ограничена продължителност на съхранението (член 5, параграф 1, буква д);

□ мерки, допринасящи за правата на субектите на данни:

□ информиране 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 на ограничаване на обработването (членове 18, 19 и 21);

□ взаимоотношения с обработващите лични данни (член 28);

□ гаранции при международно предаване на данни (глава V);

□ предварителна консултация (член 36).

□ управляват се рисковете за правата и свободите на субектите на данни (член 35, параграф 7, буква в)):

□ оценяват се произходът, естеството, спецификата и степента на рисковете (вж. съображение 84), или по-конкретно за всеки риск, (незаконен достъп, нежелани изменения и изчезване на данни) от гледна точка на субектите на данни:

□ вземат се предвид източниците на риска (съображение 90);

□ определят се потенциалните въздействия върху правата и свободите на субектите на данни в случай на определени събития, включително незаконен достъп, нежелани изменения и изчезване на данни;

□ определят се заплахи, които биха могли да доведат до незаконен достъп, нежелани изменения и изчезване на данни;

□ изчисляват се вероятността и тежестта (съображение 90);

□ определят са мерки за третиране на тези рискове (член 35, параграф 7, буква г) и съображение 90);

□ заинтересованите страни участват:

□ иска се становището на ГССИ (член 35, параграф 2);

□ по целесъобразност се търсят становищата на субектите на данни или техните представители (член 35, параграф 9)

НАСОКИ НА РАБОТНА ГРУПА ПО ЧЛ. 29 ОТ ДИРЕКТИВА 95/46/ЕО ОТНОСНО ПРАВОТО НА ПРЕНОСИМОСТ НА ДАННИТЕ

Обобщение

С член 20 от Общия регламент относно защитата на данните се въвежда ново право на преносимост на данните, което е тясно свързано с правото на достъп, но в много аспекти се различава от него. С това право субектите на данните могат да получават личните данни, които са предоставили на администратор, в структуриран, широко използван и пригоден за машинно четене формат и да прехвърлят тези данни на друг администратор. С това ново право се цели на субекта на данните да бъдат предоставени правомощия и по-висока степен на контрол над личните данни, които се отнасят до него.

Тъй като с правото на преносимост на данните се разрешава прякото предаване на лични данни от един администратор на данни на друг, то е също така важен инструмент, с който ще се подкрепя свободното движение на лични данни в ЕС и ще се насърчава конкуренцията между администраторите. Това право ще улесни преминаването от един доставчик на услуги към друг и следователно ще способства за развитието на нови услуги в контекста на стратегията за цифров единен пазар.

С настоящото становище се предоставят насоки относно начина на тълкуване и прилагане на правото на преносимост на данните, въведено с ОРЗД. То е насочено към обсъждане на правото на преносимост на данните и на неговия обхват. С него се изясняват условията, при които се прилага новото право, като се вземат предвид правното основание за обработване на данните (съгласието на субекта на данните или необходимостта от изпълнение на договор), както и фактът, че това право е ограничено до личните данни, предоставени от субекта на данните. В становището са дадени също така конкретни примери и критерии за пояснява не на обстоятелствата, при които правото е приложимо. В това отношение Работната група по член 29 счита, че правото на преносимост на данните обхваща данните, които са предоставени съзнателно и активно от субекта на данните, както и личните данни, генерирани от неговата дейност. Това ново право не може да бъде изпразвано от съдържание и да бъде ограничавано до личната информация, предоставена пряко от субекта на данните, например в онлайн формуляр.

Като добра практика администраторите на данни следва да започнат да разработват средствата, които ще допринесат за удовлетворяването на исканията за преносимост на данните, като инструменти за сваляне и приложно-програмни интерфейси. Те следва да гарантират, че личните данни се предават в структуриран, широко използван и пригоден за машинно четене формат, и следва да бъдат насърчавани да гарантират оперативната съвместимост на формата на данните, които се предоставят в изпълнение на искането за преносимост на данните.

Със становището се помага също така за ясното разбиране на съответните задължения на администраторите на данни и се препоръчват най-добри практики и инструменти, които подпомагат спазването на правото на преносимост на данните. Накрая, в становището се препоръчва заинтересованите страни от отрасъла и професионалните организации да разработят съвместно общ набор от оперативно съвместими стандарти и формати с цел изпълняване на изискванията, свързани с правото на преносимост на данните.

I. Въведение

С член 20 от Общия регламент относно защитата на данните (ОРЗД) се въвежда ново право на преносимост на данните. С това право субектите на данни могат да получават личните данни, които са предоставили на администратор на данни, в структуриран, широко използван и пригоден за машинно четене формат и да прехвърлят тези данни на друг администратор на данни без възпрепятстване. Това право, което е приложимо, при условие че са изпълнени определени условия, подкрепя избора на потребителя, контрола от негова страна и оправомощаването му.

Физическите лица, които желаеха да се възползват от своето право на достъп съгласно Директивата за защита на данните (Директива 95/46/ЕО), бяха ограничени от формата, избран от администратора на данни за предоставяне на поисканата информация. **С новото право на преносимост на данните се цели да бъдат предоставени правомощия на субектите на данни по отношение на техните собствени лични данни, тъй като то улеснява възможността им да преместват, копират или предават лични данни без затруднения от една ИТ среда към друга** (независимо дали към техните собствени системи, системите на доверени трети страни или на нови администратори на данни).

Като утвърждава личните права на физическите лица и техния контрол над личните данни, които ги засягат, преносимостта на данните представлява също така възможност за „възстановяване на равнопоставеността“ в отношението между субектите на данни и администраторите на данни[1].

Макар че правото на преносимост на личните данни може да подобри така също конкуренцията между услугите (като се улеснява смяната на доставчика), с ОРЗД се уреждат личните данни, а не аспектите на конкуренцията. По-специално с член 20 преносимите данни не са ограничени до такива, които са необходими или полезни за смяната на доставчика[2].

Въпреки че преносимостта на данните е ново право, вече съществуват и други типове преносимост или се обсъждат в други области на законодателството (например в контекста на прекратяването на договори, роуминга при съобщителните услуги и трансграничния достъп до услуги[3]). Възможно е да бъдат реализирани някои полезни взаимодействия между различните типове преносимост и дори ползи за физическите лица, ако се предоставят комбинирано, макар че към случаи, основани на аналогия, следва да се подхожда внимателно.

В настоящото становище са дадени насоки за администраторите на данни, за да могат да актуализират техните практики, процеси и политики, и се изяснява значението на понятието „преносимост на данните“, за да се даде възможност на субектите на данни ефективно да използват новото си право.

II. Кои са основните елементи на преносимостта на данните?

В член 20, параграф 1 от ОРЗД правото на преносимост на данните е определено, както следва:

Субектът на данните има право да получи личните данни, които го засягат и които той е предоставил на администратор, в структуриран, широко използван и пригоден за машинно четене формат и има правото да прехвърли тези данни на друг администратор без възпрепятстване от администратора, на когото личните данни са предоставени [...].

- Право на получаване на лични данни

Първо, преносимост на данните представлява **правото на субекта на данните да получи поднабор от личните данни**, които го засягат и които са обработени от администратора на данни, и да съхранява тези данни за по-нататъшна лична употреба. Това съхранение може да се осъществи на частно устройство или в частна облачна среда, без да е задължително данните да се предават на друг администратор на данни.

В това отношение правото на преносимост на данните допълва правото на достъп. Една от специфичните особености на преносимостта на данните се дължи на факта, че тя предлага лесен начин, по който субектите на данните самостоятелно да управляват и повторно да използват личните данни. Тези данни следва да бъдат получени *„в структуриран, широко използван и пригоден за машинно четене формат“*. Например субектът на данните може да се интересува от извличане на своята текуща плейлиста (или хронология на слушаните песни) от услуга за стрийминг на музика, за да разбере

1 С преносимостта на данните се цели основно да се засили контролът на физическите лица върху техните лични данни и да се гарантира, че те играят активна роля в екосистемата на данните.

2 Например това право може да позволи на банките да предоставят допълнителни услуги под контрола на потребителя, като използват лични данни, които първоначално са събрани като част от услугата за доставка на електроенергия.

3 Вж. Дневен ред на Европейската комисия за цифров единен пазар: https://ec.europa.eu/digital-agenda/en/digital-single-market, по-специално първият стълб на политиката „По-добър онлайн достъп до цифрови стоки и услуги“.

колко пъти е слушал определени песни или за да провери каква музика желае да закупи или да слуша на друга платформа. По същия начин той може да пожелае да извлече и списъка със своите контакти от приложението към уеб-базираната си поща, за да състави например сватбен списък, да получи информация за покупките с различни карти за лоялност или да определи своя въглероден отпечатък[4].

- Право на предаване на лични данни от един администратор на данни към друг администратор на данни

Второ, с член 20, параграф 1 на субектите на данните се предоставя **правото да предават лични данни от един администратор на данни към друг администратор на данни** „без възпрепятстване“. Данните може да се предават направо от един администратор на данни към друг по искане на субекта на данните и когато това е технически осъществимо (член 20, параграф 2). В тази връзка в съображение 68 администраторите на данни се насърчават да разработват оперативно съвместими формати, които дават възможност за преносимост на данните[5], но без да се поражда задължение за администраторите да приемат или поддържат технически съвместими системи за обработване[6]. Съгласно ОРЗД обаче се забранява на администраторите да създават пречки пред предаването.

По същество този елемент на преносимостта на данните дава възможност на субектите на данни не само да получат и да използват повторно данните, които са предоставили, но също така да ги предават на друг доставчик на услуги (независимо дали в същия или в различен сектор на стопанска дейност). С правото на преносимост на данните, освен че на потребителя се предоставят правомощия чрез предотвратяване на поставянето му в зависимост („lock-in“), се очаква да се насърчават възможностите за иновации и да се споделят лични данни между администраторите на данни по безопасен и сигурен начин и под контрола на субекта на данните[7]. С преносимостта на данните може чрез потребителите да се поощрява контролираното и ограничено споделяне на лични данни между организации, а оттам и да се обогатява опита с услугите и потребителите[8]. Преносимостта на данните, които засягат потребителите, може да улесни предаването и повторното използване на лични данни между различните услуги, от които те се интересуват.

- Администриране

Преносимостта на данните гарантира правото да се получават и да се обработват лични данни според желанията на субекта на данните[9].

Администраторите на данни, когато отговарят на искания за преносимост, съгласно определените в член 20 условия, не носят отговорност за обработване, осъществено от субекта на данните или от друго дружество, получило личните данни. Те действат от името на субекта на данните, включително когато личните данни се предават направо на друг администратор на данни. В това отношение администраторът на данни не носи отговорност за съответствието на получаващия администратор на данни с правото в областта на защитата на данните, като се има предвид, че получателят не се избира от изпращащия администратор на данни. В същото време администраторът следва да предвиди гаранции с цел потвърждаване, че действително ще действа от името на субекта на данните. Например може да се въведат процедури, за да се гарантира, че предаваните лични данни наистина са от вида, който субектът на данните желае да предаде. Това може да се постигне, като се получи потвърждение от субекта на данните или преди предаването, или по-рано, когато е дадено първоначалното съгласие за обработване или е финализиран договорът.

4 В тези случаи обработването на данните от страна на субекта на данни може или да попадне в обхвата на дейностите в рамките на домакинството, когато цялото обработване се извършва единствено под контрола на субекта на данните, или може да бъде осъществено от дадена друга страна от името на субекта на данните. В последния случай другата страна следва да се счита за администратор на данни, дори да е единствено с цел съхраняване на личните данни, като трябва да се спазват принципите и задълженията, определени в ОРЗД.

5 Вж. също раздел V.

6 В резултат на това следва да се обърне специално внимание на формата на предаваните данни, за да се гарантира, че с малко усилия данните може да се използват повторно от субекта на данните или от друг администратор на данни. Вж. също раздел V.

7 Вж. няколко експериментални приложения в Европа, например MiData в Обединеното кралство, MesInfos / SelfData от FING във Франция.

8 Областите, наречени „самоизмерване на жизнени показатели“ и „интернет на нещата“, са показали ползата (и рисковете) от свързването на личните данни от различни аспекти на живота на дадено физическо лице като фитнес, активност и прием на калории, за да се даде по-пълно описание за живота на физическото лице в рамките на един файл.

9 Правото на преносимост на данните не е ограничено до лични данни, които са полезни и са от значение за аналогични услуги, предоставяни от конкурентите на администратора на данни.

Когато администраторите на данни отговарят на искане за преносимост на данните, те нямат специално задължение преди да предадат данните да проверяват и удостоверяват качеството им. Разбира се тези данни вече следва да са точни и актуални в съответствие с принципите, посочени в член 5, параграф 1 от ОРЗД. Освен това с преносимостта на данните не се налага задължение на администратора на данни да запазва лични данни за по-дълъг период от необходимото или след даден определен период на запазване[10]. Важно е да се отбележи, че няма допълнително изискване за запазване на данни след иначе приложимите периоди на запазване, само за да се отговори на евентуално бъдещо искане за преносимост на данните.

Когато поисканите лични данни се обработват от даден обработващ лични данни, сключеният в съответствие с член 28 от ОРЗД договор трябва да включва задължението да се подпомага „администратора, (...), чрез подходящи технически и организационни мерки (...) да отговори на искания за упражняване на предвидените (...) права на субектите на данни“. Следователно администраторът на данни следва да въведе специални процедури в сътрудничество с обработващите лични данни, с които работи, за да отговори на исканията за преносимост на данните. В случай на съвместно администриране, следва ясно да бъдат разпределени в договор отговорностите между всеки администратор на данни, що се отнася до обработването на искания за преносимост на данните.

Освен това получаващият администратор на данни[11] отговаря за осигуряването на гаранция, че предоставените преносими данни са релевантни и не са прекомерни във връзка с новото обработване на данните. Например ако към услуга за уеб-базирана поща е отправено искане за преносимост на данните, когато искането се използва от субекта на данните за получаването на електронни съобщения и за изпращането им към сигурна платформа за архивиране, не е необходимо новият администратор на данни да обработва данните за контакт на кореспондентите на субекта на данните. Ако тази информация не е от значение предвид целта на новото обработване, тя не следва да се пази и обработва. Във всички случаи получаващите администратори на данни не са задължени да приемат и обработват лични данни, които са предадени вследствие на искане за преносимост на данните. Аналогично, когато субект на данните поиска предаване на данни за неговите банкови операции към услуга, която подпомага управлението на бюджета му, получаващият администратор на данни не е нужно да приема всички данни или да запазва подробна информация за операциите, след като те са отбелязани за целите на новата услуга. С други думи, следва да се приемат и запазват само онези данни, които са необходими и релевантни за услугата, предоставяна от получаващия администратор на данни.

„Получаващата“ организация става новият администратор на данни по отношение на тези лични данни и трябва да спазва принципите, посочени в член 5 от ОРЗД. Следователно „новият“ получаващ администратор на данни трябва ясно и непосредствено да посочи целта на новото обработване при всяко искане за предаване на преносими данни в съответствие с изискванията за прозрачност, посочени в член 14[12]. Що се отнася до всяко друго обработване на данни, което се извършва на негова отговорност, администраторът на данни следва да прилага определените в член 5 принципи като законосъобразност, добросъвестност и прозрачност, ограничение на целите, свеждане на данните до минимум, точност, цялостност и поверителност, ограничение на съхранението и отчетност[13].

Администраторите на данни, които съхраняват лични данни, следва да са подготвени да способстват за упражняването на правото на преносимост на данните, предоставено на техните субекти на данните. Администраторите на данни могат да изберат така също да приемат данни от даден субект на данни, но не са задължени да го направят.

10 В горния пример, ако администраторът на данни не запазва записи на пусканите песни от потребителя, тогава тези лични данни не могат да бъдат включвани в искането за преносимост на данните.

11 т.е. който получава личните данни, след като субектът на данните е отправил искане за преносимост на данните към друг администратор на данни.

12 Освен това новият администратор на данни не следва да обработва лични данни, които не са релевантни, а обработването трябва да бъде ограничено до необходимото за новите цели дори ако личните данни са част от по-голям набор от данни, който е предаден чрез процеса на преносимост. Личните данни, които не са необходими за постигането на целта на новото обработване, следва да бъдат изтрити възможно най-скоро.

13 След като администраторът на данни получи личните данни, изпратени при упражняването на правото на преносимост на данните, те може да се считат за „предоставени от“ субекта на данните и да бъдат препредадени в съответствие с правото на преносимост на данните, доколкото са изпълнени останалите условия, които са приложими по отношение на това право (т.е. правното основание на обработването, ...).

- Преносимост на данните спрямо другите права на субектите на данните

Когато физическото лице упражнява своето право на преносимост на данните, това се извършва без да се засяга никое друго право (какъвто е случаят с всички други права според ОРЗД). Субектът на данните може да продължи да използва и да се ползва от услугата на администратора на данни дори след операцията по преносимост на данните. Преносимостта на данните не води автоматично до изтриването на данните[14] от системите на администратора на данни и не засяга първоначалния период на запазване, който се отнася за предадените данни. Субектът на данните може да упражнява своите права, докато администраторът на данни продължава да обработва данните.

Също така, ако субектът на данните желае да упражни своето право на изтриване (правото „да бъдеш забравен“ съгласно член 17), администраторът на данни не може да използва преносимостта на данните като причина да отложи или откаже въпросното изтриване.

Ако субект на данните установи, че личните данни, поискани според правото на преносимост на данните, не отговарят напълно на неговото искане, всяко следващо искане на лични данни според правото на достъп следва да бъде изпълнено в пълна степен при спазване на член 15 от ОРЗД.

Освен това, ако специално европейско право или право на държава членка в друга област също предвижда някаква форма на преносимост на въпросните данни, определените условия по тези специални закони също трябва да бъдат взети предвид, когато се удовлетворява искането за преносимост на данните съгласно ОРЗД. Първо, ако от направеното от субекта на данните искане е видно, че намерението му не е да упражнява права съгласно ОРЗД, а по-скоро да упражнява права само съгласно отрасловото законодателство, тогава разпоредбите за преносимост на данните според ОРЗД няма да се прилагат по отношение на това искане[15]. От друга страна, ако искането касае преносимостта съгласно ОРЗД, наличието на такова специално законодателство не отменя общоприложимостта на принципа на преносимост на данните по отношение на всеки администратор на данни, както е предвидено в ОРЗД. Вместо това на база конкретен случай трябва да се преценява как въпросното специално законодателство може да засегне правото на преносимост на данните, ако изобщо това е възможно.

III. Кога се прилага преносимост на данните?

- Кои операции по обработване са обхванати от правото на преносимост на данните?

С оглед на спазването на ОРЗД от администраторите на данни се изисква да разполагат с ясно правно основание за обработването на лични данни.

В съответствие с член 20, параграф 1, буква а) от ОРЗД, **за да попаднат в обхвата на преносимостта на данните**, операциите по обработване трябва да са основани:

- или на съгласието на субекта на данните (съгласно член 6, параграф 1, буква а), или съгласно член 9, параграф 2, буква а), когато става дума за специални категории лични данни);
- или на договор, по който субектът на данните е страна съгласно член 6, параграф 1, буква б).

Например заглавията на книгите, закупени от дадено физическо лице от онлайн книжарница, или песните, които са слушани чрез услуга за музикален стрийминг, представляват примери за лични данни, които обикновено попадат в обхвата на преносимостта на данните, защото се обработват въз основа на изпълнението на договор, по който субектът на данните е страна.

С ОРЗД не се установява общо право на преносимост на данните за случаите, когато обработването на лични данни не е основано на съгласие или на договор[16]. Например финансовите

14 както е посочено в член 17 от ОРЗД.

15 Например ако искането на субекта на данните се отнася изрично до предоставянето на достъп до информация за неговата банкова сметка към доставчик на услуги, свързани с информация за сметки, за целите на Втората директива за платежните услуги (ДПУ2), този достъп следва да бъде предоставен в съответствие с разпоредбите на тази директива.

16 Вж. съображение 68 и член 20, параграф 3 от ОРЗД. В член 20, параграф 3 и съображение 68 се посочва, че преносимостта на данните не се прилага, когато обработването на данните е необходимо за изпълнението на задача от обществен интерес или при упражняването на официални правомощия, които са предоставени на администратора на данни, както и когато администраторът на данни изпълнява обществените си задължения или спазва дадено правно задължение. По тази причина администраторите на данни не са задължени да осигуряват преносимост в тези случаи. Добра практика е обаче да се разработват процеси за автоматично отговаряне на искания за преносимост чрез спазване на принципите, уреждащи правото на преносимост на данните. Пример за това би била дадена държавна служба, осигуряваща лесно сваляне на подадените документи за

институции не са задължени да отговарят на искане за преносимост на данните, което се отнася до лични данни, обработвани в рамките на техните задължения да предотвратяват и откриват изпиране на пари и други финансови престъпления; преносимостта на данните не обхваща също така данните за контакт в професионалната сфера, обработвани в отношението между дружества, когато обработването не се основава нито на съгласието на субекта на данните, нито на договор, по който той е страна.

Когато се касае за данни на служители, правото на преносимост на данните се прилага само ако обработването е основано на договор, по който субектът на данните е страна. В много случаи съгласието няма да се счита за свободно дадено в този контекст поради неравнопоставеността между работодателя и служителя по отношение на правомощията[17]. Вместо това някои случаи на обработване, касаещи човешките ресурси, се базират на правното основание за законен интерес или са необходими за спазването на конкретни правни задължения в областта на трудовата заетост. На практика правото на преносимост на данните в контекста на човешките ресурси несъмнено ще е свързано с определени операции по обработване (като услуги по заплащане и обезщетяване, вътрешно наемане на персонал), но в много други ситуации ще е необходим подход, основан на конкретен случай, за да се удостовери дали са изпълнени всички условия, които са приложими за правото на преносимост на данните.

Накрая, правото на преносимост на данните се прилага само ако обработването на данните „става по автоматичен начин“ и следователно не обхваща повечето досиета на хартиен носител.

- Какви лични данни трябва да се включват?

В съответствие с член 20, параграф 1, за да попадат в обхвата на правото на преносимост, данните трябва да бъдат:

- лични данни, които засягат субекта на данните; както и

- които субектът на данните е предоставил на администратор на данни.

В член 20, параграф 4 се казва също така, че спазването на това право не следва да влияе неблагоприятно върху правата и свободите на други лица.

Първо условие: лични данни, които засягат субекта на данните

В обхвата на искане за преносимост на данните се включват само лични данни. Следователно всички данни, които са анонимни[18], или не се отнасят до субекта на данните, не биха попаднали в обхвата. В обхвата обаче се включват данни за псевдонимите, които ясно могат да бъдат свързани с даден субект на данни (например тъй като той е предоставил съответния идентификатор, вж. член 11, параграф 2).

В много случаи администраторите на данни обработват информация, която съдържа личните данни на различни субекти на данни. Когато случаят е такъв, администраторите на данни не следва да тълкуват изречението „лични данни, свързани със субекта на данните“ прекалено ограничително. Например записите в телефон, при обмен на съобщения между абонати или гласова връзка чрез интернет (VoIP) може да включват (в хронологията в акаунта на абоната) данни на трети страни, които участват във входящи или изходящи повиквания. Макар че в такъв случай записите ще съдържат лични данни, които засягат множество лица, абонатите следва да имат възможност тези записи да им се предоставят в отговор на искания за преносимост на данните, тъй като записите (също) засягат субекта на данните. Когато обаче тези записи след това се предават на нов администратор на данни, този нов администратор на данни не следва да ги обработва за никакви цели, които влияят неблагоприятно върху правата и свободите на трети страни (вж. по-долу: трето условие).

личните данъци върху доходите за минали периоди. Като добра практика за преносимост на данните в случай на обработване, основано на правно основание по необходимост, за законен интерес и за съществуващи доброволни схеми вж. стр. 47 и 48 от Становище 6/2014 относно законните интереси на Работната група по член 29 (WP217).

17 Както беше посочено от Работната група по член 29 в нейното Становище 8/2001 от 13 септември 2001 г. (WP48).

18 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216 en.pdf

Второ условие: данните са предоставени от субекта на данните

Второто условие стеснява обхвата до данните, „предоставени от“ субекта на данните.

Има много примери за лични данни, които са „предоставени от“ субекта на данните съзнателно и активно, като данни за акаунт (например адрес за кореспонденция, потребителско име, възраст), които са предоставени чрез онлайн формуляр. Все пак данни, „предоставени от“ субекта на данните, също се генерират в резултат от наблюдението на неговата дейност. Съответно Работната група по член 29 счита, че, за да се осигурят всички ползи от това право, в „предоставени от“ трябва да се включват също така личните данни, които са генерирани при наблюдението на дейностите на потребителите, като първични данни, обработени от интелигентно измервателно устройство или други видове свързани предмети[19], дневници на дейността, хронология на използването на уебсайтове или търсения.

Тази последна категория данни не включва данните, създадени от администратора на данни (с използване на наблюдаваните данни или на пряко предоставените входни данни), като потребителски профил, създаден чрез анализ на първичните данни, събрани от интелигентно измервателно устройство.

Разграничават се различни категории данни в зависимост от техния произход, за да се определи дали са обхванати от правото на преносимост на данните. Следните категории данни може да бъдат определени като „предоставени от субекта на данните“:

- **данни, които активно и съзнателно са предоставени от субекта на данните** (например адрес за кореспонденция, потребителско име, възраст и т.н.);

- **наблюдавани данни, предоставени от субекта на данните посредством използването на дадена услуга или дадено устройство.** Те може да включват например хронология на търсенията на лицето, данни за трафика и данни за местоположението. Може да включват също така други първични данни като например пулса, отчетен от носимо устройство.

Обратно, логически изведените данни и производните данни са създадени от администратора на данни въз основа на данните, „предоставени от субекта на данните“. Например резултатът от оценка на здравето на потребител или профилът, създаден в контекста на управлението на риска и финансовите разпоредби (например за определяне на кредитоспособността или за спазване на правилата за борба с изпирането на пари), не може сами по себе си да се считат за „предоставени от“ субекта на данните. Въпреки че тези данни може да са включени в профил, който се съхранява от администратор на данните, и да са логически изведени или производни от анализа на данните, предоставени от субекта на данните (например чрез действията му), тези данни обикновено не се считат за „предоставени от субекта на данните“ и съответно не попадат в обхвата на това ново право[20].

Обикновено, като се имат предвид целите на политиката във връзка с правото на преносимост на данните, терминът „предоставени от субекта на данните“ трябва да се тълкува разширително, като не се допускат „логически изведените данни“ и „производните данни“, които включват лични данни, създадени от доставчик на услуги (например алгоритмични резултати). Администраторът на данни може да изключи тези логически изведени данни, но следва да включи всички други лични данни, предоставени от субекта на данните чрез технически средства, които са осигурени от администратора[21].

Следователно терминът „предоставени от“ включва лични данни, които се отнасят до дейността на субекта на данните или са резултат от наблюдаването на поведението на даденото физическо

19 Благодарение на възможността да се извличат данни от наблюдението на неговата дейност, субектът на данните ще може също така да получи по-добра представа за изборите, свързани с прилагането и направени от администратора на данни във връзка с обхвата на наблюдаваните данни, и ще бъде в състояние по-добре да избере какви данни желае да предостави, за да получи аналогична услуга, както и да е наясно в каква степен се зачита правото му на неприкосновеност на личния живот.

20 Въпреки това субектът на данните все пак може да се възползва от своето „право да получи от администратора потвърждение дали се обработват лични данни, свързани с него, и ако това е така, да получи достъп до данните“, както и информация относно „съществуването на автоматизирано вземане на решения, включително профилирането, посочено в член 22, параграфи 1 и 4, и поне в тези случаи съществена информация относно използваната логика, както и значението и предвидените последствия от това обработване за субекта на данните“ в съответствие с член 15 от ОРЗД (който се отнася до правото на достъп).

21 Тук се включват всички наблюдавани данни за субекта на данните по време на дейностите, за целите на които се събират данните, като хронология на операциите или дневник на достъпа. Данните, които се събират чрез проследяване и записване на субекта на данните (като приложение, което записва пулса, или технология, използвана за проследяване на разглежданията), също следва да се считат за „предоставени от“ него, дори когато данните не са предадени активно или съзнателно.

лице, но не включва данните, генерирани от последващия анализ на това поведение. Обратно, всички лични данни, които са създадени от администратора на данни в рамките на обработването на данните, например чрез процес на персонализация или препоръчване, чрез категоризиране или профилиране на потребители, представляват производни или логически изведени данни от личните данни, предоставени от субекта на данните, и не са обхванати от правото на преносимост на данните.

Трето условие: правото на преносимост на данните не следва да влияе неблагоприятно върху правата и свободите на други лица

По отношение на личните данни, засягащи други субекти на данни:

С третото условие се цели да се избегне извличането и предаването на данни, съдържащи лични данни на други субекти на данни (които не са дали съгласие), към нов администратор на данни в случаи, когато има вероятност тези данни да бъдат обработвани по начин, който би повлиял неблагоприятно върху правата и свободите на други субекти на данни (член 20, параграф 4 от ОРЗД)[22].

Например подобно неблагоприятно влияние би настъпило, ако предаването на данни от един администратор на данни към друг, би попречило на трети страни да упражняват техните права като субекти на данни съгласно ОРЗД (като правата на информация, достъп и т.н.).

Субектът на данни, който инициира предаването на данните си към друг администратор на данни, или дава съгласие новият администратор да ги обработва, или сключва договор с този администратор. Когато лични данни на трети страни са включени в набора от данни, трябва да се определи друго правно основание за обработването. Например администраторът на данни може да преследва законен интерес съгласно член 6, параграф 1, буква е), по-специално когато целта на администратора на данни е да предостави услуга на субекта на данните, която позволява на последния да обработва лични данни за чисто лични или домакински дейности. Субектът на данните продължава да носи отговорност за операциите по обработването, инициирани от него в контекста на лична дейност, която засяга или евентуално влияе върху трети страни, доколкото решението за такова обработване по никакъв начин не е взето от администратора на данни.

Например услуга за уеб-базирана поща може да позволи създаването на директория с контактите, приятелите, родините, семейството и по-широкото обкръжение на субекта на данните. Тъй като тези данни са свързани с (и са създадени от) физическо лице, което може да бъде идентифицирано и което желае да упражни неговото право на преносимост на данните, администраторите на данни следва да предадат цялата директория с входящи и изходящи електронни съобщения на въпросния субект на данните.

Аналогично банковата сметна на субекта на данни може да съдържа лични данни относно операциите не само на титуляря на сметката, но също така на други физически лица (например ако са превели пари на титуляря на сметката). Съществува малка вероятност правата и свободите на тези трети страни да бъдат повлияни неблагоприятно от предаването на информация за банковата сметка на титуляря на сметката в изпълнение на отправено искане за преносимост, при условие че и в двата примера данните се използват за една и съща цел (например адрес за контакт, който се използва само от субекта на данните или хронология на операциите с банковата сметка на субекта на данните).

Обратно, правата и свободите на трети страни няма да бъдат зачетени, ако новият администратор на данни използва личните данни за други цели, например ако получаващият администратор на данни използва личните данни на други физически лица, съдържащи се в директорията с контактите на субекта на данните, за целите на маркетинга.

Следователно, за да се избегнат неблагоприятни последици за свързаната трета страна, обработването на такива лични данни от друг администратор е разрешено само доколкото данните се съхраняват под пълния контрол на потребителя, отправил искането, и се управляват единствено за лични или домакински нужди. Получаващият „нов“ администратор на данни (на когото данните

22 В съображение 68 се казва, че „когато в определен пакет от лични данни е засегнат повече от един субект на данни, правото личните данни да бъдат получавани следва да не засяга правата и свободите на други субекти на данни в съответствие с настоящия регламент“.

може да бъдат предадени по искане на потребителя) не може да използва предадените данни на трета страна за свои собствени цели, например за да предлага продукти и услуги на въпросните субекти на данни — трети страни. Например тази информация не следва да се използва за обогатяване на профила на субекта на данни трета страна, и за пресъздаването на неговата социална среда без неговото знание и съгласие[23]. Не може да се използва така също за извличането на информация за такива трети страни и за създаването на специфични профили дори когато техните лични данни вече се съхраняват от администратора на данни. В противен случай това обработване може да се окаже незаконосъобразно и недобросъвестно, и по-специално ако съответните трети страни не са уведомени и не могат да упражнят своите права като субекти на данни.

Освен това една от водещите практики за всички администратори на данни (както „изпращащите“, така и „получаващите“ страни) се състои във внедряването на инструменти, чрез които субектите на данните могат да избират съответните данни, които желаят да получат и предадат, и да изключват, когато е целесъобразно, данните на други физически лица. Това допълнително ще спомогне да се намалят рисковете за третите страни, чиито лични данни може да бъдат пренесени.

Освен това администраторите на данни следва да внедрят механизми за предоставяне на съгласие от другите свързани субекти на данни, за да се улесни предаването на данните в случаите, когато такива страни желаят да дадат съгласие, например ако те също желаят да прехвърлят техните данни към някой друг администратор на данни. Такава ситуация може да възникне например при социалните мрежи, но администраторите на данни следва да решат коя водеща практика да използват.

Относно данните, които са обект на интелектуална собственост и търговска тайна:

Правата и свободите на други лица се споменават в член 20, параграф 4. Въпреки че не са пряко свързани с преносимостта, това може да се разбира като включително „търговската тайна или интелектуалната собственост, и по-специално върху авторското право за защита на софтуера“. Макар че тези права трябва да бъдат взети предвид преди да се отговори на дадено искане за преносимост на данните, все пак „тези съображения [обаче] не следва да представляват отказ за предоставяне на цялата информация на съответния субект на данни“. Освен това администраторът на данни не следва да отхвърля искане за преносимост на данните въз основа на нарушаване на друго договорно право (например неуреден дълг или търговски конфликт със субекта на данните).

Правото на преносимост на данните не представлява право физическото лице да злоупотребява с информацията по начин, който би могло да се определи като нелоялна практика или който би бил нарушение на права на интелектуална собственост.

Потенциалният стопански риск обаче сам по себе си не може да служи като основание за отказ да се отговори на искане за преносимост и администраторите на данни могат да предават личните данни, предоставени от субекти на данни, по такъв начин, че да не се издава информация, която е обект на търговска тайна или права на интелектуална собственост.

IV. Как общите правила, уреждащи упражняването на правата на субектите на данни, се прилагат по отношение на преносимостта на данните?

- Каква предварителна информация трябва да бъде предоставена на субекта на данните?

В изпълнение на новото право на преносимост на данните, администраторите на данни трябва да уведомяват субектите на данни за наличието на новото право на преносимост. Когато съответните лични данни се събират направо от субекта на данните, това трябва да стане „в момента на получаване на личните данни“. Ако личните данни не са били получени от субекта на данните, администраторът на данни трябва да предостави информацията, предвидена по член 13, параграф 2, буква б) и член 14, параграф 2, буква в).

23 Услуга за социални мрежи не следва да обогатява профила на своите членове, като използва лични данни, предадени от даден субект на данни при упражняване на неговото право на преносимост на данните, без да се зачита принципът на прозрачност и също така като се гарантира, че те са базирани на подходящо правно основание, що се отнася до това конкретно обработване.

„Когато личните данни не са получени от субекта на данните“, според член 14, параграф 3 се изисква информацията да бъде предоставена в рамките на разумен срок, който да не превишава един месец след получаването на данните, при осъществяване на първия контакт със субекта на данните или когато данните се разкриват пред трети страни[24].

Когато предоставят изискваната информация, администраторите на данни трябва да гарантират, че те правят разликата между правото на преносимост на данните и останалите права. По тази причина Работната група по член 29 препоръчва по- специално администраторите на данни ясно да обясняват разликата между видовете данни, които субектът на данните може да получава въз основа на правата на субекта на достъп до данни и преносимост на данните.

Освен това Работната група препоръчва администраторите на данни винаги да включват информация относно правото на преносимост на данните, преди субектите на данни да закрият даден акаунт, който може да имат. Това позволява на потребителите да проверят техните лични данни и лесно да изпратят данните към свое собствено устройство или към друг доставчик, преди съответният договор да бъде прекратен.

В заключение трябва да се отбележи, че Работната група по член 29 препоръчва на „получаващите“ администратори на данни като водеща практика да се предоставя на субектите на данни пълна информация за естеството на личните данни, които са релевантни за изпълнението на техните услуги. Освен че по този начин се подкрепя добросъвестното обработване, по този начин се позволява на потребителите да ограничат рисковете за третите страни и също така всяко друго ненужно дублиране на личните данни дори когато не са обвързани други субекти на данни.

- Как администраторът на данни може да идентифицира субекта на данните, преди да отговори на неговото искане?

В ОРЗД не са предписани изисквания за това как да се установява автентичността на субекта на данните. В член 12, параграф 2 от ОРЗД все пак се казва, че администраторът на данни, не следва да отказва да предприеме действия по искане на субекта на данните за упражняване на правата му (в това число правото на преносимост на данните), освен ако обработва лични данни за цели, за които не се изисква идентифициране на субекта на данните и може да докаже, че не е в състояние да идентифицира субекта на данните. Съгласно член 11, параграф 2 обаче при такива обстоятелства субектът на данните може да предостави допълнителна информация, позволяваща неговото идентифициране. Освен това в член 12, параграф 6 се казва, че когато администраторът на данни има основателни опасения във връзка със самоличността на субекта на данните, той може да поиска допълнителна информация за потвърждаване на самоличността на субекта на данните. Когато субект на данните предоставя допълнителна информация, позволяваща неговото идентифициране, администраторът на данни не следва да отказва предприемане на действия по искането. Когато информацията и данните, събирани онлайн, са свързани с псевдоними или еднозначни идентификатори, администраторите на данни могат да прилагат подходящи процедури, позволяващи физическото лице да отправи искане за преносимост на данните и да получи данните, които се отнасят до него. Във всеки случай администраторите на данни трябва да приложат процедура за установяване на автентичността, за да могат категорично да се убедят в идентичността на субекта на данните, който иска своите лични данни или в по-общ план упражнява правата си, предоставени от ОРЗД.

Такива процедури вече съществуват в много случаи. Автентичността на субектите на данните често е установена от администратора на данни, преди още да се сключи договор или да се получи съгласието му относно обработването. В резултат на това личните данни, използвани за регистриране на физическото лице, което е засегнато от обработването, може да се използват също така като доказателство при установяване на автентичността на субекта на данните за целите на преносимостта[25].

24 Според член 12 се изисква администраторите на данни да предоставят „всякаква комуникация [...] в кратка, прозрачна, разбираема и лесно достъпна форма, на ясен и прост език, особено що се отнася до всяка информация, конкретно насочена към деца“.

25 Когато например обработването на данните е свързано с потребителски акаунт, предоставянето на съответното потребителско име и парола може да е достатъчно, за да бъде идентифициран субектът на данните.

Макар че в тези случаи предварителното идентифициране на субектите на данни може да налага изискването на доказателство за тяхната правосубектност, подобно удостоверяване може да не е релевантно за оценяването на връзката между данните и съответното физическо лице, тъй като тази връзка не е свързана с официалната или правната идентичност. По същество правото на администратора на данни да изисква допълнителна информация за удостоверяване на идентичността на дадено лице, не може да води до прекомерни изисквания и до събирането на лични данни, които не са релевантни или необходими за утвърждаване на връзката между физическото лице и поисканите лични данни.

В много случаи вече са въведени подобни процедури за установяване на автентичността. Например потребителските имена и паролите често се използват, за да получат физическите лица достъп до своите данни в акаунтите си за електронна поща, акаунтите в социалните мрежи и акаунтите, използвани за различни други услуги, някои от които физическите лица избират да използват, без да разкриват тяхното пълно име и идентичност.

Ако предаването по интернет е проблемно с оглед на обема на поисканите данни от страна на субекта на данните, вместо евентуално да се възползва от удължения срок от най-много три месеца за изпълнение на искането[26], може да се наложи също така администраторът на данни да разгледа алтернативни средства за предоставяне на данните като използване на стрийминг или съхраняване на CD, DVD или други физически носители, както и създаване на възможност за предаване на личните данни директно към друг администратор на данни (съгласно член 20, параграф 2 от ОРЗД, когато това е технически осъществимо).

- Какъв е определеният срок за отговор на искане за преносимост?

Според член 12, параграф 3 се изисква администраторът на данни да предоставя на субекта на данните „информация относно действията, предприети [...], без ненужно забавяне“ и във всички случаи „в срок от един месец от получаване на искането“. Този едномесечен срок може да бъде удължен най-много до три месеца при сложни случаи, при условие че субектът на данните е бил уведомен относно причините за въпросното забавяне в рамките на един месец от първоначалното искане.

Администраторите на данни, които изпълняват услуги на информационното общество, вероятно са по-добре оборудвани, за да могат да изпълняват искания в много кратък срок. Добра практика, за да се отговори на очакванията на потребителите, е да се определи срокът, в рамките на който обичайно може да се отговори на дадено искане за преносимост на данните и субектите на данните да бъдат уведомени за този срок.

Съгласно член 12, параграф 4 администраторът на данни, който отказва да отговори на искане за преносимост на данните, следва да уведоми субекта на данните за „причините да не предприеме действия и за възможността за подаване на жалба до надзорен орган и търсене на защита по съдебен ред“ в рамките на един месец след получаване на искането.

Администраторите на данни трябва да спазват задължението за отговор в рамките на дадения срок, дори когато се касае за отказ. С други думи, администраторът на данни не може да запази мълчание, когато бъде помолен да отговори на искане за преносимост на данните.

- В какви случаи искането за преносимост на данните може да бъде отхвърлено или да се наложи такса за него?

С член 12 се забранява на администраторите на данни да налагат такса за предоставянето на лични данни, освен ако администраторът на данни може да докаже, че исканията са явно неоснователни или прекомерни, „по-специално поради своята повторяемост“. За услуги на информационното общество, специализирани в автоматизираното обработване на лични данни, внедряването на автоматизирани системи като приложно-програмни интерфейси (API)[27] може да улесни обмена на

26 член 12, параграф 3: „Администраторът предоставя на субекта на данни информация относно действията, предприети във връзка с искане“.
27 Приложно-програмен интерфейс (API) означава интерфейсите на приложения или интернет услуги, предоставяни от администраторите на данни, за да може други системи или приложения да се свързват и да работят с техните системи.

информация със субекта на данните, а оттам и да намали потенциалната тежест, произтичаща от повтарящи се искания. Следователно би трябвало да има много малко случаи, в които администраторът на данни да може да обоснове отказа да предостави поисканата информация, дори по отношение на многократни искания за преносимост на данните.

Освен това общите разходи по процесите, които са създадени, за да се отговори на исканията за преносимост на данните, не следва да се вземат предвид при определянето на прекомерността на дадено искане. Всъщност член 12 от ОРЗД се отнася до исканията, отправени от един субект на данните, а не до общия брой искания, получени от администратора на данни. По тази причина общите разходи за внедряването на системата не следва нито да се налагат на субектите на данните, нито да се използват, за да се обоснове отказ да се изпълнят искания за преносимост.

V. Как трябва да се предоставят преносимите данни?

- Какви средства се очаква да бъдат внедрени от страна на администратора на данни за целите на предоставянето на данни?

В член 20, параграф 1 от ОРЗД е предвидено, че субектите на данни имат правото да прехвърлят данните на друг администратор без възпрепятстване от администратора, на когото личните данни са предоставени.

Подобно възпрепятстване може да бъде определено като всякакви правни, технически или финансови пречки, отбелязани от администратора на данни, за да се въздържи или да забави достъпа, предаването или повторното използване от субекта на данните или от друг администратор на данни. Такова възпрепятстване би било например: да се искат такси за предоставяне на данните, липса на оперативна съвместимост или достъп до формата на данните или API, или предоставеният формат на данните, прекомерното забавяне или сложността при извличането на пълния набор данни, умишленото объркване на наборите данни или специфични, безпричинни или прекомерни изисквания за секторно страндартизиране или акредитиране[28].

Съгласно член 20, параграф 2 администраторите на данни са задължени също така да предават преносимите данни направо на други администратори на данни, „когато това е технически осъществимо“.

Техническата осъществимост на предаването от един администратор на данни към друг, осъществявано под контрола на субекта на данните, следва да се преценява на база конкретен случай. В съображение 68 допълнително са пояснени границите на това какво е „технически осъществимо“, като е посочено, че това „не следва да поражда задължение за администраторите да възприемат или поддържат технически съвместими системи за обработване“.

От администраторите на данни се очаква да предават личните данни в оперативно съвместим формат, макар че това не поражда задължения за другите администратори на данни да поддържат тези формати. Следователно пряко предаване от един администратор на данни към друг би могло да се осъществи, когато е възможна комуникация между двете системи по сигурен начин[29] и когато получаващата система от техническа гледна точка може да получи входящите данни. Ако има технически пречки, които да не позволяват пряко предаване, администраторът на данни следва да обясни на субектите на данните какви са тези пречки, тъй като в противен случай последиците от неговото решение ще са аналогични на отказ да предприеме действия във връзка с искане на субект на данните (член 12, параграф 4).

На техническо ниво администраторите на данни следва да разгледат и преценят два различни и допълващи се варианта на предоставяне на преносимите данни на разположение на субектите на данни или на други администратори на данни:

28 Възможно е все пак да възникнат някои основателни пречки, които са свързани с правата и свободите на други лица, посочени в член 20, параграф 4, или които се отнасят до сигурността на собствените системи на администраторите на данни. Администраторът на данни следва да носи отговорност за обосноваване на причините защо въпросните пречки са основателни и защо не представляват възпрепятстване по смисъла на член 20, параграф 1.

29 Посредством съобщение с установяване на автентичност и с необходимото ниво на криптиране на данните.

- пряко предаване на целия набор от преносими данни (или няколко извадки от части от общ набор данни);

- автоматизиран инструмент, позволяващ извличането на релевантните данни.

Администраторите на данни може да предпочитат втория вариант в случаи, касаещи сложни и големи набори данни, тъй като при него е възможно извличането на всяка част от набора данни, която е от значение за субекта на данните в контекста на неговото искане, може да допринесе за намаляването на риска до минимум и евентуално да позволи използването на механизми за синхронизиране на данни[30] (например в рамките на редовна комуникация между администраторите на данни). За „новия“ администратор на данни това може да е по-добрият начин да се осигури съответствие, а за първоначалния администратор на данни би било добра практика за намаляване на рисковете за неприкосновеността на личния живот.

Тези два различни и евентуално допълващи се начина за предоставяне на релевантните преносими данни може да бъдат приложени чрез предоставянето на данните на разположение посредством различни средства, например като сигурни съобщения, SFTP сървър, сигурен WebAPI или WebPortal. Субектите на данни следва да имат възможност да използват персонално хранилище за данни, персонална система за управление на информация[31] или други видове доверени трети страни, да държат и съхраняват личните данни и да дават разрешение на администраторите на данни за достъп и обработване на личните данни, когато това е необходимо.

- Какъв е очакваният формат на данните?

С ОРЗД за администраторите на данни се поставят изисквания да предоставят личните данни, които са поискани от дадено физическо лице, във формат, позволяващ тяхната повторна употреба. По-специално в член 20, параграф 1 от ОРЗД се казва, че личните данни трябва да се предоставят „в структуриран, широко използван и пригоден за машинно четене формат“. В съображение 68 е дадено допълнително пояснение, че този формат следва да бъде оперативно съвместим − термин, който в ЕС се определя[32] като:

способността на различни и разнообразни по своя характер организации да си взаимодействат за постигане на взаимноизгодни и съгласувани общи цели, което включва обмен на информация и знания между организациите чрез стопанските процеси, които те поддържат, посредством обмен на данни между съответните им системи на ИКТ.

Термините „структуриран“, „широко използван“ и „пригоден за машинно четене“ представляват набор от минимални изисквания, които следва да улеснят оперативната съвместимост на формата на данните, в който администраторът на данни ги предоставя. По този начин „структуриран, широко използван и пригоден за машинно четене“ са спецификации за средствата, а оперативната съвместимост е желаният резултат.

В съображение 21 от Директива 2013/37/ЕС[33,34] „машинночетим“ е определен като:

файлов формат, който е структуриран по начин, по който софтуерните приложения да могат лесно да идентифицират, разпознават и извличат специфични данни, включително отделни факти и тяхната вътрешна структура. Данните, кодирани във файлове, които са структурирани в машинночетим формат, са машинночетими данни. Машинночетимите формати могат да бъдат отворени или да бъдат защитени от право на собственост; те могат да бъдат официални стандарти или не. Документи, кодирани във файлов формат, който ограничава автоматичната

30 Механизмът за синхронизиране може да спомогне да се изпълнят общите задължения по член 5 от ОРЗД, в който се казва, че „личните данни са (...) точни и при необходимост да бъдат поддържани в актуален вид“.

31 Относно персоналните системи за управление на информация (PIMS) вж. например Становище 9/2016 на ЕНОЗД, което е на разположение на: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mYSite/shared/Documents/Consultation/Opinions/2016/16 -10-20 PIMS opinion EN.pdf.

32 Член 2 от Решение № 922/2009/ЕО на Европейския парламент и на Съвета от 16 септември 2009 г. за решения за оперативна съвместимост за европейските публични администрации (ISA) (ОВ L 260, 3.10.2009 г., стр. 20).

33 Директива 2013/37/ЕС за изменение на Директива 2003/98/Е0 относно повторната употреба на информацията в обществения сектор.

34 В речника на ЕС (http://eur-lex.europa.eu/eli-register/glossary.html) са дадени допълнителни пояснения относно очакванията, свързани с понятията, които са използвани в настоящите насоки, като пригоден за машинно четене, оперативна съвместимост, отворен формат, стандарт, метаданни.

обработка поради факта, че данните не могат въобще или не могат лесно да бъдат извлечени от тези документи, не следва да се считат за такива в машинночетим формат. Държавите членки, по целесъобразност, следва да насърчават използването на отворени, машинночетими формати.

Като се има предвид широкият диапазон от потенциални типове данни, които може да бъдат обработвани от даден администратор на данни, ОРЗД не налага конкретни препоръки относно формата на предоставяните лични данни. В различните сектори най-подходящият формат е различен и може вече да съществуват подходящи формати, които винаги следва да се избират, за да се постигне целта за оперативна съвместимост и да се осигури за субекта на данните висока степен на преносимост на данните. Форматите, които подлежат на скъпоструващи лицензионни ограничения, не биха били приети като подходящ подход.

В съображение 68 се пояснява, че „*правото на субекта на данни да предава или получава отнасящи се до него лични данни не следва да поражда задължение за администраторите да възприемат или поддържат технически съвместими системи за обработване*“. **Следователно с преносимостта се цели създаването на оперативно съвместими системи, а не на съвместими системи[35].**

Очаква се личните данни да се предоставят във формати с високо ниво на абстракция от всеки вътрешен или собствен формат. В това качество преносимостта на данните предполага допълнителен слой на обработване на данните от администраторите на данни, за да бъдат извлечени данните от платформата и личните данни да бъдат филтрирани извън обхвата на преносимостта, като например логически изведени данни или данни, свързани със сигурността на системите. По този начин администраторите на данни се насърчават предварително да идентифицират в техните собствени системи данните, които попадат в обхвата на преносимостта. Това допълнително обработване на данните ще се счита за допълнително към основното обработване на данните, тъй като то не се извършва с оглед на постигането на нова цел, определена от администратора на данни.

Когато в даден отрасъл или в даден контекст няма широко използвани формати, **администраторите на данни следва да предоставят личните данни в широко използвани отворени формати (например XML, JSON, CSV и др.) заедно с полезни метаданни с възможно най-подходящата степен на детайлност,** като се запази високо ниво абстракция. В тази връзка следва да се използват подходящи метаданни, за да се опише точното значение на обменяната информация. Тези метаданни трябва да са достатъчни, за да се позволи функционирането и повторното използване на данните, но, разбира се, без да се разкриват търговски тайни. Следователно, малка е вероятността, ако на физическо лице се предоставят версии в PDF на входящите електронни съобщения, те да са достатъчно структурирани или описателни, за да може данните за входящите електронни съобщения лесно да се използват повторно. Вместо това данните за електронните съобщения следва да бъдат предоставени във формат, в който се запазват всички метаданни, за да може данните ефективно да се използват повторно. Съответно, когато избира формата на данните, в който да предоставя личните данни, администраторът на данни следва да вземе предвид по какъв начин този формат ще повлияе или попречи на правото на физическото лице да използва данните повторно. В случаи, в които администраторът на данни може да даде избор на субекта на данните по отношение на предпочитания формат на личните данни, следва да бъде предоставено ясно обяснение за въздействието на избора. Все пак обработването на допълнителни метаданни с единствената цел, че те може да са нужни или желани, за да се отговори на искане за преносимост на данните, не дава законно основание за такова обработване.

Работната група по член 29 силно препоръчва сътрудничество между заинтересованите страни от отрасъла и търговските органи за съвместна работа по общ набор от оперативно съвместими стандарти и формати, за да се изпълнят изискванията, свързани с правото на преносимост на данните. Това предизвикателство е било разгледано също така от Европейската рамка за оперативна съвместимост (EIF), по л иния на която е разработен съгласуван подход към

35 В ISO/IEC 2382-01 оперативната съвместимост е определена, както следва: „способността за общуване, изпълнение на програми или предаване на данни между различни функционални единици по начин, изискващ от потребителя малко или никакви знания относно уникалните характеристики на тези единици.“

оперативната съвместимост за организации, които желаят съвместно да предоставят публични услуги. В обхвата на нейната приложимост рамката определя набор от общи елементи като речник, понятия, принципи, политики, насоки, препоръки, стандарти, спецификации и практики[36].

- Как следва да се процедира със събирането на лични данни с голям обем или сложност?

В ОРЗД не е посочено как да се подхожда към предизвикателството по отговаряне на искане в случай на събиране на данни с голям обем, със сложна структура или ако възникнат други технически въпроси, които може да породят трудности за администраторите на данни или за субектите на данните.

Във всички случаи обаче е съществено важно физическото лице да може напълно да разбере определението, схемата и структурата на личните данни, които може да бъдат предоставени от администратора на данни. Възможно е например първо данните да бъдат предоставени в обобщен вид, като се използват информационни таблици, позволяващи на субекта на данните да не пренася личните данни в пълен обем, а поднабори от тях. Администраторът на данни следва да направи обзор „в кратка, прозрачна, разбираема и лесно достъпна форма, на ясен и прост език“ (вж. член 12, параграф 1 от ОРЗД) по такъв начин, че субектът на данните винаги да разполага с ясна информация какви данни да свали или предаде на друг администратор на данни във връзка с дадена цел. Например субектите на данни следва да имат възможност да използват софтуерни приложения за лесното идентифициране, разпознаване и обработване на специфични данни от него.

Както е посочено по-горе, практичен начин, по който администраторът на данни може да отговаря на искания за преносимост на данните, може да бъде чрез предлагане на подходящ сигурен и документиран API. Това може да даде възможност на физическите лица да отправят към администратора на данни искания за техните лични данни чрез техния собствен софтуер или чрез софтуера на трета страна, или да предоставят разрешение други лица да направят това от тяхно име (включително друг администратор на данни), както е предвидено в член 20, параграф 2 от ОРЗД. Като се предоставя достъп до данни чрез API с външен достъп, може да е възможно също така да се предложи по-усъвършенствана система за достъп, позволяваща на физическите лица да отправят последващи искания за данни, независимо дали за пълно сваляне, или като делта функция, съдържаща само промени, направени след последното сваляне, без тези допълнителни искания да са в тежест за администратора на данни.

- Как може да бъде гарантирана сигурността на преносимите данни?

По принцип администраторите на данни следва да гарантират „подходящо ниво на сигурност на личните данни, включително защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане, като се прилагат подходящи технически или организационни мерки“ в съответствие с член 5, параграф 1, буква е) от ОРЗД.

Въпреки това при предаването на лични данни към субекта на данните също може да възникнат някои проблеми по сигурността:

Как администраторите на данни могат да гарантират сигурното предаване на личните данни към правилното лице?

Тъй като с преносимостта на данните се цели личните данни да бъдат извадени от информационната система на администратора на данни, предаването може да се превърне в потенциален източник на риск за тези данни (по-специално нарушение на сигурността на данните по време на предаването). Администраторът на данни е отговорен за предприемането на всички необходими мерки по сигурността, за да се гарантира не само сигурното предаване на личните данни (чрез използването на комплексни решения или криптиране на данните) до правилното местоназначение (чрез използването на сериозни мерки за установяване на автентичността), но също така да се запази защитата на личните данни, които остават в техните системи, както и прозрачни процедури за справяне с евентуални нарушения на сигурността на данните[37]. Следователно администраторите на данни

36 Източник: http://ec.europa.eu/isa/documents/isa_annex_ii_eif_en.pdf.

37 В съответствие с Директива (ЕС) 2016/1148 относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза

следва да оценяват конкретните рискове, свързани с преносимостта на данните и да предприемат подходящи мерки за намаляване на рисковете.

Тези мерки за намаляване на риска може да включват: ако за субекта на данните вече е необходимо установяване на автентичността — използване на допълнителна информация за

установяване на автентичността като споделена тайна или друг фактор за целта, като например еднократна парола; прекратяване или спиране на предаването, ако има съмнение, че акаунтът е бил компрометиран; в случаи на пряко предаване от един администратор на данни към друг администратор на данни, следва да се използва установяване на автентичността чрез предоставяне на мандат, като например установяване на автентичността чрез токен-устройство.

Тези мерки по сигурността не трябва да бъдат възпрепятстващи по своя характер и не трябва да пречат на потребителите да упражняват техните права, например като налагат допълнителни разходи.

Как може да се помогне на потребителите да имат сигурност при съхранението на техните лични данни в собствените им системи?

Когато извличат техните лични данни от дадена онлайн услуга, винаги има риск потребителите да ги съхранят в системи с по-ниско ниво на сигурност от предлаганото от услугата. Субектите на данните, които отправят искане за данни, носят отговорност за определяне на правилните мерки, за да се гарантира сигурността на личните данни в тяхната собствена система. Потребителят обаче следва да бъде осведомен за това, за да може да предприеме стъпки за защита на информацията, която е получил. Като пример за водеща практика, администраторите на данни могат също така да препоръчват подходащ(и) формат(и), инструменти за криптиране и други мерки за сигурност, за да подпомогнат субектите на данните за постигането на тази цел.

ПРИЛОЖЕНИЕ — Често задавани въпроси

1. Какво се цели с правото на преносимост на данните?

По същество преносимостта на данните дава възможност на субектите на данни да получават и да използват „своите“ данни за собствени цели и във връзка с различни услуги. Това право ги улеснява да преместват, копират или прехвърлят лични данни от една ИТ среда към друга без възпрепятстване. Освен че по този начин на потребителя се предоставят правомощия чрез предотвратяване на поставянето му в зависимост („lock-in“), се предполага, че това право ще повиши възможностите за иновации и обмен на лични данни между администраторите на данни по безопасен и сигурен начин под контрола на субекта на данните.

2. Какви възможности дава упражняването на правото на преносимост на данните?

Първо, това е право да се получат лични данни („в структуриран, широко използван и пригоден за машинно четене формат“), които се обработват от администратор на данни, и да се съхранят за по-нататъшна лична употреба на частно устройство, без да се прехвърлят към друг администратор на данни. Това право предлага на субектите на данните лесен начин да управляват самостоятелно своите лични данни. Второ, това право дава възможност на субектите на данни също така да предават своите лични данни от един администратор на данни към друг администратор на данни „без възпрепятстване“ и ги улеснява да преместват, копират или прехвърлят лични данни от една ИТ среда към друга.

3. Кои инструменти се препоръчват при отговаряне на исканията за преносимост на данните?

Първо, администраторите на данни следва да предлагат на субекта на данните възможност за директно сваляне и, второ, те следва да позволяват на субектите на данните директно да предават данните към друг администратор на данни. Това например може да се осъществи чрез осигуряването на приложно-програмен интерфейс.

Субектите на данни могат да използват също така хранилище за лични данни — доверена трета страна, която да съхранява личните данни и да предоставя разрешение за достъп на администраторите

на данни с цел обработване на личните данни според нуждите, така че да може данните да се прехвърлят лесно от един администратор на друг.

4. Доколко администраторите на данни са отговорни за данните, които се прехвърлят или получават чрез упражняване на правото на преносимост на данните?

Администраторите на данни, които отговарят на искания за преносимост на данните, не носят отговорност за обработването от страна на субекта на данните или от друго дружество, което получава данните. Наред с това получаващият администратор на данни носи отговорност да гарантира, че предоставените преносими данни са релевантни и не са прекомерни, що се отнася до новото обработване на данни, че субектът на данните ясно е уведомен за целта на новото обработване и в по-общ план, че са спазени принципите за защита на данните, които са приложими към даденото обработване в съответствие с разпоредбите на ОРЗД.

5. Упражняването на правото на преносимост на данните засяга ли упражняването на други права на субекта на данните?

Когато физическо лице упражнява своето право на преносимост на данните (или друго право по ОРЗД), въпросното лице прави това, без да се засяга никое друго право. Субектът на данните може да упражнява своите права, докато администраторът на данни все още обработва данните. Например субектът на данните може да продължи да използва и да се ползва от услугите на администратора на данни дори след приключване на операцията по преносимост на данните. Също така, ако субектът на данните желае да упражни своето право на изтриване, на възразяване или на достъп до своите лични данни, администраторът на данни не може да използва предишно или последващо упражняване на правото на преносимост на данните като основание за забавяне или отказ да изпълни други права на субекта на данните. Освен това преносимостта на данните не води автоматично до изтриване на данните от системите на администратора на данни и не засяга първоначалния период на запазване, който е приложим за предадените данни според правото на преносимост на данните.

6. Кога е приложимо правото на преносимост на данните?

Това ново право е приложимо при **три кумулативни условия**.

Първо, поисканите лични данни следва да се обработват с автоматизирани средства (т.е. без досиета на хартиен носител) на базата на предварителното съгласие на субекта на данните или на изпълнението на договор, по който субектът на данните е страна.

Второ, поисканите лични данни трябва да засягат субекта на данните и да са предоставени от него. Работната група по член 29 препоръчва на администраторите на данни да не приемат твърде ограничително тълкуване на изречението „лични данни, свързани със субекта на данните“, когато данни на трети страни се съдържат в набор от данни, свързани със субекта на данните и предоставени от него, и се използват за лични цели от субекта на данните, който е отправил искането. Обичайни примери за набори от данни, включващи данни на трети страни, са телефонни записи (съдържащи входящи и изходящи повиквания), които субект на данните желае да получи, или хронология на операциите с банкова сметка, включваща входящи плащания от трети страни.

Личните данни може да се считат за предоставени от субекта на данните, когато са „предоставени“ съзнателно и активно от субекта на данните, като данни от акаунт (например адрес за кореспонденция, потребителско име, възраст), предоставени чрез онлайн формуляри, но също така когато са генерирани от или събрани чрез дейността на потребителите посредством използването на услугата или устройството. Обратно, личните данни, които са производни или са логически изведени от данните, предоставени от субекта на данните, като например потребителски профил, създаден чрез анализ на първичните данни, събрани от интелигентно измервателно устройство, са изключени от обхвата на правото на преносимост на данните, тъй като те не са предоставени от субекта на данните, а са създадени от администратора на данните.

Според третото условие упражняването на това ново право не следва да засяга неблагоприятно правата и свободите на трети страни. Например ако наборът от данни, който се предава по искане на субекта на данните, съдържа лични данни, свързани с други физически лица, новият администратор

на данните следва да обработва тези данни само ако има подходящо правно основание за това. Обикновено за подходящо се приема обработване единствено под контрола на субекта на данните, в рамките на изцяло лични или домакински дейности.

7. Как следва да бъдат информирани субектите на данните относно това ново право?

Администраторите на данни следва да информират субектите на данни относно съществуването на правото на преносимост на данните „в кратка, прозрачна, разбираема и лесно достъпна форма, на ясен и прост език“. В това отношение Работната група по член 29 препоръчва администраторите на данни ясно да обясняват разликата между различните типове данни, които субектът на данните може да получава въз основа на правото на преносимост или на правото на достъп, както и да предоставят конкретна информация относно правото на преносимост на данните преди евентуално закриване на акаунт, за да може субектът на данните да извлече или съхрани своите лични данни.

Овен това администраторите на данни, които получават преносими данни по искане на субекта на данните, като най-добра практика могат да предоставят на субектите на данни пълна информация за естеството на личните данни, които са релевантни за предоставянето на услугите им.

8. По какъв начин администраторът на данни може да идентифицира субекта на данните, преди да отговори на неговото искане?

Работната група по член 29 препоръчва администраторът на данните да въведе подходящи процедури, даващи възможност на физическото лице да отправя искане за преносимост на данните и да получава данните, свързани с него. Администраторите на данни трябва да разполагат с процедура за установяване на автентичността, за да могат категорично да се убедят в идентичността на субекта на данните, който иска неговите лични данни или в по-общ план упражнява правата, предоставени от ОРЗД.

9. Какъв е предвиденият срок да се отговори на искане за преносимост?

Съгласно член 12 на администратора на данни е забранено да налага такса за предоставянето на личните данни, освен ако администраторът на данни може да докаже, че исканията са явно неоснователни или прекомерни, „*по-специално поради своята повторяемост*“. Малка е вероятността при услуги на информационното общество или аналогични онлайн услуги, специализирани в автоматичната обработка на лични данни, отговарянето на множество искания за преносимост на данните да бъде счетено за налагащо прекомерна тежест. В такива случаи Работната група по член 29 препоръчва да се определи разумен срок, който е съобразен с контекста, и да се съобщи на субектите на данните.

10. Как трябва да се предоставят преносимите данни?

Личните данни следва да се предават в структуриран, широко използван и пригоден за машинно четене формат. Тези спецификации, които са приложими към средствата, следва да гарантират оперативната съвместимост на формата, в който данните се предоставят от администратора на данни, като оперативната съвместимост се счита за желания резултат. Това все пак не означава, че администраторите на данни следва да поддържат съвместими системи. Освен това администраторите на данни следва да предоставят с данните възможно най-много метаданни с възможно най-доброто ниво на точност и детайлност, за да се запази точният смисъл да предаваната информация.

Като се има предвид широкият диапазон от потенциални типове данни, които може да се обработват от администратора на данни, с ОРЗД не се налагат конкретни препоръки относно формата, в който следва да се предоставят личните данни. Най-подходящият формат е различен в различните сектори и може вече да съществуват подходящи формати, но те винаги следва да се избират с оглед на постигането на целта за разбираемост.

Работната група по член 29 силно насърчава сътрудничеството между заинтересованите страни от отраслите и търговските органи за разработването на общ набор от оперативно съвместими стандарти и формати, свързани с изпълнението на изискванията на правото на преносимост на данните.

НАСОКИ НА РАБОТНА ГРУПА ПО ЧЛ. 29 ОТ ДИРЕКТИВА 95/46/ЕО ОТНОСНО ПРИЛАГАНЕТО И ОПРЕДЕЛЯНЕТО НА АДМИНИСТРАТИВНИТЕ НАКАЗАНИЯ "ГЛОБА" ИЛИ "ИМУЩЕСТВЕНА САНКЦИЯ" ЗА ЦЕЛИТЕ НА РЕГЛАМЕНТ (ЕС) 2016/79

I. Въведение

ЕС проведе всеобхватна реформа на регулирането по отношение на защитата на данните в Европа. Реформата се основава на няколко стълба (основни компонента): съгласувани правила, опростени процедури, координирани действия, участие на ползвателите, по-ефективно информиране и засилени правомощия за прилагане.

Отговорностите на администраторите и обработващите лични данни бяха увеличени, за да се гарантира, че личните данни на лицата са защитени по ефективен начин. Надзорните органи разполагат с правомощия да гарантират, че принципите на Общия регламент относно защитата на данните (наричан по-нататък „Регламентът"), както и правата на засегнатите лица се спазват в съответствие с буквата и духа на Регламента.

Последователното прилагане на правилата за защита на данните е от основно значение за хармонизирания режим за защита на данните. Административните наказания „глоба" или „имуществена санкция" представляват основен елемент в новия режим на правоприлагане, въведен с Регламента, като заемат важно място в набора от инструменти за правоприлагане на надзорните органи заедно с другите мерки, предвидени в член 58.

Настоящият документ е предназначен да се използва от надзорните органи, за да се гарантира по-добро прилагане и изпълнение на Регламента, и изразява тяхното общо разбиране на разпоредбите на член 83 от Регламента, както и взаимодействието му с членове 58 и 70 и съответните им съображения.

По-специално съгласно член 70, параграф 1, буква д) Европейският комитет по защита на данните (наричан по-нататък „ЕКЗД") е оправомощен да издава насоки, препоръки и най-добри практики с цел насърчаване на съгласуваното прилагане на Регламента, а в член 70, параграф 1, буква к) се предвиждат насоки относно определянето на размера на административните наказания „глоба" или „имуществена санкция".

Настоящите насоки не са изчерпателни, нито включват разяснения относно разликите между административноправните, гражданскоправните или наказателноправните системи при налагането на административни санкции като цяло.

За да се постигне съгласуван подход по отношение на налагането на административните наказания „глоба" или „имуществена санкция", който да отразява адекватно всички принципи в настоящите насоки, ЕКЗД постигна съгласие по общо разбиране за критериите за оценка в член 83, параграф 2 от Регламента, и следователно ЕКЗД и отделните надзорни органи са съгласни да използват настоящите насоки като общ подход.

II. Принципи

След като бъде установено нарушение на Регламента въз основа на оценка на фактите по случая, компетентният надзорен орган трябва да определи най-подходящата корективна мярка или мерки с цел справяне с нарушението. В разпоредбите на член 58, параграф 2, букви б)–й)[1] се посочва какви инструменти могат да бъдат използвани от надзорните органи с цел справяне с нарушение от страна на администратор или обработващ лични данни. При използването на тези правомощия надзорните органи трябва да спазват следните принципи:

1 В член 58, параграф 2, буква а) се предвижда, че могат да се отправят предупреждения, когато „има вероятност операции по обработване на данни [...] да нарушат разпоредбите на настоящия регламент". С други думи, в обхванатия от разпоредбата случай все още не е извършено нарушение на Регламента.

1. Нарушението на Регламента следва да води до налагане на „еквивалентни санкции“

Понятието „еквивалентност“ е от основно значение при определянето на обхвата на задълженията на надзорните органи, за да се гарантира съгласуваност при използването на корективните им правомощия съгласно член 58, параграф 2 като цяло, и в частност налагането на административни наказания „глоба“ или „имуществена санкция“[2].

За да се гарантира последователно и високо ниво на защита на физическите лица, както и за да се премахнат препятствията пред движението на лични данни в Съюза, ***нивото на защита следва да бъде равностойно*** *във всички държави членки (съображение 10).* В съображение 11 се пояснява фактът, че равностойното ниво на защита на личните данни навсякъде в Съюза наред с другото изисква *„еквивалентни правомощия за наблюдение и гарантиране на спазването на правилата за защита на личните данни и еквивалентни санкции за нарушенията в държавите членки*“. В допълнение към това еквивалентните санкции във всички държави членки, както и ефективното сътрудничество между надзорните органи на отделните държави членки се възприемат като начин „*да се попречи на различията да възпрепятстват свободното движение на лични данни в рамките на вътрешния пазар*“, в съответствие със съображение 13 от Регламента.

В сравнение с Директива 95/46/ЕО в Регламента се определя по-солидна основа за по-високо ниво на съгласуваност, тъй като Регламентът е пряко приложим в държавите членки. Докато надзорните органи действат „напълно независимо“ (член 52) от националните правителства, администраторите или обработващите лични данни, те са задължени да си сътрудничат *„с оглед осигуряване на съгласувано прилагане и изпълнение на настоящия регламент*“ (член 57, параграф 1, буква ж).

В Регламента се призовава за по-голяма съгласуваност при налагането на санкции в сравнение с Директива 95/46/ЕО. В трансгранични случаи съгласуваността се постига най-вече чрез механизма за сътрудничество („обслужване на едно гише“) и до известна степен чрез механизма за съгласуваност, определен в новия Регламент.

В обхванатите от Регламента случаи от национален мащаб надзорните органи ще прилагат настоящите насоки в дух на сътрудничество в съответствие с член 57, параграф 1, буква ж) и член 63 с цел да се гарантира последователно прилагане и изпълнение на Регламента. Въпреки че надзорните органи остават независими при избора на корективни мерки измежду посочените в член 58, параграф 2, следва да се избягва избирането на различни корективни мерки от надзорните органи в сходни случаи.

Същият принцип се прилага, когато тези корективни мерки се налагат под формата на глоби или имуществени санкции.

2. Като всички корективни мерки, налагани от надзорните органи, административните наказания „глоба“ или „имуществена санкция“ следва да бъдат „ефективни, пропорционални и възпиращи“

Подобно на всички корективни мерки като цяло, административните наказания „глоба“ или „имуществена санкция“ следва да отразяват адекватно естеството, тежестта и последиците от нарушението, а надзорните органи трябва да оценят всички факти по случая по начин, който е последователен и обективно обоснован. Оценката за това, какви мерки са ефективни, пропорционални и възпиращи във всеки отделен случай, също така ще трябва да отразява целта, преследвана с избраната корективна мярка, т.е. възстановяване на спазването на правилата или санкциониране на неправомерно поведение (или и двете).

Надзорните органи следва да определят корективни мерки, които са „*ефективни, пропорционални и възпиращи*“ (член 83, параграф 1), както в случаите от национален мащаб (член 55), така и в случаите, свързани с трансгранично обработване на лични данни (съгласно определението в член 4, параграф 23).

2 Дориакоправнитесистеминанякоидържави–членкинаЕС,непозволяватналаганенаадминистративнитенаказания„глоба”или„имущественасанкция”, посочени в Регламента, прилагането на правилата в тези държави членки трябва да има ефект, равностоен на административни наказания „глоба” или „имуществена санкция”, налагани от надзорни органи (съображение 151). Съдилищата са обвързани от Регламента, но не и от настоящите насоки на ЕКЗД.

В настоящите насоки се признава, че е възможно в националното законодателство да са определени допълнителни изисквания относно процедурите по правоприлагане, които надзорните органи трябва да следват. Те могат да включват например съобщаване на адрес, формуляри, крайни срокове за представяне на становища, обжалване, правоприлагане, заплащане[3].

Такива изисквания обаче не следва да възпрепятстват на практика постигането на ефективност, пропорционалност или възпиращ ефект.

Ефективността, пропорционалността и възпиращият ефект ще бъдат определени по-точно с практиките, които ще се установят в рамките на надзорните органи (във връзка със защитата на данните, както и натрупания опит от други регулаторни сектори), както и чрез съдебната практика, свързана с тълкуването на тези принципи.

С цел да налага глоби или имуществени санкции, които са ефективни, пропорционални и възпиращи, надзорният орган следва да използва определението на понятието за предприятие, предоставено от Съда на ЕС за целите на прилагането на членове 101 и 102 от ДФЕС, а именно, че понятието за предприятие **се разбира като означаващо** стопанска единица, която може да се състои от дружеството майка и всички участващи дъщерни дружества. В съответствие с правото на ЕС и европейската съдебна практика[4] понятието „предприятие“ трябва да се разбира като стопанска единица, която извършва търговски/стопански дейности, независимо от съответното юридическо лице (съображение 150).

3. Компетентният надзорен орган прави оценка „ във всеки конкретен случай“

Административните наказания „глоба“ или „имуществена санкция“ могат да се налагат във връзка с редица нарушения. В член 83 от Регламента се предвижда хармонизиран подход към нарушенията на задълженията, посочени изрично в параграфи 4−6. Съгласно законодателството на държавите членки прилагането на член 83 може да бъде разширено, така че да обхване публичните органи и органите, установени в съответната държава членка. Освен това законодателството на държавите членки може да предвижда възможност или дори задължение за налагането на глоба или имуществена санкция за нарушаване на други разпоредби, различни от посочените в член 83, параграфи 4−6.

Съгласно Регламента се изисква оценяването на всеки случай да се извършва индивидуално[5]. Отправната точка за такава индивидуална оценка е член 83, параграф 2. Този параграф гласи: „*Когато се взема решение дали да бъде наложено административно наказание „глоба“ или „имуществена санкция“ и се определя нейният размер, във всеки конкретен случай надлежно се разглеждат следните елементи...*“ В съответствие с това и също така с оглед на съображение 148[6] надзорният

3 Например в конституционната рамка и законопроекта относно защитата на данните в Ирландия се предвижда, че преди да се извърши оценка на размера на санкцията или санкциите, се взема официално решение относно наличието на нарушение, което се съобщава на съответните страни. Решението относно наличието на нарушение не подлежи на преразглеждане по време на оценката на размера на санкцията или санкциите.

4 Определението в съдебната практика на Съда на ЕС е: „понятието за предприятие обхваща всяко образувание, което извършва стопанска дейност, независимо от неговия правен статут и начина му на финансиране” (дело Hofner и Eisner, ECLI:EU:C:1991:161, т. 21). Предприятието „трябва да се схваща като обозначаващо една стопанска единица, макар и от правна гледна точка тази стопанска единица да е съставена от няколко физически или юридически лица” (дело Confederation Espanola de Empresarios de Estaciones de Servicio, ECLI:EU:C:2006:784, т. 40).

5 В допълнение към прилагането на критериите по член 83 съществуват и други разпоредби за укрепване на основата за прилагането на този подход, като например:

- съображение 141: „Разследването въз основа на жалби следва да се извършва под съдебен контрол и в целесъобразна за конкретния случай степен”.
- съображение 129: „Надзорните органи следва да упражняват правомощията си в съответствие с подходящите процедурни гаранции, определени в правото на Съюза и правото на държава членка, независимо, справедливо и в разумен срок”. По-специално всяка мярка следва да бъде подходяща, необходима и пропорционална с оглед на осигуряването на съответствие с настоящия регламент, като се отчитат обстоятелствата при всеки конкретен случай...”.
- член 57, параграф 1, буква е): „[...] разглежда жалбите, подадени от субект на данни или от структура, организация или сдружение в съответствие с член 80, и разследва предмета на жалбата, доколкото това е целесъобразно”.

6 „За да се укрепи прилагането на правилата на настоящия регламент, освен или вместо подходящи мерки, наложени от надзорния орган съгласно настоящия регламент, при нарушение на регламента следва да се налагат санкции, включително административни наказания „глоба” или „имуществена санкция”. При леки нарушения или ако глобата, която може да бъде наложена, представлява несъразмерна тежест за физическо лице, вместо глоба може да бъде отсъдено порицание. Следва обаче да се отдаде надлежно внимание на естеството, тежестта и продължителността на нарушението, умишления характер на нарушението, действията за смекчаване на последиците от претърпените вреди, степента на отговорност или евентуални предишни нарушения от подобен характер, начина, по който нарушението е станало известно на надзорния орган, спазването на мерките, наложени на

орган носи отговорност да определи най-подходящата мярка или мерки. В случаите, посочени в член 83, параграфи 4−6, този избор **трябва** да включва разглеждане на всички корективни мерки, което означава и да се разгледа дали да се наложи подходящо административно наказание „глоба“ или „имуществена санкция“, било то самостоятелно или в съчетание с друга корективна мярка съгласно член 58, параграф 2.

Глобите или имуществените санкции представляват важен инструмент, който надзорните органи следва да използват в подходящи обстоятелства. Надзорните органи се насърчават да следват внимателно обмислен и балансиран подход при използването на корективни мерки, така че отговорът на нарушението да бъде както ефективен и възпиращ, така и пропорционален. Целта е глобите или имуществените санкции да не се разглеждат като крайна мярка и да не се избягва налагането им, но същевременно и да не се използват по начин, който би обезсилил ефективността им като инструмент.

Когато ЕКЗД е компетентен в съответствие с член 65 от Регламента, той приема решения със задължителен характер по спорове между органи, свързани по-специално с определянето дали е налице нарушение. Когато чрез относимо и обосновано възражение се повдигне въпросът дали корективната мярка е в съответствие с Регламента, в решението на ЕКЗД също така се разглежда начинът, по който са спазени принципите на ефективност, пропорционалност и възпиране във връзка с административното наказание „глоба“ или „имуществена санкция“, предложено в проекта на решение на компетентния надзорен орган. Отделно ще бъдат изготвени насоки на ЕКЗД относно прилагането на член 65 от Регламента с повече подробности относно вида решение, което следва да се взема от ЕКЗД.

4. Хармонизираният подход към административните наказания „глоба“ или „имуществена санкция“ в областта на защитата на данните изисква активно участие и обмен на информация между надзорните органи

В настоящите насоки се признава, че за някои национални надзорни органи правомощията за налагане на глоби или имуществени санкции представляват новост в областта на защитата на данните, като пораждат многобройни въпроси, що се отнася до ресурсите, организацията и процедурата. Съществено е, че решенията, чрез които надзорните органи упражняват предоставените им правомощия за налагане на глоби или имуществени санкции, ще подлежат на обжалване пред националните съдилища.

Надзорните органи следва да осъществяват сътрудничество помежду си и ако е целесъобразно, с Европейската комисия, чрез определените в Регламента механизми за сътрудничество, така че да се подпомогнат официалният и неофициалният обмен на информация, например чрез провеждане на редовни работни срещи. Това сътрудничество следва да е съсредоточено върху техния опит и практика при упражняването на правомощията за налагане на глоби или имуществени санкции, така че в крайна сметка да се постигне подобрена съгласуваност.

Проактивното споделяне на информация, в допълнение към нововъзникващата съдебна практика относно използването на тези правомощия за налагане на глоби или имуществени санкции, може да доведе до преразглеждането на принципите или специфичните подробности в настоящите насоки.

III. Критерии за оценка в член 83, параграф 2

В член 83, параграф 2 е представен списък с критерии, които се очаква да бъдат използвани от надзорните органи, когато се преценява дали следва да бъде наложена глоба или имуществена санкция и какъв да бъде нейният размер. Препоръчва се не да бъдат оценявани многократно едни и

администратора или на обработващия лични данни, придържането към кодекс на поведение и всякакви други утежняващи или смекчаващи фактори. Налагането на санкции, включително административни наказания „глоба” или „имуществена санкция”, следва да подлежи на подходящи процедурни мерки за защита в съответствие с общите принципи на правото на Съюза и Хартата, включително ефективна съдебна защита и справедлив съдебен процес”.

същи критерии, а да се извършва оценка, при която да се вземат предвид всички обстоятелства по конкретния случай, както е предвидено в член 83[7].

Заключенията от първия етап на оценката могат да се използват на втория етап, свързан с определянето на размера на глобата или имуществената санкция, като по този начин се избягва необходимостта от повторно оценяване с използване на същите критерии.

В настоящия раздел се съдържат насоки за надзорните органи по отношение на начина на тълкуване на отделните факти по случая с оглед на критериите в член 83, параграф 2.

а) естеството, тежестта и продължителността на нарушението

В разпоредбите на член 83, параграфи 4–6 почти всички задължения на администраторите и обработващите лични данни съгласно Регламента са категоризирани в зависимост от тяхното **естество.** С определянето в Регламента на два различни максимални размера на административните наказания „глоба“ или „имуществена санкция“ (10/20 милиона евро) вече се посочва, че нарушението на някои разпоредби на Регламента може да е по-сериозно от нарушението на други разпоредби. При все това, когато компетентният надзорен орган оценява фактите по случая в светлината на общите критерии, предвидени в член 83, параграф 2, той може да реши, че в конкретния случай има по-голяма или съответно по-малка необходимост да се реагира с корективна мярка под формата на глоба или имуществена санкция. Когато бъде наложена глоба или имуществена санкция като единствената или като една от няколко подходящи корективни мерки, се прилага категоризацията от Регламента (член 83, параграфи 4–6), за да се определи максималната глоба или имуществена санкция, която може да бъде наложена в съответствие с естеството на въпросното нарушение.

Със съображение 148 се въвежда понятието „леки нарушения“. Те могат да представляват нарушение на една или няколко от разпоредбите на Регламента, посочени в член 83, параграфи 4 или 5. В резултат на оценката на критериите в член 83, параграф 2 обаче надзорният орган може да счете, че в конкретните обстоятелства по случая нарушението например не създава значителен риск за правата на съответните субекти на данни и не засяга същността на въпросното задължение. В такива случаи глобата или имуществената санкция може (но невинаги) да бъде заменена с порицание.

В съображение 148 не се съдържа задължение за надзорния орган винаги да заменя глоба или имуществена санкция с порицание в случай на леко нарушение („*вместо глоба може да бъде отсъдено порицание*“), а по-скоро възможност, която може да бъде използвана след извършването на конкретна оценка на всички обстоятелства по случая.

Съображение 148 осигурява същата възможност за замяна на глоба или имуществена санкция с порицание, когато администраторът е физическо лице и глобата или имуществената санкция, която може да бъде наложена, би представлявала несъразмерна тежест. Отправната точка за това е, че надзорният орган трябва да прецени дали се изисква налагането на глоба или имуществена санкция с оглед на обстоятелствата по разглеждания случай. Ако прецени, че трябва да се наложи глоба или имуществена санкция, надзорният орган трябва също така да прецени дали тя би представлявала несъразмерна тежест за дадено физическо лице.

В Регламента не се посочват конкретни суми за отделни нарушения, а само таван (максимален размер). Това може да бъде индикация за относително по-ниска степен на тежест при нарушение на задълженията, посочени в член 83, параграф 4, в сравнение с посочените в член 83, параграф 5. Ефективният, пропорционален и възпиращ отговор на нарушение на член 83, параграф 5 обаче ще зависи от обстоятелствата по случая.

Следва да се отбележи, че нарушенията на Регламента, които по своето естество могат да попадат в категорията „до 10 000 000 EUR или до 2 % от общия годишен световен оборот“, както е

7 В някои държави, поради националните процесуални правила, произтичащи от конституционни изисквания, оценката на санкцията, която следва да бъде наложена, може да се извършва отделно, след като се извърши оценка за това дали е налице нарушение. Следователно това може да ограничи съдържанието и степента на подробност на проекта на решение, което се постановява от водещия надзорен орган в тези държави.

посочено в член 83, параграф 4, при определени обстоятелства могат да бъдат причислени към по-висока категория (20 милиона евро). Такъв вероятно би бил случаят, ако тези нарушения вече са били предмет на разпореждане[8] на надзорния орган, което администраторът или обработващият лични данни не е спазил[9] (член 83, параграф 6). На практика разпоредбите на националното законодателство могат да окажат въздействие върху тази оценка[10]. Редом с естеството на нарушението, „*обхватът или целта на съответното обработване, както и броят на засегнатите субекти на данни и степента на причинената им вреда*“ също са показателни за **тежестта** на нарушението. При наличието на няколко отделни нарушения, извършени заедно в рамките на конкретен единичен случай, надзорният орган може да наложи административни наказания „глоба“ или „имуществена санкция“ на ниво, което е ефективно, пропорционално и възпиращо, като не надхвърля максималния размер за най-тежкото нарушение. Следователно ако бъде установено нарушение на членове 8 и 12, надзорният орган може да наложи корективните мерки, определени в член 83, параграф 5, които отговарят на категорията на по-тежкото нарушение, а именно на нарушението на член 12. Предоставянето на повече подробности на този етап попада извън обхвата на настоящите насоки (подробните изчисления ще бъдат разгледани на евентуален следващ етап от разработването на насоките).

Изброените по-долу фактори следва да се оценяват заедно, например броят на субектите на данни заедно с възможното въздействие върху тях.

Следва да се оцени **броят** на засегнатите субекти на данни, за да се определи дали това е изолиран случай, или показва по-системно нарушение или липса на подходящи практики. Това не означава, че изолираните случаи не следва да подлежат на действия по правоприлагане, тъй като дори един изолиран случай може да засегне множество субекти на данни. В зависимост от обстоятелствата по случая това ще зависи например от общия брой на регистрираните лица във въпросната база данни, броя на ползвателите на дадена услуга, броя на потребителите или цялото население на страната.

Също така трябва да се оцени **целта** на обработването на данни. В становището на Работната група по член 29 относно „ограничаването в рамките на целта“[11] бяха анализирани двата основни градивни елемента на този принцип в законодателството за защита на данните: конкретизиране на целта и съвместимо използване. Когато оценяват целта на обработването в контекста на член 83, параграф 2, надзорните органи следва да проучват степента, в която при обработването се спазват двата основни компонента на този принцип[12]. В определени ситуации надзорният орган може да сметне за необходимо да извърши по-задълбочен анализ на целта на обработването в рамките на анализа по член 83, параграф 2.

---

8 Предвидените разпореждания в член 58, параграф 2 са:
• да разпорежда на администратора или обработващия лични данни да изпълнят исканията на субекта на данни да упражнява правата си съгласно настоящия регламент;
• да разпорежда на администратора или обработващия лични данни да съобразят операциите по обработване на данни с разпоредбите на настоящия регламент и, ако е целесъобразно, това да стане по указан начин и в определен срок;
• да разпорежда на администратора да съобщава на субекта на данните за нарушение на сигурността на личните данни;
• да налага временно или окончателно ограничаване, в т.ч. забрана, на обработването на данни;
• да разпорежда коригирането или изтриването на лични данни, или ограничаването на обработването им съгласно членове 16, 17 и 18, както и уведомяването за тези действия на получатели, пред които личните данни са били разкрити съгласно член 17, параграф 2 и член 19;
• да разпорежда на сертифициращия орган да отнеме сертификат, издаден съгласно членове 42 и 43, или да разпорежда на сертифициращия орган да не издава сертификат, ако изискванията за сертифицирането не са спазени или вече не се спазват;
• да разпорежда преустановяването на потока на данни към получател в трета държава или към международна организация.

9 При прилагането на член 83, параграф 6 по необходимост трябва да се зачита националното процесуално право. В националното законодателство се определя как се издава разпореждане, как се прави уведомление за него, от кой момент поражда действие, дали има „гратисен период“ за предприемане на мерки за спазване на правилата. По-специално следва да бъде взет предвид ефектът от евентуалното обжалване на изпълняемостта на разпореждането.

10 В резултат на законовите разпоредби за давностни срокове е възможно предишно разпореждане на надзорния орган вече да не може да бъде взето под внимание поради периода, който е изминал от издаването на предишното разпореждане. В някои юрисдикции съществуват правила, съгласно които след като изтече давностният срок по отношение на дадено разпореждане, не може да се налага глоба или имуществена санкция съгласно член 83, параграф 6 за неспазването на това разпореждане. Всеки надзорен орган в рамките на всяка юрисдикция трябва да определи какво ще бъде отражението върху него от подобни правила.

11 WP 203, Становище 03/2013 относно ограничаването в рамките на целта, достъпно на: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion- recommendation/files/2013/wp203_en.pdf

12 Вж. също така WP 217, Становище 6/2014 относно понятието за законни интереси на администратора на лични данни съгласно член 7 от Директива 95/46/ЕО, стр. 24, във връзка с въпроса: „Какво прави един интерес законен или незаконен?“.

Ако субектите на данни претърпят **вреди**, трябва да бъде взета предвид степента на причинените им вреди. Обработването на лични данни може да породи рискове за правата и свободите на лицата, както е посочено в съображение 75:

„Рискът за правата и свободите на физическите лица, с различна вероятност и тежест, може да произтича от обработване на лични данни, което би могло да доведе до физически, материални или нематериални вреди, по-специално: когато обработването може да породи дискриминация, кражба на самоличност или измама с фалшива самоличност, финансови загуби, накърняване на репутацията, нарушаване на поверителността на лични данни, защитени от професионална тайна, неразрешено премахване на псевдонимизация, или други значителни икономически или социални неблагоприятни последствия; или когато субектите на данни могат да бъдат лишени от свои права и свободи или от упражняване на контрол върху своите лични данни; когато се обработват лични данни, които разкриват расов или етнически произход, политически възгледи, религиозни или философски убеждения, членство в професионална организация, и обработването на генетични данни, данни за здравословното състояние или данни за сексуалния живот или за присъди и нарушения или свързани с тях мерки за сигурност; когато се оценяват лични аспекти, по- специално анализиране или прогнозиране на аспекти, отнасящи се до представянето на работното място, икономическото положение, здравето, личните предпочитания или интереси, надеждността или поведението, местонахождението или движенията в пространството, с цел създаване или използване на лични профили; когато се обработват лични данни на уязвими лица, по-специално на деца; или когато обработването включва голям обем лични данни и засяга голям брой субекти на данни".

Ако в резултат на нарушението на Регламента са били претърпени вреди или е вероятно да бъдат претърпени такива, надзорният орган следва да вземе това предвид при избора си на корективна мярка, макар че самият той не е компетентен да постанови конкретно обезщетение за претърпените вреди.

Налагането на глоба или имуществена санкция не зависи от това, дали надзорният орган е в състояние да установи причинно-следствена връзка между нарушението и имуществените вреди (вж. например член 83, параграф 6).

Продължителността на нарушението може да е индикация например за:

а) умишлено поведение от страна на администратора, или

б) непредприемане на подходящи превантивни мерки, или

в) неспособност да се въведат изискваните технически и организационни мерки.

б) дали нарушението е извършено умишлено или по небрежност

По принцип „умисъл" включва съзнаване на характеристиките на нарушението и воля за извършването му, докато „неумишлено" означава, че не е било налице намерение да се извърши нарушението, но въпреки това администраторът/обработващият лични данни не е положил дължимата грижа, както се изисква по закон.

Като цяло се приема, че умишлените нарушения, при които се демонстрира явно незачитане на законовите разпоредби, са по-тежки от неумишлените нарушения и че поради това при първите е по-вероятно да е основателно налагането на административно наказание „глоба" или „имуществена санкция". Съответните заключения дали нарушението е извършено умишлено, или по небрежност се правят въз основа на данните за обективните елементи на поведението, събрани от фактите по случая. Освен това нововъзникващата съдебна практика и практиките в областта на защитата на данните във връзка с прилагането на Регламента ще покажат кои обстоятелства съставляват по-ясни прагове за оценка дали нарушението е умишлено.

Примери за обстоятелства, които са показателни за умишлени нарушения, могат да бъдат неправомерно обработване на данни, разпоредено изрично от висшето ръководство на администратора или в разрез със съветите на длъжностното лице по защита на данните, или при незачитане на съществуващи политики, например получаване и обработване на данни относно служителите на конкурентно дружество с цел дискредитирането му на пазара.

Други примери могат да бъдат:

• промяната на лични данни, за да се създаде подвеждащо (положително) впечатление, че дадени цели са постигнати – свидетели сме на това в контекста на целите за времето на изчакване в болница;

• търговията с лични данни за маркетингови цели, т.е. продажбата на данните като данни, за които е дадено разрешение за обработване от субектите на данни, като не се проверява или се пренебрегва тяхното мнение за това как следва да бъдат използвани техните данни.

Други обстоятелства, като например непознаване и неспазване на съществуващите политики, човешка грешка, липса на проверка дали в публикуваната информация има лични данни, липса на своевременно инсталиране на технически актуализации, неприемане на политики (а не просто неприлагането им), могат да са индикация за небрежност.

Предприятията следва да отговарят за осигуряването на адекватни структури и ресурси в зависимост от естеството и сложността на своята дейност. Администраторите и обработващите лични данни не могат да оправдават нарушенията на законодателството в областта на защитата на данните с недостиг на ресурси. Рутинните практики и документирането на дейностите по обработване следват основан на риска подход в съответствие с Регламента.

Съществуват „сиви зони“, които ще оказват влияние върху вземането на решения дали да се наложи корективна мярка или не, и може да се наложи органът да проведе по-обстойно разследване, за да определи фактите по случая и да гарантира, че всички специфични обстоятелства по конкретния случай са взети предвид в достатъчна степен.

в) действията, предприети от администратора или обработващия лични данни за смекчаване на последиците от вредите, претърпени от субектите на данни

Администраторите и обработващите лични данни са задължени да прилагат технически и организационни мерки за осигуряване на съобразено с риска ниво на сигурност, да извършват оценки на въздействието върху защитата на личните данни и да ограничат произтичащите от обработването на лични данни рискове за правата и свободите на физическите лица. Когато обаче бъде извършено нарушение и субектът на данни претърпи вреди, отговорната страна трябва да направи всичко възможно, за да ограничи последиците от нарушението за засегнатото лице или лица. Такова отговорно поведение (или липсата му) би трябвало да бъде взето предвид от надзорния орган при избора на корективна мярка или мерки, както и при определянето на размера на санкцията, която да бъде наложена в конкретния случай.

Въпреки че утежняващите или смекчаващите фактори са особено подходящи за адаптиране на размера на глобата или имуществената санкция с оглед на конкретните обстоятелства по случая, тяхната роля при избора на подходяща корективна мярка не следва да се подценява. В случаите, когато оценката въз основа на други критерии не позволява на надзорния орган категорично да заключи, че е уместно да се наложи административното наказание „глоба“ или „имуществена санкция“ като самостоятелна корективна мярка или в съчетание с други мерки по член 58, такива утежняващи или смекчаващи обстоятелства могат да помогнат при избора на подходящи мерки, като наклонят везните към мерките, които са по-ефективни, пропорционални и възпиращи в дадения случай.

Тази разпоредба функционира като оценка на степента на отговорност на администратора след извършването на нарушението. Тя може да обхване случаи, в които администраторът/обработващият

лични данни очевидно не е походил необмислено/небрежно, и е направил всичко възможно да коригира своите действия, когато е разбрал за нарушението.

Регулаторният опит на надзорните органи във връзка с Директива 95/46/ЕО вече показа, че може да бъде уместно да се действа с известна степен на гъвкавост спрямо администраторите/обработващите лични данни, които са признали своите нарушения и са поели отговорност да коригират или ограничат въздействието от своите действия. Това може да включва (макар да не би довело до по-гъвкав подход във всеки отделен случай) примери като:

• осъществяване на контакт с други администратори/обработващи лични данни, които може да са участвали в допълнително обработване на данните, например ако част от данните погрешно са били споделени с трети страни.

• своевременни действия, предприети от администратора/обработващия лични данни, с цел да не се позволи нарушението да продължи или да се разрасне до степен или етап, на който би имало много по-сериозно въздействие.

г) степента на отговорност на администратора или обработващия лични данни, като се вземат предвид технически и организационни мерки, въведени от тях в съответствие с членове 25 и 32

С Регламента се въвежда много по-високо ниво на отчетност на администратора в сравнение с Директива 95/46/ЕО за защита на личните данни.

Оценката на степента на отговорност на администратора или обработващия лични данни в контекста на прилагането на подходящи корективни мерки може да включва следните въпроси:

• Въвел ли е администраторът технически мерки, които следват принципите за защита на данните на етапа на проектирането или по подразбиране (член 25)?

• Въвел ли е администраторът организационни мерки, с които се прилагат принципите за защита на данните на етапа на проектирането и по подразбиране (член 25) на всички равнища в организацията?

• Въвел ли е администраторът/обработващият лични данни подходящо ниво на сигурност (член 32)?

• Известни ли са съответните рутинни практики/политики за защита на данните и прилагат ли се на подходящото управленско равнище в рамките на организацията (член 24)?

Съгласно членове 25 и 32 от Регламента се изисква администраторите да вземат 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*“. С тези разпоредби не се налага задължение по отношение на целта, а задължения по отношение на средствата, т.е. администраторът трябва да извърши необходимите оценки и да достигне до подходящи заключения. Въпросът, на който след това трябва да отговори надзорният орган, е до каква степен администраторът е „отговорил на очакванията“ предвид естеството, целите или обема на обработването с оглед на наложените му задължения съгласно Регламента.

При тази оценка следва надлежно да се вземат предвид всички процедури или методи, представляващи „най-добри практики“, когато такива съществуват и се прилагат. Важно е да се вземат предвид стандартите в съответния отрасъл, както и кодексите за поведение в съответната област или професия. Професионалните кодекси могат да дадат индикация за това какво се счита за обичайна практика в областта и какво е нивото на знанията относно различните средства за справяне с типични проблеми, свързани със сигурността при обработването на данни.

Макар че в идеалния случай по принцип следва да се прилагат най-добрите практики, при оценката на степента на отговорност по всеки конкретен случай трябва да се вземат предвид специфичните обстоятелства.

д) евентуални свързани предишни нарушения, извършени от администратора или обработващия лични данни

Целта на този критерий е да се оценят досегашните резултати на образуването, извършило нарушението. Надзорните органи следва да вземат предвид, че обхватът на оценката по тази точка може да бъде изключително широк, защото всеки вид нарушение на Регламента, макар и с различно естество в сравнение с понастоящем разследваното от надзорния орган нарушение, може да бъде „свързано“ за целите на оценката, тъй като може да показва общо ниво на недостатъчни знания или незачитане на правилата за защита на данните.

Надзорният орган следва да направи оценка за следното:

• Извършвал ли е администраторът/обработващият лични данни същото нарушение и преди?

• Извършвал ли е администраторът/обработващият лични данни нарушение на Регламента по същия начин? (например вследствие на недостатъчни знания за съществуващите рутинни практики в организацията или вследствие на неподходяща оценка на риска, липса на своевременен отговор на искания от субекта на данни, необосновано забавяне при отговора на искания и др.).

е) степента на сътрудничество с надзорния орган с цел отстраняване на нарушението и смекчаване на евентуалните неблагоприятни последици от него

В член 83, параграф 2 се предвижда степента на сътрудничество да може да се разглежда „надлежно“, когато се взема решение дали да бъде наложено административно наказание „глоба“ или „имуществена санкция“ и се определя нейният размер. Регламентът не съдържа точен отговор на въпроса по какъв начин да се вземат предвид усилията на администраторите или обработващите лични данни за отстраняване на вече установено от надзорния орган нарушение. Освен това е ясно, че критериите биха се прилагали обикновено при определянето на размера на глобата или имуществената санкция, която ще бъде наложена.

Когато обаче в резултат на намесата на администратора отрицателните последици по отношение на правата на лицата не са се проявили или са имали по-ограничено въздействие, отколкото биха могли да имат без тази намеса, това също би могло да се вземе предвид при избора на коригирана мярка, която е пропорционална в конкретния случай.

Следният въпрос представлява пример за случай, при който евентуално би било уместно да се отчете сътрудничеството с надзорния орган:

• Реагирало ли е образуването по определен начин на исканията на надзорния орган на етапа на разследване на конкретния случай, в резултат на което въздействието върху правата на лицата е било ограничено значително?

Следва да се отбележи обаче, че не би било уместно да се придава допълнителна тежест на сътрудничество, което се изисква по закон, например образуването при всички случаи е задължено да осигури достъп на надзорния орган до помещенията с цел одит/проверка.

ж) категориите лични данни, засегнати от нарушението

По-долу са дадени някои примери за ключови въпроси, на които надзорният орган може да счете за необходимо да отговори в тази връзка, според случая:

• Свързано ли е нарушението с обработване на специални категории данни по членове 9 или 10 от Регламента?

• Могат ли данните да бъдат идентифицирани пряко или непряко?

• Обработването включва ли данни, разпространението на които би довело до непосредствени вреди/затруднения за лицето (и които попадат извън обхвата на категориите по членове 9 или 10)?

• Достъпни ли са данните пряко, без да е налице техническа защита, или са криптирани[13]?

з) начина, по който нарушението е станало известно на надзорния орган, по-специално дали и до каква степен администраторът или обработващият лични данни е уведомил за нарушението

Надзорният орган може да разбере за нарушението в резултат на разследване, жалба, статия в пресата, анонимен сигнал или уведомление от администратора. Съгласно Регламента администраторът е задължен да уведоми надзорния орган за нарушения на сигурността на личните данни. Когато администраторът просто изпълнява това задължение, спазването му не може да се тълкува като смекчаващ фактор. По подобен начин надзорният орган може да счете, че администратор/обработващ лични данни, който е действал небрежно, без да уведоми за нарушението, или поне без да уведоми за всички подробности по него, поради неадекватна оценка на степента на нарушението, също заслужава по-сериозна санкция, т.е. това вероятно няма да бъде категоризирано като леко нарушение.

и) когато на засегнатия администратор или обработващ лични данни преди са налагани мерки, посочени в член 58, параграф 2, във връзка със същия предмет на обработването, дали посочените мерки са спазени

Даден администратор или обработващ лични данни може вече да бъде в полезрението на надзорния орган с цел проследяване дали са спазени мерките, след като е било извършено предишно нарушение. В такива случаи контактите с длъжностното лице по защита на данните, ако има такова, вероятно са били интензивни. Следователно надзорният орган ще вземе предвид предишните контакти.

За разлика от критерия по буква д), този критерий за оценка цели единствено да напомни на надзорните органи да вземат предвид мерките, които самите те са постановили по-рано за същия администратор или обработващ лични данни „във връзка със същия предмет на обработването“.

й) придържането към одобрени кодекси на поведение съгласно член 40 или одобрени механизми за сертифициране съгласно член 42

Всеки надзорен орган има задължението да „наблюдава и осигурява прилагането на настоящия регламент“ (член 57, параграф 1, буква а). Администраторът или обработващият лични данни може да използва придържането към одобрени кодекси на поведение като начин да демонстрира спазването на изискванията в съответствие с член 24, параграф 3, член 28, параграф 5 или член 32, параграф 3.

Ако бъде нарушена разпоредба на Регламента, придържането към одобрен кодекс на поведение може да е индикация за степента на необходимостта от намеса от страна на надзорния орган посредством ефективно, пропорционално, възпиращо административно наказание „глоба“ или „имуществена санкция“ или друга корективна мярка. Съгласно член 40, параграф 4 одобреният кодекс на поведение съдържа „*механизми, които позволяват на надзорния орган да извършва задължителното наблюдение на спазването на неговите разпоредби*“.

Когато администраторът или обработващият лични данни се е придържал към одобрен кодекс на поведение, надзорният орган може да се увери, че самата общност, която отговаря за прилагането на този кодекс, предприема подходящи действия срещу своя член, например чрез схеми за наблюдение и изпълнение на въпросния кодекс на поведение. Следователно надзорният орган може да счете, че тези мерки са достатъчно ефективни, пропорционални или възпиращи в конкретния случай и че не е необходимо да се налагат допълнителни мерки от самия надзорен орган. В съответствие с член 41,

13 Фактът, че нарушението засяга единствено данни, позволяващи само непряко идентифициране, или дори псевдонимизирани/криптирани данни, невинаги следва да се счита за допълнителен смекчаващ фактор. За такива нарушения общата оценка на другите критерии може да сочи, в умерена или силна степен, че следва да бъде наложена глоба или имуществена санкция.

параграф 2, буква в) и член 42, параграф 4 чрез схемата за наблюдение могат да се наложат определени мерки за санкциониране на неспазването, включително суспендиране на членството в общността, за която се прилага кодексът, или изключване от нея на съответния администратор или обработващ лични данни. Независимо от това правомощията на органа за наблюдение не засягат „*задачите и правомощията на компетентния надзорен орган*“, което означава, че надзорният орган не е задължен да вземе предвид наложените преди това санкции по схемата за саморегулиране.

Неспазването на мерките за саморегулиране също така би могло да разкрие небрежност или умишлено неспазване от страна на администратора/обработващия лични данни.

к) всякакви други утежняващи или смекчаващи фактори, приложими към обстоятелствата по случая, като пряко или косвено реализирани финансови ползи или избегнати загуби вследствие на нарушението

Самата разпоредба съдържа примери за това какви други елементи могат да бъдат взети предвид, когато се определя дали административното наказание „глоба“ или „имуществена санкция“ е подходящо във връзка с нарушение на разпоредбите, посочени в член 83, параграфи 4−6.

Информацията относно реализираните печалби в резултат на нарушението може да бъде особено важна за надзорните органи, тъй като икономическата печалба от нарушението не може да се неутрализира чрез мерки, които нямат паричен компонент. Сам по себе си фактът, че администраторът е извлякъл изгода от нарушението на Регламента, може да е сериозна индикация, че следва да бъде наложена глоба или имуществена санкция.

IV. Заключение

Обмислянето на въпроси като посочените в предния раздел ще помогне на надзорните органи да определят въз основа на съответните факти по случая кои критерии са най-полезни, когато се взема решение дали да се наложи подходящо административно наказание „глоба“ или „имуществена санкция“ в допълнение към други мерки по член 58 или вместо тях. Като вземе предвид контекста, предоставен чрез тази оценка, надзорният орган ще определи най- ефективната, пропорционална и възпираща корективна мярка в отговор на нарушението.

В член 58 се предвиждат някои насоки относно мерките, които надзорният орган може да избере, тъй като самите корективни мерки са различни по своето естество и са подходящи за постигането на различни цели. Някои от мерките по член 58 дори могат да се съчетават, като така се постига регулаторно действие, състоящо се от повече от една корективна мярка.

Невинаги е необходимо съответната мярка да се допълва като се използва друга корективна мярка. Така например ефективността и възпиращият ефект на намесата на надзорния орган, като се отдаде необходимото внимание на това, какви мерки са пропорционални в конкретния случай, могат да бъдат постигнати чрез налагането само на глоба или имуществена санкция.

По същество органите трябва да възстановяват спазването чрез всички корективни мерки, които са на тяхно разположение. Надзорните органи също така са задължени да изберат най- подходящия канал за осъществяването на регулаторни действия. Това би могло да включва например наказателни санкции (когато съществуват на национално равнище).

Практиката на съгласувано налагане на административни наказания „глоба“ или „имуществена санкция“ в рамките на Европейския съюз постепенно се развива. Надзорните органи следва да работят заедно, когато предприемат действия, така че съгласуваността постоянно да се подобрява. Това може да се постигне чрез редовен обмен на информация чрез работни срещи за разглеждане на случаи или други мероприятия, които позволяват сравнение на случаи на поднационално, национално и трансгранично равнище. За да бъде подпомогната текущата дейност, се препоръчва към съответното подразделение на ЕКЗД да бъде създадена постоянна подгрупа.

НАСОКИ ЗА ОПРЕДЕЛЯНЕ НА ВОДЕЩ НАДЗОРЕН ОРГАН НА АДМИНИСТРАТОР ИЛИ ОБРАБОТВАЩ ЛИЧНИ ДАННИ

1. Определяне на водещ надзорен орган: основни понятия

1.1. „Трансгранично обработване на лични данни“

Водещ надзорен орган се определя само когато администратор или обработващ лични данни извършва трансгранично обработване на лични данни. В член 4, параграф 23 от Общия регламент относно защитата на данните (ОРЗД) „трансгранично обработване“ се определя или като:

- *обработване на лични данни, което се осъществява в контекста на дейностите на местата на установяване в повече от една държава членка на администратор или обработващ лични данни в Съюза, като администраторът или обработващият лични данни е установен в повече от една държава членка; или*

- *обработване на лични данни, което се осъществява в контекста на дейностите на едно-единствено място на установяване на администратор или обработващ лични данни в Съюза, но което засяга съществено или е вероятно да засегне съществено субекти на данни в повече от една държава членка.*

Това означава, че ако дадена организация има места на установяване във Франция и Румъния например и обработването на лични данни се извършва в контекста на техните дейности, тогава това ще представлява трансгранично обработване.

Алтернативно организацията може да осъществява дейности по обработване само в контекста на своето място на установяване във Франция. Ако обаче дейността засяга съществено или е вероятно да засегне съществено субекти на данните във Франция и Румъния, тогава тя също представлява трансгранично обработване.

1.1.1. „Засяга съществено“

В ОРЗД не е дадено определение нито на „съществено“, нито на „засяга“. С тази формулировка се цели да се гарантира, че не всяка дейност по обработване с *какъвто и да било* ефект и извършвана в контекста на едно-единствено място на установяване попада в обхвата на определението на „трансгранично обработване“.

Най-важните обичайни значения на английската дума „substantial“ („съществен“) включват: „с голям или значителен обем или размер; порядъчно голям, относително едър“, както и „със сериозна ценност или стойност, с реално значение; солиден; тежък, важен“ (Oxford English Dictionary).

Най-важното обичайно значение на глагола „засягам“ е „влияя“ или „причинявам съществено въздействие върху“. Производното съществително – „засягане“ – означава, наред с други неща, „резултат“ или „последица“ (Oxford English Dictionary). Това означава, че да *засегне* някого обработването на данни, означава да има някаква форма на въздействие върху него. Обработването, което не засяга съществено физическите лица, не попада в обхвата на втората част от определението на „трансгранично обработване“. То обаче би попаднало в първата част на определението, ако обработването на лични данни се осъществява в контекста на дейностите на местата на установяване на администратора или обработващия лични данни в повече от една държава членка в Съюза, когато администраторът или обработващият лични данни е установен в повече от една държава членка.

Обработването може да бъде включено във втората част на определението, ако има вероятност за съществено засягане, а не само при реално съществено засягане. Следва да се има предвид, че „е вероятно да“ не означава, че има малка вероятност за съществено засягане. Същественото засягане трябва да е по-скоро вероятно, отколкото не. От друга страна, това означава също така, че не е задължително физическите лица реално да са засегнати: вероятността за съществено засягане

е достатъчна, за да се включи обработването в рамките на определението за „трансгранично обработване“.

Фактът, че операция по обработване на данни може да включва обработване на личните данни на доста, дори на голям брой, физически лица в няколко държави членки, не означава задължително, че обработването ги е засегнало съществено или е вероятно да ги засегне съществено. Обработването, което не засяга съществено субекти на данни, не представлява трансгранично обработване за целите на втората част на определението, независимо колко физически лица засяга.

Надзорните органи ще тълкуват „засегне съществено“ на база конкретен случай. Ние ще вземем предвид контекста на обработването, типа на данните, целта на обработването и фактори като например дали обработването:

- причинява или е вероятно да причини щети, загуба или страдание на физически лица;
- има или е вероятно да има въздействие от гледна точка на ограничаване на права или лишаване от възможност;
- засяга или е вероятно да засегне здравето, благосъстоянието или спокойствието на физически лица;
- засяга или е вероятно да засегне финансовото или икономическото състояние или материалното положение на физически лица;
- излага физически лица на дискриминация или несправедливо третиране;
- включва анализирането на специални категории лични или други предполагащи вмешателство данни, особено личните данни на деца;
- кара или е вероятно да накара физическите лица значително да променят своето поведение;
- има необичайни, неочаквани или нежелани последици за физически лица;
- причинява неудобство или други отрицателни резултати, в това число увреждане на репутацията; или
- включва обработването на широк диапазон от лични данни.

В крайна сметка, с теста, свързан със „засяга съществено“, се цели да се гарантира, че надзорните органи са длъжни да си сътрудничат официално чрез предвидения в ОРЗД механизъм за съгласуваност, само *„когато даден надзорен орган възнамерява да приеме мярка, целяща да породи правни последици по отношение на операции по обработване на данни, които засягат съществено значителен брой субекти на данни в няколко държави членки“. (съображение 135)*

1.2. Водещ надзорен орган

Казано по-просто, „водещият надзорен орган“ е органът, който носи основната отговорност по отношение на дейност, включваща трансгранично обработване, например когато субект на данни подава жалба във връзка с обработването на неговите лични данни.

Водещият надзорен орган ще координира всяко разследване, в което са включени други „засегнати“ надзорни органи.

Определянето на водещ надзорен орган зависи от определянето на местоположението на „основното място на установяване“ или „единственото място на установяване“ в ЕС на администратора. В член 56 от ОРЗД се казва, че:

- *„надзорният орган на основното място на установяване или на единственото място на установяване на администратора или обработващия лични данни е компетентен да действа като водещ надзорен орган за трансграничното обработване, извършвано от посочения администратор или обработващ лични данни в съответствие с процедурата по член 60“.*

1.3. Основно място на установяване

В член 4, параграф 16 от ОРЗД се казва, че „основно място на установяване“ означава:

- по отношение на администратор, установен в повече от една държава членка – мястото, където се намира ***централното му управление*** *в Съюза, освен в случаите, когато* ***решенията по отношение на целите и средствата*** *за обработването на лични данни се вземат на друго място на установяване на администратора в Съюза и на това място на установяване има* ***правомощия за прилагане на тези решения,*** *в който случай мястото на установяване, където са взети тези решения, се счита за основно място на установяване;*

- по отношение на обработващ лични данни, установен в повече от една държава членка – мястото, където се намира централното му управление в Съюза, или ако обработващият лични данни няма централно управление в Съюза, мястото на установяване на обработващия лични данни в Съюза, където се осъществяват основните дейности по обработването в контекста на дейностите на дадено място на установяване на обработващия лични данни, доколкото обработващият има специфични задължения съгласно настоящия регламент.

2. Стъпки за определяне на водещ надзорен орган

2.1. Определяне на „основно място на установяване“ на администратори

За да се определи къде се намира основното място на установяване, преди всичко е необходимо да се идентифицира централното управление на администратора на данни в ЕС, ако има такова[1]. Предвиденият в ОРЗД подход се състои в това, че централното управление в ЕС е мястото, където се вземат решенията по отношение на целите и средствата на обработването на лични данни, и съответното място има правомощия за прилагането на тези решения.

По същество принципът за водещ орган в рамките на ОРЗД се състои в това, че надзорът върху трансграничното обработване следва да се води само от един надзорен орган в ЕС. В случаи, когато решения, свързани с различни дейности по трансгранично обработване, се вземат в централното управление в ЕС, водещият надзорен орган ще бъде един за различни дейности по обработване на данни, които се извършват от мултинационалното дружество. Може да има случаи обаче, когато на дадено място на установяване, различно от мястото на централното управление, се вземат независими решения по отношение на целите и средствата на конкретна дейност по обработване. Това означава, че може да има ситуации, когато може да бъде определен повече от един водещ орган, т.е. случаи, в които дадено мултинационално дружество реши да поддържа отделни центрове за вземане на решения в различни държави за различни дейности по обработване.

Струва си да се напомни, че когато едно мултинационално дружество централизира всички решения, свързани с целите и средствата на дейностите по обработване, в едно от своите места на установяване в ЕС (и това място на установяване има правомощия да прилага въпросните решения), за мултинационалното дружество ще бъде определен само един водещ надзорен орган.

В тези ситуации ще е съществено важно дружествата много точно да определят къде се вземат решенията по отношение на целта и средствата на обработването. Правилното определяне на основното място на установяване е в интерес на администраторите и обработващите лични данни, защото така се осигурява яснота от гледна точка на това с кой надзорен орган те трябва да работят по отношение на разнообразните си задължения за спазване съгласно ОРЗД. Тези задължения за спазване може да включват, по целесъобразност, определянето на длъжностно лице по защита на данните или консултиране във връзка с рискова дейност по обработването, когато администраторът не може да намали риска с разумни средства. Със съответните разпоредби на ОРЗД се цели тези задачи по спазването да са изпълними.

1 ОРЗД е от значение за ЕИП и ще се прилага, след като бъде включен в Споразумението за ЕИП. Понастоящем ОРЗД е в процес на преглед с оглед на включването му, вж. http://www.efta.int/eea-lex/32016R0679.

Примерите по-долу показват това:

Пример 1: Седалището на търговец на дребно на храни (т.е. неговото „място на централно управление“) се намира в Ротердам, Нидерландия. Той има места на установяване в редица други държави от ЕС, които осъществяват контакти с физически лица. Всички места на установяване използват един и същ софтуер за обработването на личните данни на потребителите с маркетингови цели. Всички решения по отношение на целите и средствата на обработването на личните данни на потребителите с маркетингови цели се вземат в неговото седалище в Ротердам. Това означава, че водещият надзорен орган на дружеството за тази трансгранична дейност по обработване е нидерландският надзорен орган.

Пример 2: Корпоративното седалище на дадена банка се намира във Франкфурт и всички[2] нейни банкови дейности по обработване се организират от там, но застрахователният и отдел се намира във Виена. Ако мястото на установяване във Виена има правомощия за вземане на решения по отношение на всички дейности по обработване на застрахователните данни и да прилага тези решения за целия ЕС, тогава, както е предвидено в член 4, параграф 16 от ОРЗД, австрийският надзорен орган би бил водещият орган по отношение на трансграничното обработване на лични данни със застрахователни цели, а германските органи (надзорен орган на Хесен) биха осъществявали надзор върху обработването на лични данни с банкови цели, независимо къде се намират клиентите[3].

2.1.1. Критерии за определяне на основното място на установяване на администратор в случаи, когато то не съвпада с мястото на централното му управление в ЕС

Съображение 36 от ОРЗД е от полза за пояснияване на основния фактор, който следва да се използва за определяне на основното място на установяване на администратора, ако критерият за централното управление не е приложим. Това означава да бъде определено къде действително и реално се осъществяват дейностите по управление, определящи основните решения по отношение на целите и средствата на обработването на базата на сериозни договорености. В съображение 36 е пояснено, че „наличието и употребата на технически средства и технологии за обработване на лични данни или дейностите по обработване не представляват сами по себе си основно място на установяване и следователно не са определящи критерии за понятието „основно място на установяване“.

Администраторът на данни сам определя къде се намира неговото основно място на установяване и съответно кой надзорен орган е неговият водещ орган. Това обаче в последствие може да бъде оспорено от съответния засегнат надзорен орган.

Посочените по-долу фактори са от полза за определяне на местоположението на основното място на установяване на администратора в съответствие с условията по ОРЗД в случаи, когато то не съвпада с мястото на централното му управление в ЕС.

- Къде се извършва окончателното „одобряване и подписване“ на решенията относно целите и средствата на обработването?
- Къде се вземат решенията относно стопанските дейности, включващи обработване на данни?
- Къде практически са съсредоточени правомощията за прилагане на решенията?
- Къде се помещава директорът (или директорите), носещ отговорност за цялостното управление на трансграничното обработване?
- Къде е регистриран администраторът или обработващият лични данни като дружество, ако става дума за една територия?

2 Ние отчитаме, че в контекста на обработването на лични данни с банкови цели има много различни дейности по обработване. С оглед на опростяването обаче ние ги разглеждаме като една цел. Същото важи за обработването със застрахователни цели.

3 Следва да се напомни също така, че в ОРЗД е предвидена възможността за наблюдение на местно равнище в специални случаи. Вж. съображение 127. „*Всеки надзорен орган, който* ***не функционира като водещ*** *надзорен орган,* ***следва да бъде компетентен да разглежда случаи на местно равнище****, когато администраторът или обработващият лични данни е установен в повече от една държава членка, но предметът на конкретното обработване засяга* ***единствено обработването, извършвано в една държава членка, и включва единствено субекти на данни в тази единствена държава членка,*** *например когато предметът се отнася до обработването на лични данни на наети лица в контекста на специфично трудово правоотношение в държава членка.*“ Според този принцип надзорът върху данните за човешките ресурси, свързани с трудовата заетост на местно равнище, би могъл да попада в компетентността на няколко надзорни органа.

Следва да се има предвид, че това не е изчерпателен списък. Може да има и други релевантни фактори, зависещи от администратора или съответната дейност по обработване. Ако даден надзорен орган има основания за съмнение, че определеното от администратора място на установяване действително е основното място на установяване за целите на ОРЗД, той, разбира се, може да изиска от администратора да представи необходимата допълнителна информация, за да докаже къде се намира неговото основно място на установяване.

2.1.2. Групи предприятия

Когато обработването се осъществява от група предприятия, чието седалище се намира в ЕС, мястото на установяване на предприятието, което упражнява пълния контрол, се приема за център на вземане на решения по отношение на обработването на лични данни и съответно ще се счита за основното място на установяване на групата, освен когато решенията по отношение на целите и средствата на обработването се вземат на друго място на установяване. Най-често дружеството майка или оперативното седалище на групата предприятия в ЕС е вероятно да бъде основното място на установяване, защото то би било мястото на нейното централно управление.

Това, че в определението е включено мястото на централно управление на администратора, е подходящо за организациите със седалища с централизирана процедура на вземане на решения и структура с клонове. В такива случаи е ясно, че седалищата на дружествата упражняват правомощията за вземане на решения относно трансграничното обработване на данни и за изпълнението им. В такива случаи определянето на местоположението на основното място на установяване и съответно кой надзорен орган е водещият надзорен орган е ясно и не създава затруднения. Все пак системата на вземане на решения в група от дружества може да е по-сложна и да включва предоставянето на правомощия за вземане на самостоятелни решения по отношение на трансграничното обработване на различни места на установяване. Посочените по-горе критерии следва да са в помощ на групите предприятия при определяне на тяхното основно място на установяване.

2.1.3. Съвместни администратори на данни

В ОРЗД не е специално разгледан въпросът с определянето на водещ орган, когато двама или повече администратори, установени в ЕС, съвместно определят целите и средствата на обработването − т.е. съвместни администратори. В член 26, параграф 1 и съображение 79 ясно е посочено, че в случаите със съвместни администратори те определят по прозрачен начин съответните си отговорности за изпълнение на задълженията по Регламента. Следователно, за да се възползват от принципа за „обслужване на едно гише“, съвместните администратори следва да определят (измежду местата на установяване, на които се вземат решения), кои места на установяване на съвместните администратори ще имат правомощията да прилагат решенията по отношение на обработването, що се касае до всички съвместни администратори. Тогава въпросното място на установяване ще се счита за основно място на установяване за целите на обработването, осъществявано от съвместните администратори. Договореностите между съвместните администратори не засягат правилата относно отговорността, предвидени по ОРЗД, и по-специално с член 82, параграф 4.

2.2. Гранични случаи

Ще има също така гранични случаи и сложни ситуации, в които е трудно да се определи основното място на установяване или да се прецени къде се вземат решенията относно обработването на данните. Такъв може да е случаят, когато е налице дейност по трансгранично обработване и администраторът е установен в няколко държави членки, но няма централно управление в ЕС и нито едно от местата на установяване в ЕС не взема решения по отношение на обработването (т.е. решенията се вземат изцяло извън ЕС).

В горния случай дружеството, което извършва трансгранично обработване, може да е заинтересовано да бъде регулирано от даден водещ орган, за да се възползва от принципа за

„обслужване на едно гише“. ОРЗД обаче не предлага решение за подобни ситуации. При тези обстоятелства дружеството трябва да определи като свое основно място на установяване мястото на установяване, което има правомощията да прилага решенията по отношение на дейността по обработване и което да носи отговорността за обработването, в това число да притежава достатъчно активи. Ако дружеството не определи основно място на установяване по този начин, тогава няма да е възможно да определи водещ орган. Надзорните органи винаги ще имат възможност да разследват допълнително дали това е целесъобразно.

Според ОРЗД не се разрешава „търсене на най-благоприятната правна система“. Ако дружество обяви, че основното му място на установяване се намира в една държава членка, но дейност по управление или вземане на решения по отношение на обработването на лични данни не се осъществява ефективно и реално там, съответните надзорни органи (или в крайна сметка Европейският комитет по защита на данните − ЕКЗД) ще решат кой е „водещият“ надзорен орган въз основа на обективни критерии и преглед на доказателствата. В процеса по определяне къде се намира основното място на установяване може да се наложи активен обмен на информация и сътрудничество между надзорните органи. Заключенията не може да се базират единствено на декларации от страна на разглежданата организация. Тежестта на доказване в крайна сметка се носи от администраторите и обработващите лични данни, които следва да докажат пред съответните надзорни органи къде се вземат съответните решения по отношение на обработването и къде са налични правомощията за прилагането на тези решения. Реалните регистри относно дейността по обработване на данни биха помогнали както на организациите, така и на надзорните органи при определянето на водещия орган. Водещият надзорен орган или засегнатите органи могат да отхвърлят направения от администратора анализ въз основа на обективен преглед на съответните факти, като поискат допълнителна информация, ако е необходимо.

В някои случаи съответните надзорни органи ще искат от администратора да предостави ясни доказателства в съответствие с насоките на ЕКЗД относно това къде се намира основното му място на установяване или къде се вземат решенията относно конкретна дейност по обработване на данни. На тези доказателства ще бъде обърнато необходимото внимание и съответните надзорни органи ще си сътрудничат, за да решат кой от тях ще бъде водещ в разследванията. Такива случаи ще се отнасят само към ЕКЗД за решение по член 65, параграф 1, буква б), когато надзорните органи имат противоречиви виждания по отношение на определянето на водещ надзорен орган. В повечето случаи обаче очакваме съответните надзорни органи да успяват да съгласуват помежду си взаимно приемлив курс на действие.

2.3. Обработващ лични данни

Според ОРЗД механизмът „обслужване на едно гише“ се предлага също в помощ на обработващите лични данни, които попадат под действието на ОРЗД и имат места на установяване в повече от една държава членка.

В член 4, параграф 16, буква б) от ОРЗД се казва, че основното място на установяване на обработващия лични данни ще бъде мястото на централното му управление в ЕС или, ако няма централно управление в ЕС, мястото на установяване в ЕС, където се осъществяват основните дейности по обработване (на обработващия лични данни).

Според съображение 36 обаче в случаи, включващи както администратор, така и обработващ лични данни, компетентният водещ надзорен орган следва да бъде водещият надзорен орган на администратора. В такава ситуация надзорният орган на обработващия лични данни ще бъде „засегнат надзорен орган“ и следва да участва в процедурата за сътрудничество. Това правило ще се прилага само когато администраторът е установен в ЕС. В случаите, когато администраторите попадат в обхвата на ОРЗД въз основа на член 3, параграф 2, за тях няма да се прилага механизмът „обслужване на едно гише“. Един обработващ лични данни може да предоставя услуги на множество администратори, които се намират в различни държави членки − например голям доставчик на облачни услуги.

В такива случаи водещ надзорен орган ще бъде надзорният орган, който е компетентен да бъде водещ за администратора. Всъщност това означава, че на един обработващ лични данни може да се наложи да работи с много надзорни органи.

3. Други съответни въпроси

3.1. Ролята на „засегнат надзорен орган“

В член 4, параграф 22 от ОРЗД се казва, че:

„засегнат надзорен орган“ означава надзорен орган, който е засегнат от обработването на лични данни, тъй като: а) администраторът или обработващият лични данни е установен на територията на държавата членка на този надзорен орган; б) субектите на данни с местопребиваване в държавата членка на този надзорен орган са засегнати съществено или е вероятно да бъдат засегнати съществено от обработването; или в) до този надзорен орган е подадена жалба.

Понятието засегнат надзорен орган е предвидено да гарантира, че моделът с „водещ орган“ няма да пречи на други надзорни органи да изразяват становището си относно това как следва да се реши въпросът, когато например физически лица с местопребиваване извън територията на компетентност на водещия орган, са засегнати съществено от дейността по обработване на данни. Що се отнася до фактора в буква а) по-горе, приложими са същите съображения, както за определяне на водещия орган. Следва да се има предвид, че в случая на буква б) субектът на данните само трябва да пребивава във въпросната държава членка; не е задължително да е гражданин на тази държава. При буква в) по принцип ще е лесно да се определи фактически дали даден надзорен орган е получил жалба.

В член 56, параграфи 2 и 5 от ОРЗД е предвидено засегнатият надзорен орган да участва в разглеждането на случая, без да е водещ надзорен орган. Когато водещ надзорен орган реши да не разглежда даден случай, засегнатият надзорен орган, който е уведомил водещия, следва да го разгледа. Това съответства на процедурите по член 61 (Взаимопомощ) и член 62 (Съвместни операции на надзорни органи) от ОРЗД. Случаят може да е такъв, когато маркетингово дружество с основно място на установяване в Париж пуска продукт, който засяга само субекти на данните, живущи в Португалия. В такъв случай френските и португалските надзорни органи може да се разберат, че е подходящо португалският надзорен орган да бъде водещ при решаването на въпроса. Надзорните органи може да поискат администраторите на данни да представят информация, за да разяснят корпоративните договорености между тях. Като се има предвид, че дейността по обработване има отражение само на местно равнище, т.е. върху физически лица в Португалия, в съответствие със съображение 127 френските и португалските надзорни органи имат правото да решат кой надзорен орган да разгледа въпроса.

Според ОРЗД се изисква водещите и засегнатите надзорни органи да си сътрудничат, като обръщат дължимото внимание на становищата си, за да се гарантира, че въпросът ще се разследва и реши по задоволителен и за двете страни начин и че ще бъде намерено ефективно решение за субектите на данни. Надзорните органи следва да правят опити за постигането на взаимно приемлив курс на действие. Към официалния механизъм за съгласуваност следва да се прибягва само когато сътрудничеството не даде взаимно приемлив резултат.

Взаимното приемане на решенията може да се прилага за материално-правните заключения, но също така за възприетия курс на действие, в това число дейностите по прилагане (например пълно разследване или разследване с ограничен обхват). То може да се прилага и за решение даден случай да не се разглежда в съответствие с ОРЗД, например поради официална политика на приоритизиране или защото има други засегнати органи, както е описано по-горе.

Консенсусът и добрата воля на надзорните органи са от съществена важност, за да се постигне успех в процеса на сътрудничество и съгласуваност в съответствие с ОРЗД.

3.2. Обработване на местно равнище

Дейността по обработване на данни на местно равнище не попада под действието на разпоредбите за сътрудничество и съгласуваност на ОРЗД. Надзорните органи ще се съобразяват с компетентността на другите да разглеждат дейността по обработването на данни на местно равнище. Извършваното от публичните органи обработване също винаги ще се разглежда на „местно равнище“.

3.3. Дружества, които не са установени в ЕС

Механизмът за сътрудничество и съгласуваност в рамките на ОРЗД е приложим само за администратори с място или места на установяване в рамките на Европейския съюз. Ако дружеството няма място на установяване в рамките на ЕС, единствено наличието на представител в държава членка не води до прилагането на механизма „обслужване на едно гише“. Това означава, че администратори без никакво място на установяване в ЕС трябва да работят с местните надзорни органи във всяка държава членка, в която осъществяват дейност, посредством техния местен представител.

ПРИЛОЖЕНИЕ – Насочващи въпроси за определянето на водещия надзорен орган

1. Осъществява ли администраторът или обработващият лични данни трансгранично обработване на лични данни?

а. Да, ако:

• администраторът или обработващият лични данни е установен в повече от една държава членка; и

• обработването на лични данни се осъществява в контекста на дейностите на места на установяване в повече от една държава членка.

В този случаи премини към раздел 2.

б. Да, ако:

• обработването на лични данни се осъществява в контекста на дейностите на единственото място на установяване на администратора на данни или обработващия лични данни в Съюза, но:

• засяга съществено или е вероятно да засегне съществено физически лица в повече от една държава членка.

В този случай водещият орган е органът по единственото място на установяване на администратора или обработващия лични данни в една държава членка. Логично това трябва да е основното място на установяване на администратора или обработващия лични данни, тъй като е неговото единствено място на установяване.

2. Как се определя „водещият надзорен орган“?

а. В случай, касаещ само администратор:

i. определяне на мястото на централно управление на администратора в ЕС;

ii. надзорният орган на държавата, в която се намира централното управление, е водещият орган на администратора;

въпреки това:

iii. ако решенията по отношение на целите и средствата на обработването се вземат на друго място на установяване в ЕС и въпросното място на установяване има правомощията да прилага тези решения, тогава водещият орган е органът, намиращ се в държавата по мястото на установяване.

б. В случай, касаещ администратор и обработващ лични данни:

i. проверява се дали администраторът е установен в ЕС и дали механизмът „обслужване на едно гише“ важи за него. В такъв случай,

ii. определя се водещият надзорен орган на администратора. Този орган ще бъде също така водещ надзорен орган за обработващия лични данни.

iii. Компетентният надзорният орган (който не е водещият) на обработващия лични данни ще бъде „засегнат орган“ – вж. точка 3 по- долу.

в. В случай, касаещ само обработващ лични данни:

i. определя се мястото на централно управление на обработващия лични данни в ЕС;

ii. ако обработващият лични данни няма централно управление в ЕС, тогава се определя мястото на установяване в ЕС, където се осъществяват основните дейности по обработване на обработващия лични данни.

г. В случай на съвместни администратори:

i. проверява се дали съвместните администратори са установени в ЕС;

ii. измежду местата на установяване, където се вземат решенията по отношение на целите и средствата на обработването, се определя мястото на установяване, което има правомощията да прилага тези решения по отношение на всички съвместни администратори. Тогава това място на установяване ще се счита за основното място на установяване за целите на обработването, извършвано от съвместните администратори. Водещият орган е този, който се намира в държавата по това място на установяване.

3. Има ли „засегнати надзорни органи“?

Даден орган е „засегнат орган“:

• когато администраторът или обработващият лични данни има място на установяване на своята територия; или

• когато субектите на данни на неговата територия са засегнати съществено или е вероятно да бъдат засегнати съществено от обработването; или

• когато конкретен орган е получил жалба.

ПРИЛОЖЕНИЕ II – Често задавани въпроси

Какво означава водещ надзорен орган?

Общото правило според ОРЗД е, че надзорът върху дейността по трансгранично обработване или такава, включваща граждани на повече от една държава от ЕС, се води само от един надзорен орган, който се нарича „водещ надзорен орган“. Това е известно като принцип на „обслужване на едно гише“.

Водещ надзорен орган е органът, който носи основната отговорност по отношение на дейността по *трансгранично обработване*, когато например се разследва дадено дружество, извършващо дейност по обработване в няколко държави членки.

Водещият орган ще координира операциите, в които участват засегнатите надзорни органи, в съответствие с членове 60–62 от регламента (например обслужване на едно гише, взаимопомощ и съвместни операции). Той ще представя всеки проект на решение на надзорните органи, които са заинтересовани от въпроса.

Какво представлява трансграничното обработване?

Структурата с водещ надзорен орган се прилага само в контекста на трансгранично обработване. Затова е необходимо да се определи дали се осъществява трансгранично обработване.

Според член 4, параграф 23 от регламента „трансгранично обработване“ означава или:

- обработване на лични данни, което се осъществява в контекста на дейностите на местата на установяване в повече от една държава членка на администратор или обработващ лични данни в Съюза, като администраторът или обработващият лични данни е установен в повече от една държава членка; или

- обработване на лични данни, което се осъществява в контекста на дейностите на едно-единствено място на установяване на администратор или обработващ лични данни в Съюза, но което засяга съществено или е вероятно да засегне съществено субекти на данни в повече от една държава членка.

Какво означава „засяга съществено“?

В Регламента не е дадено определение на „засяга съществено“.

Надзорните органи ще тълкуват „засяга съществено“ на база конкретен случай. Ние ще вземаме предвид контекста на обработването, типа на данните, целта на обработването и фактори като дали обработването:

- причинява или е вероятно да причини щети, загуба или страдание на физически лица;

- засяга или е вероятно да засегне от гледна точка на ограничаване на права или лишаване от възможност;

- засяга или е вероятно да засегне здравето, благосъстоянието или спокойствието на физически лица;

- засяга или е вероятно да засегне финансовото или икономическото състояние или обстоятелства на физически лица;

- излага физически лица на дискриминация или несправедливо третиране;

- включва анализирането на специални категории лични или други предполагащи вмешателство данни, особено личните данни на деца;

- кара или е вероятно да накара физическите лица значително да променят своето поведение;

- има невероятни, неочаквани или нежелани последици за физически лица;

- причинява неудобство или други отрицателни резултати, в това число увреждане на репутацията; или

- включва обработването на широк диапазон от лични данни.

Как се определя водещият надзорен орган за администратора?

След като се установи, че съответното обработване представлява трансгранично обработване, тогава трябва да бъде определен водещият надзорен орган.

Според член 56 от регламента надзорният орган на държавата, в която се намира основното място на установяване на организацията, ще бъде водещият орган.

Когато дадена организация има единствено място на установяване в ЕС, но обработването засяга съществено или е вероятно да засегне съществено субекти на данни в повече от една държава членка, водещият надзорен орган е надзорният орган по въпросното единствено място на установяване.

Когато дадена организация има няколко места на установяване в ЕС, принципът е, че основното място на установяване е мястото на централното управление на въпросната организация. Ако обаче решенията по отношение на целите и средствата на обработването се вземат от друго място на установяване и то има правомощията за прилагането на тези решения, тогава то става основно място на установяване. Администраторите на данни следва да определят ясно къде се вземат решенията по отношение на целите и средствата на дейностите по обработване на лични данни.

Например, ако дружество осъществява една или няколко дейности по трансгранично обработване и решенията по отношение на цялото трансгранично обработване се вземат по мястото на централното управление в ЕС, тогава ще има един водещ надзорен орган за всички дейности по трансгранично обработване. Това ще бъде надзорният орган по мястото на централно управление на дружеството.

Ако обаче дадено дружество осъществява няколко дейности по трансгранично обработване и решенията по отношение на средствата и целите на обработването се вземат на различни места на установяване, тогава ще има повече от един водещ надзорен орган. Тези органи ще бъдат органите по местата на установяване, които вземат решенията относно съответните дейности по трансгранично обработване. За да се възползват в пълна степен от механизма „обслужване на едно гише“, предвиждащ единствен водещ надзорен орган за всичките дейности по трансгранично обработване, дружествата следва да разгледат възможностите за организиране на правомощията за вземане на решения по отношение на дейностите по обработване на едно-единствено място.

Какви критерии се използват за определяне на водещ надзорен орган за администратора?

Посочените по-долу фактори са полезни при определянето на местоположението на основното място на установяване на администратора:

- Има ли едно място на установяване в ЕС?

Ако отговорът е да и ако обработването засяга съществено или е вероятно да засегне съществено субекти на данни в повече от една държава членка, водещият надзорен орган е надзорният орган по въпросното единствено място на установяване.

- Има ли седалище в ЕС?

• Ако отговорът е да, каква е неговата роля, вземат ли се в рамките на това място на установяване решения по отношение на целите и средствата на обработването и има ли това място на установяване правомощия за прилагане на решенията относно дейността по обработване?

• Ако отговорът е не, има ли други места на установяване, където:

– се вземат решения относно стопански дейности, включващи обработване на данни?

– реално са съсредоточени правомощията за прилагане на решенията?

– се помещава директорът (или директорите), носещ отговорност за цялостното управление на дейността по трансгранично обработване?

– администраторът или обработващият лични данни е регистриран като дружество, ако става дума за една-единствена територия?

Как се определя водещият надзорен орган за обработващи лични данни?

Регламентът позволява да се възползват от механизма „обслужване на едно гише“ също така обработващи лични данни, които попадат под действието на регламента и имат места на установяване в повече от една държава членка.

В член 4, параграф 16, буква б) е предвидено, че основното място на установяване на обработващия лични данни ще бъде мястото на централното му управление в ЕС или, ако няма централно управление в ЕС, мястото на установяване в ЕС, където се осъществяват основните дейности по обработване.

В съответствие със съображение 36 обаче в случаи, включващи както администратор, така и обработващ лични данни, компетентният водещ надзорен орган ще бъде водещият надзорен орган на администратора. В този случай надзорният орган на обработващия лични данни се счита за „засегнат надзорен орган“ и следва да участва в процедурата за сътрудничество.

РАЗЯСНЕНИЯ НА КЗЛД ОТНОСНО ПРАКТИЧЕСКОТО ПРИЛОЖЕНИЕ НА ОБЩИЯ РЕГЛАМЕНТ ЗА ЗАЩИТА НА ДАННИТЕ ОТ ОРГАНИТЕ НА МЕСТНОТО САМОУПРАВЛЕНИЕ (ОБЩИНИТЕ)

Като единствен надзорен орган по защитата на личните данни, КЗЛД има отговорността да проведе разяснителна кампания и на достъпен език да популяризира основните положения на реформата в ЕС в областта на личните данни и новата правна рамка, която създава Общият регламент за защита на данните. Целта е да се достигне до максимално широк кръг заинтересовани лица.

В предишните два броя на бюлетина бяха публикувани информационно-разяснителни материали на КЗЛД, озаглавени „**10 практически стъпки за прилагане на Общия регламент относно защитата на личните данни“** и **„Практически въпроси на защитата на личните данни след 25 май 2018 г.“.** Тези материали са публикувани на институционалния сайт (www.cpdp.bg), а също така се разпространяват под формата на брошури с едноименни заглавия. Брошурите са отпечатани в 24 000 екземпляра, които се разпространяват в сградата на КЗЛД, на събития с участието на КЗЛД, както и с помощта на публични и браншови организации.

В настоящия брой публикуваме разяснения на КЗЛД относно практическото приложение на Общия регламент за защита на данните от органите на местното самоуправление (общините). С цел постигане на по-голяма яснота и прегледност, разясненията са представени като конкретни въпроси и съответните отговори. Същият текст е публикуван на сайта на КЗЛД (ТУК).

Разяснения на КЗЛД относно практическото прилагане на Общия регламент за защита на данните от органите за местно самоуправление (общини)

1. Предвижда ли се да се разработят унифицирани документи или система от документи по защита на личните данни за всички общини или всяка община ще ги разработва поотделно?

Съгласно съображение 82 от Регламента, за да докаже спазването му, администраторът или обработващият лични данни следва да поддържа документация за дейностите по обработване, за които той е отговорен. В чл. 30 е визирано задължението на администратора да поддържа регистър на дейностите по обработване, като подробно са посочени и реквизитите, които трябва да съдържа. Следва да се отбележи и фактът, че общините са от типа администратори, които обработват лични данни, видът на които, целите и средствата за обработване се определят със специални закони. С оглед възможностите и спецификите на всяка община, разработването на документната система следва да се извърши след анализ и собствена преценка.

2. Какви са задължителните политики, процедури или други документи, които следва да се разработят и внедрят в общината? Регламентът задължава администраторите да опишат всеки един процес в детайл, а не само като минимални мерки за защита при обработка на данните. Означава ли това, че трябва да бъдат описани всички административни услуги, които общината изпълнява?

Като се вземе 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 Регламента, като тези мерки се преразглеждат и при необходимост се актуализират. Когато това е пропорционално на дейностите по обработване, мерките следва да включват прилагане от страна на администратора на подходящи политики за защита на данните. Следва да се отбележи, че придържането към одобрени кодекси за поведение или механизми за сертифициране, може да се използва като елемент за доказване на спазването на задълженията на администратора /арг. чл. 24 от Регламента/.

Както вече беше посочено по-горе, в чл. 30 е визирано задължението на администратора да поддържа регистър на дейностите по обработване, като подробно са посочени и реквизитите, които трябва да съдържа. Обръщаме внимание, че администраторът носи отговорност и трябва да е в състояние да докаже спазването на принципите за обработване на лични данни – т. нар. „отчетност“ /арг. чл. 5 от Регламента/.

3. Очаква ли се да се приемат общи национални правила по защита на личните данни (Кодекси за поведение) и кога евентуално?

Съгласно чл. 40 от Регламента изготвянето на кодекс за поведение е правна възможност, т.е. не е задължително. Той може да се изготвя от администраторите/обработващите лични данни, като целта му е да се улесни ефективното прилагане на Регламента, като се вземат предвид особеностите на обработването на данни в определени сектори и специфичните потребности на администраторите/обработващите. В този ред на мисли, добра практика е кодексите да се изготвят на отраслово (браншово) ниво. В тях може да се установят параметрите на задълженията на администраторите и обработващите лични данни, като се вземе предвид рискът, който е вероятно да произтече от обработването на данни за правата и свободите на физическите лица. Проектът на кодекс, негово изменение или допълнение, следва да се предостави на надзорния орган, който е компетентен да се произнесе със становище дали съответства на Регламента и го одобрява, ако установи, че осигурява достатъчно подходящи гаранции.

4. За общините задължително ли е назначаването на длъжностно лице по защита на данните?

В чл. 37, пара. 1 от Регламента се предвижда длъжностно лице по защита на личните данни да се определя задължително от:

- Публични органи или структури, освен когато става въпрос за съдилища при изпълнение на съдебните им функции;

- Администратори, чиято дейност, поради своето естество, обхват и цели, изискват редовно и систематично мащабно наблюдение на субектите на данни;

- Администратори, чиито основни дейности се състоят в мащабно обработване на специалните категории данни и на лични данни, свързани с присъди и нарушения.

Във връзка с посоченото, общините попадат в категорията на публичните структури и са задължени да определят длъжностно лице по защита на данните.

5. Какви са правните възможности за уреждане на взаимоотношенията между администратора на лични данни и длъжностното лице по защита на данните (DPO) – трудов договор, граждански договор или със заповед да се възложат допълнително функции на служител от администрацията, който да съвместява две длъжности, като се допише длъжностната му характеристика?

Лицето по защита на личните данни може да бъде част от персонала, но може и да е външен субект, който изпълнява своите задължения въз основа на сключен граждански договор. Затова администраторите нямат задължение да назначават специално такъв служител, а само имат задължение да определят лице, което да изпълнява функциите на служител но защита на данните.

Няма пречка служителят, определен за лице по защита на данните, да изпълнява и други функции в рамките на организацията, но те не следва да водят до конфликт на интереси. Изборът на вид правоотношение, при които се определя или назначава лице по защита на личните данни, е изцяло в преценката на администратора на лични данни.

6. Кога личните данни се обработват законосъобразно на основание „изпълнението на задача от обществен интерес“?

Обръщаме Ви внимание, че понятието „обществен интерес“ се използва в смисъла на едно от алтернативните основания за законосъобразност на обработване на лични данни съгласно чл. 6 от Регламента. Във връзка с качеството си на публичноправен субект в голямата част от своята дейност, общината обработва лични данни на основание спазване на законово задължение за администратора.

Понятието „обществен интерес“ е изключително трудно, а вероятно и невъзможно за дефиниране, като се държи сметка за обстоятелството, че става дума за абстрактна правна, политологическа, философска и социално-икономическа категория, чието съдържание зависи не само от състоянието на обществото в конкретен исторически момент, но и от индивидуалните интереси на членовете на обществото.

Общественият интерес не може и не трябва да бъде дефиниран, тъй като той винаги ще се влияе от време, място и възгледи.

Легална дефиниция за обществен интерес няма, макар че масово се използва понятието в редица нормативните актове. Извеждането на обществения интерес е въпрос на тълкуване за всеки конкретен случай.

7. Трябва ли да се изчака да се приемат промените в законовите и подзаконовите нормативни актове, които ще дадат по-голяма конкретика или да се започне работа от общината по привеждането на политиките и процедурите в съответствие с Регламента?

От 25 май 2018 г. във всички държави-членки на ЕС започва прякото прилагане на Общия регламент за защита на данните (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). Регламентът бе обнародван в Официален вестник на Европейския съюз на 04.05.2016 г., а отложеното му прилагане бе продиктувано от необходимостта бизнесът и гражданите да бъдат подготвени за него. Общият регламент е законодателно отражение на най-голямата реформа на Европейския съюз по този въпрос.

Както е указано в 10-те практически стъпки за прилагане на Регламента, не следва да изчаквате за промени в националното законодателство, тъй като Регламентът става част от него, има пряко приложение и дава базисната правна рамка в сферата на защита на личните данни и личната неприкосновеност.

8. До 25.05.2018 г. ли трябва общините да са готови с разработването, внедряването и евентуално сертифицирането на системата от документални и фактически процеси (технически и организационни мерки) за защита на данните?

Считано от 25 май 2018 г. се отменя Директива 95/46/ЕО, която е транспонирана в действащия в момента Закон за защита на личните данни (ЗЗЛД). Това което следва да направите е да приведете досегашната дейност на общината, касаеща обработване и защита на лични данни, в съответствие с новите нормативни изисквания.

9. Сертифицирането е доброволно, но колко ще струва за общините?

Да, сертифицирането е доброволно, но също така то не води до намаляване на отговорността на администратора за спазване на Регламента и не засяга правомощията на надзорния орган /арг. чл. 42, пара. 4/.

Създаването на механизми за сертифициране за защита на данните е в процес на разработка, като по-голяма яснота може да има след приемането на промени в законовите и подзаконовите нормативни актове.

10. След като се разработи цялата система от документи за защита на личните данни на общината, трябва ли да бъде съгласувана с Комисията, преди да бъде внедрена?

Извън изрично посочените случаи на съгласуване и консултиране по смисъла на Регламента, общината не следва да съгласува документацията си за защита на личните данни.

Такава е хипотезата на процедурата по предварителна консултация във връзка с оценка на въздействието по реда на чл. 36 от Регламента. Според разпоредбата администраторът се консултира с надзорния орган преди обработването, когато оценката на въздействието върху защитата на данните покаже, че обработването ще породи висок риск, ако администраторът не предприеме мерки за ограничаването му. Същото е възложено и като задача на длъжностното лице по защита на данните в чл. 39, пара. 1, бук. „д“ от Регламента.

Друга хипотеза е съгласуването на проект на кодекс за поведение /арг. чл. 40, пара. 5/.

В най-общ смисъл новата правна фигура на длъжностното лице по защита на данните следва да информира и съветва администратора и да наблюдава спазването на Регламента в неговата цялост.

11. Какво представлява правото да бъдеш забравен и до каква степен е приложимо в общините?

Регламентът въвежда редица изменения при обработването и защитата на личните данни. Съществена промяна по отношение на правата на гражданите е регламентирането на правото на изтриване (или „правото да бъдеш забравен“). Това право дава възможност, когато субектът на данни не желае данните му да бъдат обработвани и не съществуват законни основания за тяхното съхранение, те да бъдат заличавани.

По отношение на „правото да бъдеш забравен“, следва да се спомене Решението на Съда на Европейския съюз (ЕС) по казуса Google Spain (C-131-12), произнесено през май 2014 г., насочено към изясняване на няколко много важни въпроса, свързани с правото на субектите на лични данни да бъдат забравени, обективирано в Директива 95/46/ЕО. Решението на съда предизвика широк отзвук и разнопосочни реакции както в ЕС, така и извън него, с оглед значението му за регулиране на дигиталното пространство. В него Съдът заключи, че извършваните дейности от търсачки (Google в конкретното решение) представляват обработване на лични данни, което може да засегне значително основните права на личен живот и на защита на личните данни, тъй като улеснява потребителите

в изграждането на подробен профил на съответното лице. Основният въпрос, който решението постави, е дали то е предпоставка за намирането на справедлив баланс между правото на лична неприкосновеност на лицата, свободата на изразяване, правото на достъп до информация и другите законни интереси на лицата в интернет пространството. Съдът счита, че с оглед на основната цел на Директива 95/46/ЕС, а именно да се осигури ефективна защита на основните права и свободи на физическите лица, и в частност на правото им на личен живот, тълкуването на разпоредбата, свързана с приложимостта на правото на ЕС не може да бъде ограничително. На това основание всяко лице, независимо дали е гражданин на държава-членка на ЕС, може да поиска от лицето, предоставящо услуги за търсене в интернет на територията на съответната държава-членка на ЕС, да бъдат заличени връзките към интернет страници, съдържащи информация, която нарушава неговите права, дори и в случаите, когато публикуването на информацията само по себе си е законно.

„Правото да бъдеш забравен“ е доразвито в Регламент (ЕС) 2016/679, като създава високо ниво на защита на личните данни. То е уредено в чл. 17 от Общия регламент. Съгласно пар. 1 на същия, субектът на данни може да поиска, а администраторът е длъжен да изтрие без ненужно забавяне конкретните лични данни. Горната възможност би могла да бъде осъществена единствено при наличието на следните основания:

- личните данни повече не са необходими за целите, за които са били събрани или обработвани по друг начин;
- субектът на данните оттегля своето съгласие, върху което се основава обработването на данните;
- субектът на данни възразява срещу обработването и няма преимуществено законово основание за продължаване на обработването;
- личните данни са били обработвани незаконосъобразно;
- личните данни трябва да бъдат изтрити с цел спазването на правно задължение по правото на Съюза или правото на държава членка, което се прилага спрямо администратора;
- личните данни са били събрани във връзка с предлагането на услуги на информационното общество на дете.

Правото на изтриване е особено важно в последната хипотеза, а именно когато субектът на данни е дал съгласието си като дете и не е осъзнавал напълно рисковете, свързани с обработването. Впоследствие, ако лицето желае да премахне такива лични данни, то следва да може да упражни това право независимо от факта, че вече не е дете. Тази възможност е вследствие на основен принцип, залегнал в регламента, а именно завишената защита на личните данни по отношение на децата.

„Правото да бъдеш забравен“ като основно право в онлайн средата, следва да бъде разширено, като от администратора, който е направил личните данни обществено достъпни се изисква да уведоми администраторите, които обработват такива лични данни, да изтрият всякакви връзки към тези лични данни или техните копия или реплики. По този начин Регламент (ЕС) 2016/679 укрепва правото на изтриване, като пояснява, че организациите в онлайн средата, които правят личните данни публични, следва да информират други организации, които обработват личните данни, за да изтрият линковете или копията на въпросните лични данни. Въпреки че това може да е предизвикателство за администраторите, те трябва да се стремят да спазват тези изисквания. Те са длъжни да предприемат разумни мерки, вземайки предвид наличните технологии и средствата, с които разполагат, за да успеят да изпълнят задълженията си и да информират други администратори, които обработват лични данни, за искането на субекта на данните.

Все пак са налице са редица ситуации, в които администраторът има възможност да откаже да изтрие данните, а именно когато обработването на конкретните данни е с цел:

- да упражнява правото на свобода на изразяване и информация;
- да изпълнява правно задължение или да изпълнява задача от обществен интерес или упражняване на публична власт;

• за целите на общественото здраве;

• архивиране за цели в обществен интерес, научноизследователски исторически изследвания или статистически цели; или

• установяване, упражняване или защитата на правни претенции.

Предвид горното, „правото да бъдеш забравен“ не е абсолютно право. Всеки субект на данни може да се възползва от това си право единствено при наличие на конкретно основание.

12. През какъв интервал от време следва да се преглежда оценката на риска за съответствие с Регламента?

С цел да се поддържа сигурността и да се предотврати обработване, което е в нарушение на Регламента, администраторът или обработващият лични данни следва да извърши оценка на рисковете, свързани с обработването, и да предприеме мерки за ограничаване на тези рискове, например криптиране. Тези мерки следва да гарантират подходящо ниво на сигурност, включително поверителност, като се вземат предвид достиженията на техническия прогрес и разходите по изпълнението спрямо рисковете и естеството на личните данни, които трябва да бъдат защитени. При оценката на риска за сигурността на данните следва да се разгледат рисковете, произтичащи от обработването на лични данни, като случайно или неправомерно унищожаване, загуба, промяна, неправомерно разкриване, или достъп до предадени, съхранявани или обработвани по друг начин лични данни, което може по-конкретно да доведе до физически, материални или нематериални вреди.

В чл. 35, пара. 11 на Регламента е посочено, че при необходимост администраторът прави преглед, за да прецени дали обработването е в съответствие с оценката на въздействието върху защитата на данни, най-малкото когато има промяна в риска, с който са свързани операциите по обработване. Извършването на оценка на риска, както и тази на въздействието, е непрекъснат процес и следва да се актуализира през целия „жизнен цикъл“ на защита на данните, с оглед спецификата и по решение на самия администратор.

13. През какъв период следва да се извършват вътрешни одити на системата въз основа на Регламента и на вътрешните документи. От кого трябва да се извършват вътрешните одити?

Преценката за вида и честотата на извършване на одити се прави от администратора на лични данни /арг. чл. 24 от Регламента/, като следва да се отбележи и функцията на длъжностното лице по защита на данните да наблюдава спазването на Регламента, политиките на администратора по отношение на защитата на личните данни, включително възлагането на отговорности, повишаването на осведомеността и обучението на персонала, участващ в операциите по обработване, и съответните одити.

14. Какви ще бъдат санкциите за публичните органи?

Общите условия за налагане на административни наказания „глоба“ или „имуществена санкция“ са разписани подробно в чл. 83 на Регламента.

Когато имуществената санкция се налага на предприятие, понятието „предприятие“ следва да се разбира като предприятие в съответствие с членове 101 и 102 от ДФЕС за тези цели. При налагане на административни наказания „глоба“ и „имуществена санкция“ на лица, които нямат качеството предприятие, надзорният орган следва да има предвид общото равнище на доход в съответната държава членка, както и икономическото състояние на лицето, за да определи подходящия размер на глобата. Държавите членки следва да определят дали и до каква степен публичните органи следва да подлежат на административни наказания „глоба“ или „имуществена санкция“ /арг. съображение 150 от Регламента/.

За целите на антитръстовото законодателството на ЕС, всеки обект, който участва в икономическа дейност, т.е. дейност, при която има предлагане на стоки или услуги на даден пазар, независимо от неговото правно състояние и начина на финансиране, се нарича предприятие.

Във връзка с изложеното следва да се разгледа и понятието „публично предприятие“.

То е предприятие, при което публичните органи упражняват пряко или косвено контролиращо влияние по силата на своята собственост, финансово участие или ръководните правила. Контролиращо влияние на публичните органи е налице, когато те: а) притежават мнозинство от записания капитал на предприятието, б) контролират мнозинството от гласовете, прикрепени към акциите, емитирани от предприятието или в) са в положение, в което назначават повече от половината от членовете в административните, управленски или надзорните органи на дружеството.

ИНИЦИАТИВИ НА КЗЛД ОТНОСНО ПОДГОТОВКАТА ЗА ПРИЛАГАНЕТО НА НОВАТА ЕВРОПЕЙСКА ПРАВНА РАМКА

Комисията за защита на личните данни е ангажирана активно с подготовката за прилагане на Общия регламент за защита на личните данни (Регламент (ЕС) 2016/679) и Директивата за защита на личните данни в полицейската и наказателната дейност (Директива (ЕС) 2016/680) от момента на приемането им през 2016 г.

По отношение на информационно-разяснителните дейности трябва да се отбележи, че информационната дейност на КЗЛД е с постоянен характер и нейната цел е посланията да достигнат до максимално широк кръг заинтересовани лица – граждани и администратори на лични данни. В качеството й на надзорен орган по защита на личните данни, КЗЛД има отговорността по достъпен начин да разясни на обществото основните положения на реформата в ЕС в областта на личните данни и новата правна рамка, която създава Общият регламент за защита на данните. Във връзка с това Комисията предприе редица инициативи, като някои от по-важните са:

1. КЗЛД изготви 2 информационни брошури, чиято цел е разясняване на ключови аспекти, свързани с прилагането на Общия регламент. Брошурите са озаглавени *„Практически въпроси на защитата на личните данни след 25 май 2018 г.“* и *„10 практически стъпки за прилагане на Общия регламент относно защитата на личните данни“*. Предвид динамиката на процесите, информацията периодично ще бъде актуализирана и допълвана с разяснения и по други важни въпроси с практическа насоченост. Брошурите са публикувани на институционалния сайт на КЗЛД и са отпечатани в 24 000 екземпляра, които ще бъдат разпространявани от КЗЛД с помощта на заинтересовани публични органи и браншови организации.

2. На 29 януари 2018 г. се състоя най-мащабното събитие в България по повод влизането в сила на Общия регламент за защита на личните данни – конференция „GDPR София”, която протече при много голям интерес. Организатори на форума бяха Дигитална Национална Коалиция, със съдействието на Министерството за Българското председателство на Съвета на ЕС и КЗЛД. Конференцията бе открита от г-жа Мария Габриел – еврокомисар по цифровата икономика и общество, г-жа Лиляна Павлова – министър на българското председателство, г-н Венцислав Караджов – председател на КЗЛД и г-жа Гергана Паси – председател на Дигиталната Национална Коалиция. Над 300 участници от цялата страна се включиха в събитието, включително експерти от Европейската комисия, докладчици от Европейския парламент и представители на някои от най-големите бизнес компании.

3. КЗЛД организира разяснителна кампания в пет областни града в България – Пловдив, Велико Търново, Варна, Бургас и Стара Загора в месеците от февруари до май 2018 г. Целта на събитията бе постигане на широка обществена осведоменост по всички въпроси, свързани с реформата в ЕС в областта на личните данни и новата правна рамка, която създава Общият регламент за защита на данните. Те бяха насочени към широката публика, администраторите на лични данни и към всички заинтересовани лица. В хода на събитията бяха представени основните моменти в новата правна рамка и необходимите практически стъпки за администраторите с цел въвеждане в дейността им на новоприетите стандарти за защита и обработване на личните данни.

4. В последните месеци се проведоха редица работни срещи-дискусии с някои от най-големите администратори на лични данни, обработващи данни на милиони граждани. На 14 и 15 декември 2017 г. се проведе работна среща на експерти от КЗЛД с представители на трите мобилни оператора на територията на България – Виваком, Мобилтел и Теленор. На 2 март 2018 г. се състоя среща на председателя на КЗЛД и експерти от Комисията с представители на трите електроразпределителни дружества в България - CEZ Bulgaria, EVN Bulgaria и Energo-Pro Bulgaria. На 29 март 2018 г. представители на КЗЛД участваха в дискусия относно въвеждането на Общия регламент в туристическия бранш, проведена в рамките на годишна конференция на бранша. С нарастваща интензивност се състояха множество други подобни срещи – с Националната асоциация на секретарите общини в България, със съдии от Върховния административен съд и Административен съд София-град, с Българската стопанска камера, Българския съюз за митническо и външнотърговско обслужване, Българската търговско-промишлена палата, Държавна комисия по сигурността на информацията, Асоциацията на индустриалния капитал, Българския лекарски съюз, Българския зъболекарски съюз, Нов български университет, читалища, застрахователни дружества и др.

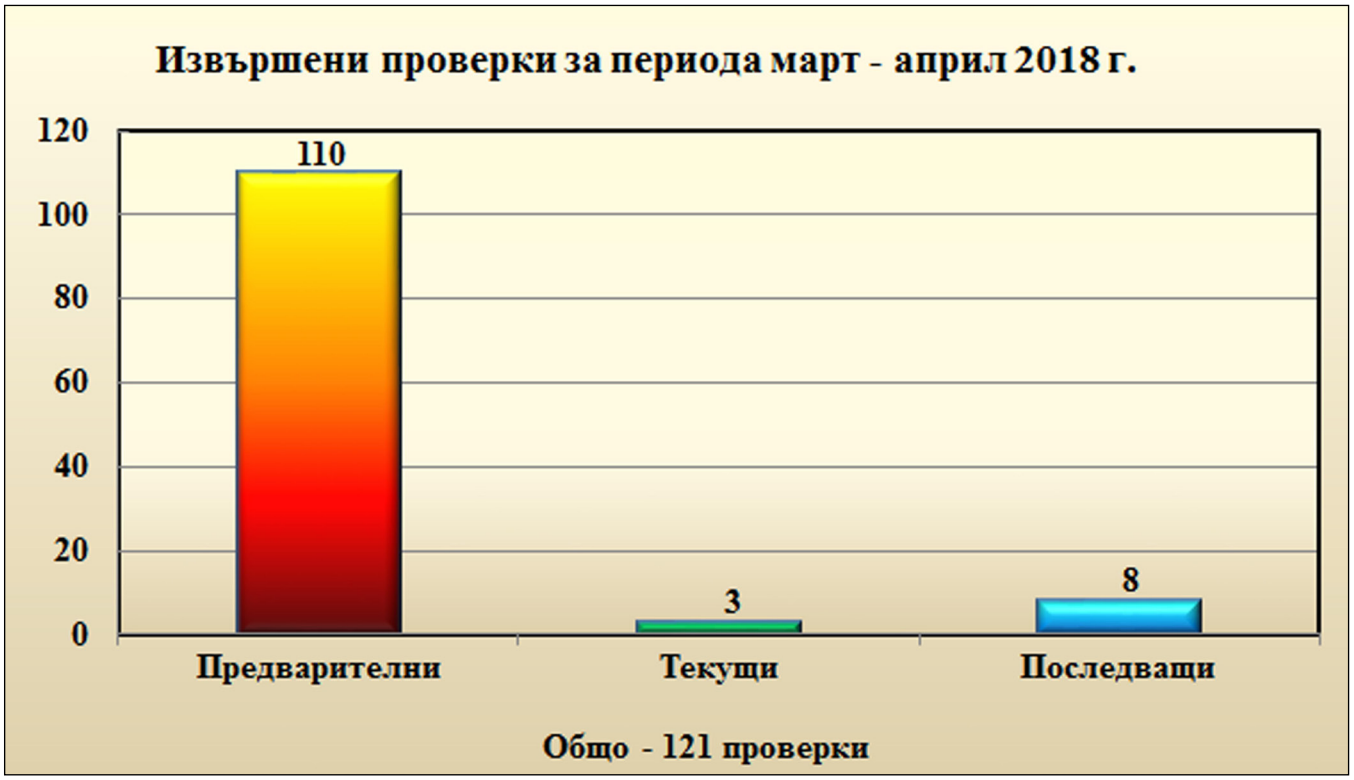
Информационно-разяснителнните дейности на КЗЛД ще продължат и след 25 май 2018 г. в зависимост от обществените потребности от тях. Поради ограничения си административен ресурс, Комисията ще съсредоточи усилията си в разяснителна кампания на секторен принцип към представителни организации на администратори на лични данни.

Едновременно с мащабните информационно-разяснителни дейности, протече и подготовката за изменения и допълнения в националното законодателство. КЗЛД работи активно по подготовката на необходимите изменения и допълнения в националното законодателство от 2016 г. В резултат на усилията на КЗЛД и другите ангажирани ведомства, на 30.04.2018 г. Министерство на вътрешните работи (МВР), което е вносител на Закона за изменение и допълнение на Закона за защита на личните данни (ЗИДЗЗЛД), го предостави за обществено обсъждане от гражданите и бизнеса, както и от заинтересованите ведомства (**www.strategy.bg**).

Относно приносите на КЗЛД по подготовката за прилагането на новата европейска правна рамка трябва да се отбележи, че Председателят на КЗЛД, както и други представители на Комисията, участват активно в изготвянето на общи насоки по приложението на новата правна рамка за защита на личните данни в ЕС.

СТАТИСТИКА И АНАЛИЗ НА КОНТРОЛНАТА ДЕЙНОСТ ЗА ПЕРИОДА МАРТ - АПРИЛ 2018 г.

На основание чл. 12 от Закона за защита на личните данни през месеците март и април 2018 г. са извършени общо 121 проверки. Най-голям е делът на предварителните проверки, извършвани на основание чл. 17б от ЗЗЛД (когато администраторът е заявил обработване на данни по чл. 5, ал. 1 от ЗЗЛД или на данни, чието обработване съгласно решение на комисията застрашава правата и законните интереси на физическите лица). За периода извършените предварителни проверки са 110 броя, на базата на които са вписани съответните администратори на лични данни или са актуализирани техните регистри с лични данни в регистъра по чл. 10, ал. 1 т. 2 от ЗЗЛД.



Разгледани са 35 искания от физически лица, включително различни запитвания по актуални въпроси, свързани със защита на личните данни. На всички податели са изпратени съответни отговори.

През периода са съставени 4 акта за установяване на административно нарушение и е издадено 1 задължително предписание.

РЕГИСТРАЦИЯ НА АЛД

ИНФОРМАЦИЯ ЗА ПРОЦЕСА ПО РЕГИСТРАЦИЯ И СТАТИСТИКА ЗА ПЕРИОДА МАРТ - АПРИЛ 2018 г.

От 25 май 2018 г. отпада задължението за регистрация на АЛД в КЗЛД. Считано от тази дата, отпада необходимостта от подаване на заявления за регистрация, молби за освобождаване от регистрация и заявления за заличаване от регистъра на КЗЛД. 25 май 2018 г. КЗЛД преустановява поддържането на публични регистри за вписване/освобождаване/отказване на регистрация на АЛД. Отпада и необходимостта от издаването на удостоверения и служебни бележки относно обстоятелствата по регистрация на АЛД.

Общият регламент за защита на данните, който започва да се прилага пряко във всички държави-членки на ЕС от 25 май 2018 г. отклонява системата на уведомяване и дава предпочитание на принципа на отчетност. Според насоките на ЕК от 24.01.2018 г. „Принципът на отчетност се осъществява на практика чрез задължения, които варират в зависимост от риска .... Въвежда се нов инструмент, който да помогне при оценяването на риска преди започване на обработката: оценка на въздействието върху защитата на данните.“

Досега извършваната регистрация на АЛД беше не само нормативно изискване на ЗЗЛД, а и стъпка към осъзнаване на отговорностите, които боравещите с личните данни на гражданите имат по опазването на тези лични данни. Във всички издавани до момента бюлетини е предоставяна информация за процеса по регистрация на АЛД. В настоящия бюлетин за пореден, и вероятно за последен път, публикуваме статистика за изтеклия двумесечен период.

През **март и април 2018 г.** в електронната система за регистрация на администратори на лични данни (еРАЛД) са създадени нови 1690 потребителски профила на АЛД. От тях 1599 са на АЛД, подали заявление за вписване в регистъра по чл. 10 ал. 1 т. 2 от ЗЗЛД и 91 - на АЛД, желаещи да бъдат освободени от задължението за вписване в този регистър. В резултат на това в еРАЛД вече има създадени 375679 потребителски профила, от които – 343811 на АЛД, подали заявления за регистрация и 31868 - на тези, които са изявили желание за освобождаване от това задължение.

През този период КЗЛД взема решения за:

- вписване в регистъра по чл.10 ал.1 т.2 от ЗЗЛД на 1426 нови АЛД. С това общият брой на вписаните АЛД в регистъра по чл.10 ал.1 т.2 от ЗЗЛД става 297082;
- освобождаване от задължението за вписване в регистъра на КЗЛД – 66 АЛД, с което общият брой на освободените от регистрация става 28554;
- заличаване от регистъра по чл. 10, ал. 1, т. 2 от ЗЗЛД на 12 АЛД. С това общият брой на заличените администратори става 464.

За проверка по чл. 17б на ЗЗЛД са подадени 101 АЛД.

През периода са обработени 1640 подадени на хартиен носител заявления за регистрация и молби за освобождаване от задължение за вписване.

СТАНОВИЩЕ
НА
КОМИСИЯТА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ
рег. № НДМСПО-01-221/13.04.2018 г.
гр. София, 26.04.2018 г.

ОТНОСНО: ***Видеонаблюдение при провеждане на държавните зрелостни изпити*****.**

Комисията за защита на личните данни (КЗЛД) в състав – членове: Цанко Цолов, Цветелин Софрониев, Мария Матева и Веселин Целков, на заседание, проведено на 25.04.2018 г., разгледа искане /вх. № НДМСПО-01-221/13.04.2018 г./ за становище от г-жа Албена Михайлова – главен секретар на Министерство на образованието и науката (МОН).

Във връзка с изпълнение на дейности по контрол на организацията, провеждането и оценяването на държавните зрелостни изпити (ДЗИ), както и осигуряване на информационната сигурност при работа с изпитните документи и на надеждна среда за провеждане на изпитите, МОН моли за становище относно законосъобразността на видеонаблюдението в изпитните зали по време на провеждане на ДЗИ и дали това би довело до неспазване на Закона за защита на личните данни (ЗЗЛД) и прилагащия се от 25.05.2018 г. Общ регламент за защита на личните данни (Регламент (ЕС) 2016/679).

В искането се посочва, че съгласно чл. 132, ал. 1 от Закона за предучилищното и училищно образование, учениците, успешно завършили XII клас, стават зрелостници и придобиват право да се явят на държавни зрелостни изпити и на държавен изпит за придобиване на професионална квалификация.

В съответствие с чл. 85 от Наредба № 11 от 01.09.2016 г. за оценяване на резултатите от обучението на учениците, издадена от министъра на образованието и науката, контролът по организацията, провеждането и оценяването на държавните зрелостни изпити се осъществява от министъра на образованието и науката и посочените от него длъжностни лица.

Съгласно чл. 84, т. 5, бук. „а“ от горепосочената наредба, министърът на образованието и науката утвърждава със заповед правила за информационна сигурност при провеждането на ДЗИ.

Във връзка с гореизложеното г-жа Михайлова поставя въпрос, в случай че извършването на видеонаблюдение е законосъобразно, може ли то да бъде регламентирано в правилата за информационна сигурност, които следва да бъдат утвърдени със заповед от министъра на образованието и науката.

Правен анализ:

Видеонаблюдението представлява действие по обработване на лични данни по смисъла на § 1, т. 1 от Допълнителните разпоредби на Закона за защита на личните данни (ЗЗЛД).

Обработването на лични данни, в случая чрез видеонаблюдение, може да се извършва при наличие на едно от основанията за законосъобразно обработване, посочени в чл. 4, ал. 1 от ЗЗЛД и при стриктно спазване на принципите, визирани в чл. 2, ал. 2 от закона.

В конкретния казус приложение може да намери основанието по чл. 4, ал. 1, т. 5, а именно: „обработването е необходимо за изпълнението на задача, която се осъществява в обществен интерес“.

При позоваването на понятието „обществен интерес“ е необходимо да се отбележи, че става дума за абстрактна правна, политическа, философска и социално-икономическа категория, чието съдържание зависи както от състоянието на обществото в конкретен исторически момент, така и от индивидуалните интереси на отделните членове на обществото.

През последните години в общественото пространство циркулира темата с провеждането на ДЗИ и необходимостта от предотвратяване на измами и спекулации по време на провеждането им. Категорично може да се направи извод, че видеонаблюдението в изпитните зали е една от мерките за противодействие на манипулиране на резултатите, като същото способства за обективното и честно провеждане на изпитите и в този ред на мисли неминуемо поражда засилен обществен интерес.

Във връзка с гореизложеното следва да се отбележи, че в Регламента основанието за законосъобразно обработване на лични данни „изпълнение на задача от обществен интерес“ е доразвито и е със завишени правни характеристики /арг. чл. 6, пара. 2 и 3 във вр. с пара. 1, бук. „д“, предл. 1/ и в конкретния случай позоваването на него след 25 май не би породило търсената правна сигурност при провеждане на ДЗИ, считано от тази дата.

Във връзка с това от правно-техническа гледна точка решение може да се намери в изменение и допълнение на визираната по-горе Наредба № 11 от 01.09.2016 г. за оценяване на резултатите от обучението на учениците, издадена от министъра на образованието и науката, в която изрично да се посочи, че видеонаблюдението е една от мерките за превенция на лошите практики при провеждане на ДЗИ.

По този начин регламентирането на дейността по извършване на видеонаблюдение в нормативен акт би гарантирало прозрачност в действията по обработване на лични данни при извършване на видеонаблюдение при провеждане на ДЗИ. По преценка на администратора – МОН, наредбата би могла да регламентира и всички други допълнителни аспекти, свързани с изпълнението на тази задача от обществен интерес, а именно: трети страни, на които евентуално биха могли да бъдат разкрити; целите, за които данните се разкриват; периода на съхранение на данните, след изтичането на който данните от видеозаписите подлежат на изтриване; мерките за гарантиране на законосъобразно и добросъвестно обработване.

При използването на технически средства за видеонаблюдение е изключително важно да се прилагат принципите за адекватност и пропорционалност при обработване на лични данни чрез видеонаблюдение:

- На първо място видеозаписите, съхранени на различен тип носители, трябва да се обработват добросъвестно и законосъобразно, за конкретни и точно определени цели /арг. чл. 2, ал. 2, т. 1 и 2 от ЗЗЛД/;

- На второ място това е задължението за прозрачност и информираност /арг. чл. 19 ЗЗЛД/, за реализиране на което, министърът на образованието и науката в качеството си на администратор следва да предостави информация за:

1. целите на обработване на лични данни;

2. получателите или категориите получатели, на които могат да бъдат разкрити данните;

3. данни за задължителния или доброволния характер на предоставяне на данните и последиците от отказ за предоставянето им;

4. информация за правото на достъп и правото на коригиране на събраните данни.

Целесъобразно е тази информация да бъде оповестена предварително по подходящ начин (напр. на интернет страницата на МОН), напр. едновременно с всяка друга относима към провеждането на ДЗИ информация. Добра практика всяко училище, в което се провеждат ДЗИ, също да оповести факта на извършване на видеонаблюдение, посредством информационни табели.

- Не трето място е и необходимостта от предприемане на необходимите технически и организационни мерки за защита на обработваните чрез системите за видеонаблюдение лични данни /арг. чл. 23 от ЗЗЛД/;

- И не на последно място след постигане целта на обработване на личните данни или преди преустановяване на обработването им администраторът е длъжен да ги унищожи /арг. чл. 25 ЗЗЛД/.

С оглед на гореизложеното и на основание чл. 10, ал. 1, т. 4 от ЗЗЛД, Комисията за защита на личните данни изразява следното

СТАНОВИЩЕ:

От гледна точка защитата на личните данни, извършването на видеонаблюдение при провеждане на държавните зрелостни изпити (ДЗИ) представлява действие по обработване на лични данни и като такова може да се извършва законосъобразно на основание „изпълнение на задача от обществен интерес“ по смисъла на чл. 4, ал. 1, т. 5 от ЗЗЛД, и при спазване на принципите, визирани в чл. 2, ал. 2 от закона.

С цел създаване на правна сигурност след стартиране на прилагането на Общия регламент след 25 май 2018 г. е препоръчително да бъдат предприети изменения и допълнения в Наредба № 11 от 01.09.2016 г. за оценяване на резултатите от обучението на учениците, издадена от министъра на образованието и науката, в която изрично да се посочи, че при провеждане на ДЗИ може да се извършва видеонаблюдение като една от мерките за превенция на лошите практики в защита на обществения интерес.

ЧЛЕНОВЕ:

Цанко Цолов /п/

Цветелин Софрониев /п/

Мария Матева /п/

Веселин Целков /п/

СТАНОВИЩЕ
НА
КОМИСИЯТА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ
Рег. № П – 5375/2017 г.
гр. София, 30.04.2018 г.

ОТНОСНО: ***Искане с вх. № П-5375/2017 год. от Председателя на Държавна агенция за закрила на детето, по въпроси, касаещи въвеждането на видеонаблюдение в детските заведения (детски ясли и детски градини), както и в училищата.***

Комисията за защита на личните данни (КЗЛД, Комисията) в състав: членове: Цанко Цолов, Цветелин Софрониев, Мария Матева и Веселин Целков, на заседание, проведено на 28.03.2018 г., разгледа преписка с вх. № П-5375/2017 г. от Председателя на Държавна агенция за закрила на детето (ДАЗД), в което посочва, че в ДАЗД е постъпило писмо с вх. № 04-22-11/29.06.2017г., от г-жа Светлана Йорданова - зам.-министър на здравеопазването, с молба за изразяване на становище, относно въвеждането на видеонаблюдение в детските заведения /детски ясли и детски градини/ и дали това ще доведе до нарушаване правата на децата.

Председателят на ДАЗД моли, във връзка с компетентността си, КЗЛД да изрази становище по темата.

В искането се посочва, че за Държавната агенция за закрила на детето е от първостепенна важност правата на всяко дете в Р. България да са гарантирани и защитени и вярва, че ползотворното сътрудничество между институциите ще осигури в пълна степен правата и интересите на децата.

Към искането е приложено копие на писмо с вх. № 04-22-11/29.06.2017г. и отговор от ДАЗД до Министерството на здравеопазването.

В писмото си Заместник-министъра на здравеопазването, отбелязва, че в последно време в различните медии е огласен и коментиран въпросът с видеонаблюдението на децата в детските заведения, с цел подобряване на сигурността и прозрачността на грижите, както и решаване на възникнали конфликти при отглеждането на децата в детските заведения. В тази връзка в Министерството на здравеопазването са постъпили редица писма от родители и медицински специалисти с въпроси по дискутираната тема.

Във връзка с горното на вниманието и на КЗЛД е изпратено и копие от отворено писмо от колектива на 31 детска ясла в гр. София, с молба за изразяване на становище, предвид компетентността на ДАЗД, дали видеонаблюдението може да се счита за нарушаване на правата на здрави деца или деца с увреждания, при осъществяване на ежедневните дейности, провеждани в детските ясли и при какви условия. Отправеното предложение за поставяне на видеонаблюдение в детските ясли е в резултат на реакцията на конкретни родители, отразена широко в медиите. Съвсем естествено и основателно това предизвиква реакция и от страна на ръководствата и персонала в детските ясли не само в столицата, но и в цялата страна.

При разглеждането на административна преписка, и направения обстоен анализ на законовата уредба, първоначалният извод, който може да бъде направен е, че към момента няма яснота и конкретно нормативно регламентиране на поставените в искането въпроси.

Поради големия обществен интерес и с оглед обстоятелството, че Държавната агенция за закрила на детето, Министерството на здравеопазването и Министерството на труда и социалната политика имат пряко отношение към разглеждания казус, беше отправено искане за становище към ръководителите на изброените по-горе ведомства.

От Министерството на здравеопазването беше изразено следното становище:

Устройството и дейността на детските ясли се регламентира с разпоредбите на Наредба № 26 от 2008 г. за устройството и дейността на детските ясли и детските кухни и здравните изисквания към тях. Изискванията към детските градини се регламентират с разпоредбите на Правилника за прилагане на Закона за народната просвета и Наредба № 3 от 2007 г. за здравните изисквания към детските градини. Към настоящия момент разпоредбите на горепосочените подзаконови нормативни актове не регламентират осъществяване на видеонаблюдение в детските ясли и градини.

Правен анализ:

Въпросът за законосъобразното извършване на видеонаблюдение е поставян многократно за произнасяне от КЗЛД, съобразно вменените нормативни правомощия като национален надзорен орган да осъществява защитата на лицата при обработването на личните им данни. Към настоящия момент работата на Комисията по този въпрос е отразена в решения по жалби на граждани, становища по приложението на Закона за защита на личните данни (ЗЗЛД), отговори на въпроси и издадени Наказателни постановления.

Практиката на КЗЛД по темата за видеонаблюдението в последните години показва, че с развитието на технологиите в национален и световен мащаб се развиват и технологиите, в областта на системите за видеонаблюдение. Посредством инсталиране на различен вид системи за видеонаблюдение, широко достъпни на пазара, се предоставя възможност на физически и юридически лица за наблюдение на различни субекти и обекти, както локално, така и чрез възможност за отдалечен достъп до изходящи образи от видеокамери и записи с видеокадри.. Това развитие на технологиите и прякото им отражение в сферата на обществения и частния живот не може да не бъде отчитано от Комисията, когато решава въпросите за законосъобразността и допустимостта на видеонаблюдението.

Поради обстоятелството, че в България видеонаблюдението, като вид обработване на лични данни не е подробно уредено, при разглеждане на отделните казуси, КЗЛД анализира и международното законодателство и практика, свързани с обработването на лични данни, осъществявано чрез видеонаблюдение. При извършване на видеонаблюдение, като вид техническа форма на обработване на лични данни, която става все по-достъпна и лесно приложима в различни области на съвременния живот, се налага и нуждата от подробна нормативна регламентация. Във връзка с масовото навлизане на видеонаблюдението във всички сфери на живота, все по-актуален става въпросът за защита на неприкосновеността на личността и личния живот.

Най-общо, основните принципи за неприкосновеността на личния и семейния живот са заложени в редица европейски и международни актове – Конвенция за защита правата на човека и основните свободи, Харта за основните права на Европейския съюз, Конвенция 108 на Европейския парламент за защита на лицата при автоматизирана обработка на личните данни, както и най-новият европейски правен акт с пряко действие в държавите-членки – 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 / General Data Protection Regulation (GDRP). В Конвенция 108 на Европейския парламент за защита на лицата при автоматизирана обработка на личните данни се прокламира една обща цел за зачитане на правата и основните свободи на всяко физическо лице и по-конкретно правото му на личен живот по отношение на автоматизираната обработка на лични данни, отнасящи се до него. Видеонаблюдението като вид автоматизирана обработка на лични данни попада под регламентацията на тази конвенция. Детайлизиране на общия принцип за неприкосновеност на личния и семеен живот е постигнато в Общият регламент за защита на данните, като основен правен акт, който урежда защитата на личните данни в Европейския съюз. Приложението на Регламент (ЕС) 2016/679 е с отложено действие, а именно: от 25 май 2018 година. Едновременно с посочените правни актове, по отношение на разглежданата категория субекти (деца и подрастващи), разпоредбите на Конвенцията на ООН за правата на детето гарантират правото на децата на неприкосновеност на личния живот.

При извършване на нормативно проучване се установява, че отделните страни в Европейския съюз са регламентирали по различен начин въпроса с видеонаблюдението – посредством закони, указания, становища. Това е наложило в Еврозоната да бъдат приети и общи правила с оглед разнообразната практика. Основна роля по уеднаквяването на практиката в различните страни-членки е на Работната група по Член 29 от Директива 95/46/ЕО. На заседание на РГ 29 е изработен „Работен документ относно обработването на лични данни чрез видеонаблюдение". По този въпрос РГ 29 има изразено и „Становище 4/2004 относно обработване на лични данни чрез средства за видеонаблюдение".

Въпросите, свързани с видеонаблюдението, могат да бъдат анализирани в няколко насоки:

- Защита на живота и здравето на лицата, обект на видеонаблюдение;
- Обществен интерес;
- Разкриване, предотвратяване и контрол на нарушения/престъпления;
- Защита на собствеността;
- Други законни интереси.

Изводът, който може да се направи е, че при използването на технически средства за видеонаблюдение е изключително важно да се прилагат принципите за адекватност и пропорционалност при обработване на лични данни чрез видеонаблюдение:

- На първо място това е въпросът с качеството на обработваните данни. Изображенията от видеокамерите, както и записите с видеокадри, съхранени на различен тип носители, трябва да се обработват добросъвестно и законосъобразно, за конкретни и точно определени цели;

- Предвид посоченото по-горе относно липсата на конкретна нормативна регламентация във връзка с искането за становище, е необходимо да бъде спазено поне едно от следните условия: защита на значими жизнени интереси на субектите на данни, изпълнение на задача, извършвана в обществен интерес;

- На трето място това са правото на информация, правото на достъп и правото на искане за коригиране от страна на лицето, обект на видеонаблюдението;

- Не на последно място е и необходимостта от предприемане на достатъчно технически и организационни мерки за защита на обработваните чрез системите за видеонаблюдение лични данни.

Факт е, че към момента не е създаден регламент, който да указва правила за инсталиране и внедряване на системи за видеонаблюдение, както в детските заведения (ясли и градини), така и в училищата. Посочените действия съставляват действия по обработване на лични данни по смисъла на § 1 , т. 1 от Допълнителните разпоредби на ЗЗЛД, както и легалната дефиниция, разписана в чл. 4, т. 2) от Регламент (ЕС) 2016/679.

По-нататък в изложението ще се посочват само разпоредбите на Регламент (ЕС) 2016/679 (приложим от 25 май 2018 год.).

Обработването на лични данни, в случая чрез видеонаблюдение, може да се извършва при наличие на една от хипотезите, разписани в чл. 6 от Регламент (ЕС) 2016/679 и при стриктно спазване на принципите, визирани в чл. 5 от регламента.

В конкретно разглеждания казус приложение може да намерят две от алтернативно изброените предпоставки за законосъобразност на обработването, разписани в чл. 6 от Регламент (ЕС) 2016/679, а именно: чл. 6, пар. 1, буква г) – обработването е необходимо, за да бъдат защитени жизнено важни интереси на субекта на данните или на друго физическо, както и чл. 6, пар. 1, буква д), предл. първо - обработването е необходимо, за изпълнение на задача от обществен интерес.

Посоченият в искането за становище аргумент за необходимостта от въвеждане на видеонаблюдение за подобряване на сигурността и прозрачността на грижите, както и решаване на възникнали конфликти при отглеждането на децата в детските заведения, а също и в училищата, е основателен мотив с цел защита живота и здравето на най-уязвимата категория от обществото като цяло – децата и непълнолетните български граждани. В този смисъл относимостта на посочената по-горе разпоредба на чл. 6, пар. 1, буква г) от Регламент (ЕС) 2016/679 е в пряка връзка с анализирания казус.

Едновременно с дотук изложеното, разглежданият въпрос е и в резултат на реакциите на много родители, отразени широко в медиите. В случая следва да се вземе предвид и обществения интерес от въвеждане на прозрачност в грижите за децата и подрастващите. При позоваването на понятието „обществен интерес" е необходимо да се държи сметка за обстоятелството, че става дума за абстрактна правна, политическа, философска и социално-икономическа категория, чието съдържание зависи както от състоянието на обществото в конкретен исторически момент, така и от индивидуалните интереси на отделните членове на обществото. На практика въпросът за сигурността, живота и здравето на българските деца и ученици е от първостепенна важност за обществото като цяло. Следователно разпоредбата на чл. 6, пар. 1, буква д), предл. първо от Регламент (ЕС) 2016/679 също е законосъобразна предпоставка за обработване на лични данни чрез извършване на видеонаблюдение.

Отделно от посоченото е важно да се отбележи, че предвид спецификата на детските ясли и градини (малката възраст на децата, определяща ги като едни от най-уязвимите групи), общите помещения за сън и игра, и общите санитарни помещения, въвеждането на видеонаблюдение в помещенията за почивка и лична хигиена на децата е в разрез с техните права. С оглед на защитата на личните права на децата е изключено поставянето на такова в спалните помещения, тъй като с наличните устройства в тези помещения не се дава право на децата на уединение и запазване на личното им достойнство, както и представлява нарушение на правото на неприкосновеност на личността. Това би създало предпоставки за прекомерна намеса в техния личен живот, в разрез с

чл. 16 от Конвенцията на ООН за правата на детето. Според разпоредбата, в услугите за деца и в институциите трябва да бъде осигурено пространство, което да гарантира неприкосновеността на личния живот на децата, поради което денонощното наблюдение на личните им стаи е недопустимо.

Допустимо е постоянното видеонаблюдение в общите помещения и дворните пространства, което да гарантира безопасността на децата и учениците при игри, занимания и в свободното им време. Такова наблюдение е допустимо единствено да бъде приложено за местата на заниманията, ако са отделени от местата за сън и почивка, и в общите части на сградата.

Отделно от извършения по-горе нормативен анализ за законосъобразните придпоставки във връзка с разглеждания казус, е необходимо да се отчетат задълженията и отговорностите на администраторите на лични данни, които следва да съобразят действията по обработване на лични данни чрез системи за видеонаблюдение с новите стандарти защита на личните данни, въведени с разпоредбите на Регламент (ЕС) 2016/679.

Съгласно чл. 24 от Общия регламент за защита на личните данни, след като вземе предвид естеството, обхвата, контекста и целите на обработването, администраторът следва да въведе подходящи технически и организационни мерки, за да гарантира, както и във всеки един момент да е в състояние да докаже, че обработването се извършва в съответствие с правилата на Регламента. В конкретния казус, още на етапа на изграждането на системите за видеонаблюдение следва да се отчетат рисковете с различна вероятност и тежест за правата на физическите лица, обект на видеонаблюдението и съответно да се въведат подходящите мерки (технически и организационни), които ще осигурят законосъобразното протичане на дейностите по обработване. По този начин ще се отговори и на изискванията на чл. 25 от Регламента – защита на данните на етапа на проектирането и по подразбиране.

В случая е важно да се отбележи, че изискванията за законосъобразно и добросъвестно обработване на лични данни в съответствие с правилата на Общия регламент за защита на личните данни важат и за обработващите лични данни, които ще обработват данни от името на администраторите на лични данни (например трети лица, които ще поддържат системите за видеонаблюдение). Ако в хода на дейностите по обработване на данните за администраторите възникне необходимост да ползват услугите на обработващ лични данни, то взаимоотношенията и отговорностите следва да бъдат уредени съобразно разпоредбите на чл. 28 от Регламент (ЕС) 2016/679.

Важно задължение за администраторите е въведено с чл. 30 от Регламент (ЕС) 2016/679, съгласно който всеки администратор е длъжен да поддържа регистър на дейностите по обработване, за които отговаря. В случая за целите на извършваното видеонаблюдение на определени категории лица, следва да поддържат отделен регистър „Видеонаблюдение", с изчерпателно посочената в чл. 30 от регламента информация.

Съществен момент във връзка със законосъобразното поведение на администраторите на лични данни е изпълнението на разпоредбите на чл. 12 и 13 от Регламент (ЕС) 2016/679 относно предоставяне на необходимата информация на субектите на данни, както и уведомяване на физическите лица за правата им във връзка със същия регламент. Това е необходимо да се осъществи при регламентиран ред, в който да се посочат лицата, които ще осъществяват видеонаблюдението и ще имат достъп (локален и отдалечен такъв) до видеокадрите и записите от системите за видеонаблюдение, ясното обозначаване на обхвата на заснемане и зоните, в които ще се използват техническите средства за наблюдение, както и данни за връзка с администратора.

В контекста на разглеждания казус администраторите следва да уведомят родителите/настойниците на децата и малолетните ученици, както и непълнолетните ученици чрез информационни табели, поставени на видно място, за използването на технически средства за видеонаблюдение и контрол. По този начин действията на администраторите ще бъдат съобразени и с разпоредбите на чл. 32, ал. 2 от Конституцията на Република България, които постановяват, че никой не може да бъде следен, фотографиран, филмиран, записван или подлаган на други подобни действия без неговото знание.

Във връзка с горното и на основание чл. 10, ал. 1, т. 4 от Закона за защита на личните данни, Комисията за защита на лични данни изразява следното

СТАНОВИЩЕ:

От гледна точка защита на личните данни, въвеждането на видеонаблюдение в ясли, детски градини и училища е допустимо с оглед подобряване на сигурността и прозрачността на грижите, както и решаване на възникнали конфликти при отглеждането на децата в детските заведения, а също и в училищата, както и с цел защита живота и здравето на най-уязвимата категория от обществото като цяло – децата и непълнолетните български граждани.

Едновременно с посоченото, в случая следва да се вземе предвид и обществения интерес от въвеждане на прозрачност в грижите за децата и подрастващите, тъй като въпросът за сигурността, живота и здравето на българските деца и ученици е от първостепенна важност за обществото като цяло.

В конкретния казус като нормативна законосъобразна предпоставка следва да се приложат разпоредбите на Регламент (ЕС) 2016/679 (Общ регламент за защита на личните данни – приложим от 25 май 2018 год.), както и националната уредба, действаща до 25.05 2018 год., разписана в Закона за защита на личните данни. В случая приложение може да намерят две от алтернативно изброените предпоставки за законосъобразност на обработването, разписани в чл. 6 от Регламент (ЕС) 2016/679, а именно: чл. 6, пар. 1, буква г) – обработването е необходимо, за да бъдат защитени жизнено важни интереси на субекта на данните или на друго физическо, както и чл. 6, пар. 1, буква д), предл. първо - обработването е необходимо, за изпълнение на задача от обществен интерес. В действащия Закон за защита на личните данни са валидни разпоредбите на чл. 4, ал. 1, т. 4 и т. 5.

С оглед на защита на правата на децата и учениците е недопустимо извършването на видеонаблюдение в помещения за сън, в санитарните помещения, в помещенията за почивка и лична хигиена на децата, тъй като с наличните устройства в тези помещения не се дава право на децата на уединение и запазване на личното им достойнство, както и представлява нарушение на правото на неприкосновеност на личността.

Допустимо е извършването видеонаблюдение в общите помещения и дворните пространства, което да гарантира безопасността на децата и учениците при игри, занимания и в свободното им време. Такова наблюдение е допустимо единствено да бъде приложено за местата на заниманията, ако са отделени от местата за сън и почивка, и в общите части на сградата.

Администраторите на лични данни е необходимо да отчетат задълженията и отговорностите си, произтичащи от разпоредбите на Регламент (ЕС) 2016/679, както и да съобразят действията по обработване на данните чрез видеонаблюдение с новите стандарти защита на личните данни, въведени с разпоредбите на регламента, подробно описани в мотивната част на настоящото становище.

Администраторите на лични данни задължително следва да уведомят родителите/настойниците на децата и малолетните ученици, както и непълнолетните ученици чрез информационни табели, поставени на видно място, за използването на технически средства за видеонаблюдение и контрол. По този начин действията на администраторите ще бъдат съобразени и с разпоредбите на чл. 32, ал. 2, предл. първо от Конституцията на Република България

Гласували четирима членове на КЗЛД - Цанко Цолов, Цветелин Софрониев, Мария Матева – за, Веселин Целков - против.

ЧЛЕНОВЕ:

Цанко Цолов /п/

Цветелин Софрониев /п/

Мария Матева /п/

Веселин Целков /п/

ЗАЩИТАТА НА ЛИЧНИТЕ ДАННИ КАТО ПРАВО НА ЛИЧНОСТТА И ГРАЖДАНИНА И ИСТОРИЯ НА НЕГОВОТО УТВЪРЖДАВАНЕ В ЕВРОПА И БЪЛГАРИЯ

ЦАНКО ЦОЛОВ

Член на Комисията за защита на личните данни

В качеството му на представител на българския надзорен орган по защита на данните, Цанко Цолов е член на Съвместния надзорен орган на Европол, Съвместния надзорен орган за Шенген, както и на Координационната група за надзор на Европейската система за автоматизирана идентификация на пръстови отпечатъци (Евродак).

Защита на личните данни като основно право

Член 8, параграф 1 от Хартата на основните права на Европейския съюз и член 16, параграф 1 от Договора за функционирането на Европейския съюз предвиждат, че всеки има право на защита на личните му данни. Защитата на физическите лица във връзка с обработването на лични данни е **основно право** и то е предназначено да служи на всички граждани. То трябва да бъде разглеждано във връзка с функцията му в обществото и да бъде в равновесие с другите основни права съгласно принципа на пропорционалност.

Двуполюсните отношения между гражданите и държавата са средство за защита на основните права на индивида от посегателствата на публичната власт върху неговата лична правна сфера и се реализира чрез законодателството. Държавата чрез своите държавните органи, между които най-вече съдилищата е задължена да осигури защита на накърнени основни права, както когато посегателството е от държавен орган, така и когато накърняването е от трето лице, за да се постигне спазване и осигуряване действието на гарантираните от обективното право основни права.[2]

Исторически погледнато човешките права могат да бъдат групирани в „три поколения права“ [3]:

• гражданските и политическите права - Американската декларация за независимостта (1776 г.) и особено с Декларацията за правата на човека и гражданина на Френската буржоазна революция (1879 г.), провъзгласяващи принципите за свобода, равенство, братство.

Гражданските права (право на живот, на свобода, **на лична сигурност**, на свобода от мъчение и деградиращо третиране, свобода от дискриминация, свобода на вярванията, религията и пр.) се отнасят до физическия и моралния интегритет на човека. Политическите права (правото на участие в управлението и в свободни избори, право на мирно сдружаване и обединяване, право на информация и на мнение) правят човека част от обществото, в което живее.

• икономически, социални и културни права се свързват като период на съзряване с втората половина на 19-ти и началото на 20-ти век и могат да се опишат като „неотложен призив към чувството за социална отговорност на държавата“ към нейните граждани.

Най-общо икономическите, социалните и културните права защитават правото на труд и на свободен избор на работа, на справедливо възнаграждение, на членуване в професионални съюзи, на обществено осигуряване, на подходящо жизнено равнище, на защита от глад, на здравеопазване и образование и държавите поемат отговорност за подобряването условията на живот на своите народи. Икономически права са правото на адекватен жизнен стандарт или правото на адекватна работа (труд).

• колективни или народни права – права на солидарност. Тази права се явяват „предварително условие за използването на всички други права“. От края на 20-ти век до днес (особено след края на „студената война“) правата на човека и тяхната защита са под влиянието на процеси, които надхвърлят националните граници и придобиват характеристики на наднационални. Това са явления като глобализацията, международният тероризъм и организираната престъпност, информационните и комуникационните технологии, биотехнологиите, генното инженерство, потребността от защита на околната среда, бедността, ксенофобията, расизмът и пр.

Тези права на човека се свързват със Световната конференция за околната среда в Рио де Женейро (1992 г.) и с появата на редица международни документи (Европейската конвенция за правата на човека, Европейската социална харта, Конвенцията за икономически, социални и културни права, Конвенцията за гражданските и политически права, Конвенцията за правата на детето и др.), наречени „твърди закони“, тъй като ратифицирането им задължава страните да прилагат записаните в тях решения.

Като основни права са признати 26-те човешки права и свободи от Всеобщата декларация за правата на човека (1948 г.), обединени в пет групи – граждански, икономически, политически, културни и социални.

Човешките права се свързват не само с биологичната, но и със социалната принадлежност или същност на човека, която се определя от живота му с другите. Социалните общности имат за задача да защитават правата на хората в новите условия, за което е необходима обществена власт. Човекът има право да се противопоставя на власт, която не изпълнява задълженията си по обществения договор и нарушава правата му.

С появата на държавата като социална организация „обществото сключва договор с държавата, предоставяйки ѝ управленски правомощия“. В замяна хората трябвало да получават защита на правата си като граждани. Така с появата на държавата и законите, правата на човека се узаконяват като права на гражданите (граждански права). Днес под граждански права се разбират конституционните и субективните права на гражданина на съответната държава. За пръв път „правата на човека“ и „правата на гражданина“ са разграничени във френската Декларация за правата на човека и гражданина от 1789 г.

В гражданското право се използва и понятието „права на личността“. Прието е, че правата на личността са същите права на човека, погледнати през друг ъгъл – през призмата на човека като личност, която живее в общество, разполага със социални права, осъществява социални контакти с други личности в обществото. В този процес се създават и нови лични права (право на информация, на здравословна среда на живот и пр.), които съпътстват развитието на обществата в условията на глобализация.

През 21-ви век към различните групи права се добавят и специфичните права на гражданите на Европейския съюз, отразени в Хартата на основните права на Европейския съюз (2012 г.). Те са представени в 50 члена, обединени в шест групи (достойнство, свободи, равенство, солидарност, гражданство, правосъдие). По-конкретно всяка от тези групи права включва[3]:

1. Достойнство, в което влизат: правото на човешко достойнство, което е „ненакърнимо“ и „трябва да се зачита и защитава“ (чл. 1); правото на живот (което определя неприложимостта на смъртното наказание); **правото на неприкосновеност на личността**; забрана на изтезания, наказания и унижения; забрана за робство и принудителен труд.

2. Свободи – в тази група права влизат: правото на свобода и сигурност; зачитане на личния и семейния живот; **защита на личните данни**; правото на брак и семейство; свобода на мисълта, съвестта и религията; свобода на мнение и информация; свобода на събранията и сдруженията; свобода на изкуствата и науките (в т.ч. на академична свобода); право на образование; свобода на избор на професия и право на труд; свобода на стопанска инициатива; право на собственост; право на убежище; защита при принудително отвеждане, експулсиране и екстрадиране.

3. Равенство – в тази група права влизат: равенство пред закона; право на недискриминация, културно, религиозно и езиково многообразие; равенство между мъжете и жените; права на детето (чл. 24); права на възрастните (на старите) хора; интеграция на хората с увреждания.

4. Солидарност – в тази група права влизат: право на информиране и консултиране на работещите; право на колективни преговори и действия; право на достъп до услуги за намиране на работа; право на защита при неоснователно уволнение; право на справедливи и равни условия на труд; забрана на детския труд и защита на работещите младежи; право на семеен и професионален живот; право на социална сигурност и социална помощ; закрила на здравето; достъп до услуги от „общ икономически интерес“; опазване на околната среда; защита на потребителите.

5. Гражданство – в тази група права влизат: право на гражданите да избират и да бъдат избирани в Европарламента, в общинските избори и пр.; право на добра администрация; право на достъп до документи; право на защита чрез Европейски омбудсман; право на петиции; свобода на движение и пребиваване; право на дипломатическа и консулска закрила.

6. Правосъдие – в тази група права влизат: право на ефективна правна защита и справедлив съдебен процес, презумпция за невиновност и право на защита; принципи на законност и пропорционалност на престъплението и наказанието; право на всеки да не бъде съден или наказван два пъти за едно и също престъпление.

Историята на Защита на личните данни в Европа

Можем да разграничим няколко етапа, които трасират приемането на съвременната европейска правна уредба, **утвърждаваща защитата на личните данни**

Първоначално осъзнаване на проблема и маркиране на отделни области от защитата на ниво национална държава:

- Англия – през 1361 г. създава Justices of the Peace Act - разпоредби против много любопитните хора, „peeping toms”.
- Франция –1858 г. забранява разгласяването на „частни факти”.
- Бавария – 1861 г. предвижда лишаване от свобода за телеграфист, който разкрие съдържанието на телеграма без разрешение.
- Норвежкото право от 1889 г. забранява публикуването на информация относно „частни или семейни дела”.
- Френската Декларация за правата на човека и гражданина от 1789 г.

Вторият етап е генерализиране на защитата, определянето й като основно право на личността и гражданина:

- Всеобщата декларация за правата на човека на ООН от 1948 г.
- Конвенция за защита на правата на човека и основните свободи (1950)
- 1951 г. – Договор за създаване на Европейската общност за въглища и стомана (Парижки договор) създаващ регионални институции за управление на въглища и стомана. Страни към Договора са Франция, Западна Германия, Италия, Белгия, Люксембург и Холандия.

• 1957 г. – Договор за създаване на Европейската икономическа общност (Договор от 1957 г на Рим)

• Договор от 1965 г. За създаване на единен съвет и единна комисия на Европейските общности (Договор за сливане). Създава общия пазар, Европейската комисия, Съвета на министрите, Европейския съд на Правосъдието и Европейския парламент.

• 1970 г. – провинция Хесен (Германия) въвежда първия съвременен регионален закон

• 1973 г. – първият национален закон за неприкосновеност на личния живот е приет в Швеция

Това е времето на създаване на система от правила и норми, насочени към определяне предмета и обхвата на защитата на личните данни.

Отправна точка за изготвяне на стандарти в законодателството за защита на лицата е **Всеобщата декларация за правата на човека** (наричана още Декларация за правата на човека), приета на 10 декември 1948 г. от Общото събрание на Организацията на обединените нации. Декларацията прокламира всеобщи ценности и традиции, признаващи „присъщото достойнство и равните и неотменими права на всички членовете на човешката раса на основата на свободата, справедливостта и мира в света“. За първи път правото на защита на личния живот е предвидено в международен правен акт, като се визира защита от други субекти или държавата.

Декларацията за правата на човека съдържа конкретни разпоредби във връзка с правото на личен и семеен живот и свободата на изразяване независимо от границите. Принципите, залегнали в Декларацията за правата на човека, са основа за всички следващи европейски закони и стандарти за защита на данните.

Правото на личен живот и свързаните с него свободи се съдържа в член 12 от Декларация за правата на човека, която гласи: „Никой не трябва да бъде подлаган на произволна намеса в личния му живот, семейството, жилището и кореспонденцията, нито на посегателства върху неговата чест и добро име. Всеки човек има право на закрила от закона срещу подобна намеса или посегателства.“

Никой не може да бъде подложен на произволна намеса в неприкосновеността на личния живот, семейството, дома или кореспонденцията, нито да бъде атакувана неговата чест и репутация. Всеки има право на защита от закона срещу такава намеса или нападение.

Друг основен аспект в Декларацията за правата на човека е правото на свобода, изразено в член 19. Всеки има право на свобода на мнение и изразяване, като това право включва и търсене, получаване и разпространяване на информация и идеи чрез всякакви медии и независимо от границите.

Съветът на Европа, създаден след края на Втората световна война (1950г.) в Рим, приема **Конвенция за защита правата на човека и основните свободи (ЕКПЧ)**, която влиза в сила през 1953 г. Тя се прилага само за държавите-членки и е „затворен инструмент“. Всички държави привеждат в действие конвенцията в своето национално законодателство, а от всеки нов член се очаква да я ратифицира при първа възможност. Страните се задължават да предоставят права и свободи на всички в рамките на своята юрисдикция.

Правото за защита на личните данни е част от правата, съгласно чл.8 от ЕКПЧ, като се допускат и ограничения на това право. Всеки има право на зачитане на неговия личен и семеен живот, на неговото жилище и тайната на неговата кореспонденция. Намесата на държавните власти в ползването на това право е недопустима, освен в случаите, предвидени в закон, при необходимост и в интерес на националната и обществената сигурност или на икономическото благосъстояние на страната, за предотвратяване на безредици или престъпления, за защита на здравето и морала или на правата и свободите на другите.

За да се гарантира спазването на правилата от Конвенцията през 1959 г. е създаден Европейски съд по правата на човека в Страсбург. Решенията на Европейския съд по правата на човека са задължителни за държавите и може да доведат до изменение на тяхното законодателство или промяна

в практиката за правораздаване. По искане на Комитета на министрите на Съвета на Европа, Съдът по правата на човека може да дава консултативни становища и тълкувания.

ЕКПЧ е мощен инструмент поради обхвата на основните права и свободите, които прокламира. Тя включва правото на живот, забрана на изтезанията, забрана на робство и принудителен труд, правото на свобода и сигурност, правото на справедлив съдебен процес, наказание без закон, уважение към личния и семейния живот, свобода на мисълта, съвестта и религията, свобода на изразяване, свобода на събранията и сдружаването, право на сключване на брак, право на ефективно средство за защита и забрана на дискриминацията

На този етап прокламираните всеобщи ценности и традиции намират изражение в първите национални закони. Закони, основани на общи принципи, но достатъчно различни, утвърждавайки националната идентичност на отделните държави.

Третият етап е белязан от набиращите сила информационни технологии и нарастващата необходимост от по-детайлни правила за защита на физическите лица чрез защита на техните (лични) данни. До средата на 70-те години на XX в. , Комитетът на министрите на Съвета на Европа приема различни резолюции относно защитата на личните данни, позовавайки се на член 8 от ЕКПЧ. [4]

• 1973-1974 г. – Решения 73/22 и 74/29 за установяване на принципи за защитата на личните данни в автоматизирани бази данни в частния и обществения сектор;

• 1979 г. – Общи закони за защита на данните са приети в седем държави-членки (Австрия, Дания, Франция, Федерална република Германия, Люксембург, Норвегия и Швеция), а в три европейски държави, Испания, Португалия и Австрия, защитата на данните е включена като основно право в Конституцията;

• 1980 г. – Насоки за защита при трансгранични потоци на лични данни;

• Конвенция на Съвета на Европа от 1981 г. за защита на лицата по отношение на Автоматичната обработка на лични данни (Конвенция 108) ;

• 1986 г. – Единният европейски акт, изменящ предишните договори и създаващ „Вътрешен пазар“ (в сила от 1992 г.) и водещ до единна валута и край на граничното регулиране;

• 1992 г. – Договорът за Европейския съюз (Договорът от Маастрихт) учреди Европейския съюз Съюз (ЕС);

• 1995 г. – Директива 95/46/ЕО за защита на лицата по отношение на обработката на лични данни и свободното движение на такива данни;

• 2000 г. – Директива 2000/31/ЕС относно някои правни аспекти на информационното общество и услуги, по-специално електронната търговия на вътрешния пазар (Директива относно електронната търговия) или Директивата за електронната търговия;

• 2000 г. – Хартата на основните права на Европейския съюз - допълнително се консолидират основните права, приложими в ЕС, включва общите принципи, изложени в ЕКПЧ, но се отнася по-конкретно към защитата на личните данни;

• 2001 г. – Допълнителен протокол към Конвенцията за защита на лицата по отношение на Автоматичната обработка на лични данни по отношение на надзорните органи властите и трансграничните потоци от данни са разработени, за да се справят с фактът, че Конвенция 108 не предвижда прехвърляне на лична информация към държави, които не са я подписали. Въвежда концепцията за адекватно (а не еквивалентно) ниво на защита за държави, които не са членки на ЕС;

• 2002 г. – Директива 2002/58/ЕО относно обработката на лични данни и защита на неприкосновеността на личния живот в сектора на електронните комуникации. Разглежда правото

на неприкосновеност на личния живот и електронните съобщения (електронната поверителност). Директивата се занимава с регулирането на редица важни въпроси като поверителността на информация, обработка на данни за трафик, спам и „бисквитки“.

• 2006 г. – Директива 2006/24/ЕО относно запазването на трафични данни при предоставяне на обществено достъпни електронни съобщителни услуги или на обществени съобщителни мрежи;

• 2007 г. – Договорът от Лисабон, предназначен за укрепване и подобряване на основните структури на Европейския съюз, за по-ефективно функциониране. Договорът създава институцията на европейски надзорник за защита на данните на ниво Европейски съюз;

• 2009 г. – Директива 2009/136/ЕО за изменение на Директива 2002/22/ЕО относно универсалната услуга и правата на потребителите, свързани с електронните съобщителни мрежи и услуги, Директива2002/58/ЕО относно обработката на лични данни данните и защитата на неприкосновеността на личния живот в сектора на електронните комуникации и Регламент (ЕО) № 2006/2004 относно сътрудничеството между националните органи органите, отговарящи за прилагането на законите за защита на потребителите.

През 1981г. беше открита за подписване Конвенция за защита на лицата при автоматизираната обработка на лични данни (Конвенция № 108). Конвенцията беше и все още продължава да бъде единственият правно обвързващ международен инструмент в областта на защитата на данните.

Конвенцията се прилага за цялостната обработка на данни, извършена в частния и публичния сектор, както и обработката на данни от съдебни и правоприлагащи органи. Тя защитава лицето срещу злоупотреби, които могат да съпровождат събирането и обработването на личните данни, и едновременно с това има за цел да уреди трансграничното предоставяне на лични данни. По отношение на събирането и обработването на лични данни, установените в конвенцията принципи се отнасят по-специално до добросъвестното и законосъобразното събиране и автоматично обработване на данни, съхранявани за определени законни цели, забрана за използване за други несъвместими с тях цели, както и да се съхраняват за по-дълъг срок, отколкото е необходимо. Разглежда се качеството на данните, тяхната достатъчност, релевантност, точност и прекомерност спрямо целта.

В допълнение са предоставени гаранции по отношение на събирането и обработването на лични данни, като забранява при липсата на подходящи правни гаранции, обработването на „чувствителни“ данни (визирани като данни относно раса, политически възгледи, здравословно състояние, религията, сексуален живот или съдебно досие на дадено лице).

Конвенцията също така утвърждава правото на лицето да бъде осведомено, че за него се съхранява информация и при необходимост, да поиска нейното коригиране. Ограниченията на правата, предвидени в конвенцията, са възможни само когато са застрашени първостепенни интереси като например държавната сигурност или отбраната.

Въпреки че конвенцията гарантира свободния обмен на лични данни между държавите - страни по нея, тя налага някои ограничения върху движението на тези данни към държави, в които правната уредба не предоставя адекватна защита.

Всички държави членки на ЕС са ратифицирали Конвенция № 108. През 1999 г. Конвенцията е изменена, за да може ЕС да стане страна по нея. През 2001 г. беше приет Допълнителен протокол към Конвенция № 108, с който бяха въведени разпоредби относно трансграничните потоци от данни към държави, които не са страни по конвенцията, така наречените трети държави, както и относно задължителното създаване на национални надзорни органи за защита на данните.

До 2016 г. основният правен инструмент на ЕС за защита на данните е **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 (Директива за защита на личните данни). Към годината на нейното приемане, няколко държави членки вече бяха приели национални закони за защита на данните. Свободното движение на стоки, капитали, услуги и хора в рамките на вътрешния пазар изискваше наличието на свободно движение на данни, което можеше да бъде осъществено само ако държавите членки можеха да разчитат на еднакво ниво на защита на данните.

Тъй като целта на приемането на Директивата за защита на личните данни беше хармонизирането на правото за защита на данните на национално равнище, Директивата позволява известна степен на специфичност, съпоставима с тази на (тогава) съществуващите национални закони за защита на данните. Директива 95/46/ЕО е създадена с цел гарантиране, че нивото на защита на правата и свободите на лицата по отношение на обработката на личните им данни е еквивалентна във всички страни членки. Сближаването на приложимите национални законодателства в тази област не трябва да води до отслабване на защитата, а обратно, да се стреми към осигуряването на високо ниво на защита в ЕС. Съответно хармонизацията на тези национални законодателства не се ограничава до минимално изискваната, а до възможно най-всеобхватната. В резултат на това, държавите членки имат само ограничена свобода на действие при прилагането на директивата. Директивата за защита на личните данни е предназначена да придаде съдържание на принципите на правото на неприкосновеност на личния живот, които вече се съдържат в Конвенция № 108, както и да ги разшири. Фактът, че всички 15 държави членки на ЕС, през 1995г. са били също и договарящи се страни по Конвенция № 108, изключва възможността за приемането на противоречиви правила в тези два правни инструмента.

Директивата за защита на личните данни обаче се основава на възможността, предвидена в член 11 от Конвенция № 108, за добавяне на инструменти за защита. По-специално въвеждането на независимия надзор като инструмент за подобряване на съответствието с правилата за защита на данните се оказа важен принос за ефективното функциониране на европейското право в областта на защитата на данните.

Териториалното прилагане на Директивата за защита на личните данни се простира отвъд 28-те държави членки на ЕС, включително и в държавите, които не са членки на ЕС, но са част от Европейското икономическо пространство (ЕИП), а именно Исландия, Лихтенщайн и Норвегия.

Съдът на Европейския съюз в Люксембург е компетентен да определя дали дадена държава членка е изпълнила своите задължения съгласно Директивата за защита на личните данни и да дава преюдициални заключения относно валидността и тълкуването на директивата, за да се гарантира нейното ефективно и еднакво прилагане в държавите членки. Важно изключение във връзка с прилагането на Директивата за защита на личните данни е т. нар. изключение за домашни дейности, а именно обработването на лични данни от физически лица само за „лични или домашни нужди“. Това обработване обикновено се разглежда като част от свободите на съответното физическо лице.

В съответствие с първичното право на ЕС, което е било в сила по време на приемането на Директивата за защита на личните данни, материалният обхват на директивата е ограничен до въпроси, свързани с вътрешния пазар. Най-важните въпроси, останали извън нейното приложно поле, са въпросите, свързани с полицейското сътрудничество и сътрудничеството в областта на наказателното правосъдие.

Тъй като Директивата за защита на личните данни е адресирана само до държавите членки на ЕС, е необходим допълнителен правен инструмент, за да се въведе защита при обработването на лични данни от институциите и органите на ЕС. Регламент (ЕО) № 45/2001 относно защитата на лицата по отношение на обработката на лични данни от институции и органи на Общността и за свободното движение на такива данни (Регламент относно защитата на данните при обработването им от институции на ЕС) изпълнява тази задача.

Освен това, дори и в области, обхванати от Директивата за защита на личните данни, често са необходими по-подробни разпоредби за защита на данните, за да се постигне необходимата яснота

по отношение на балансирането на другите законни интереси. Примери за това са Директива 2002/58/ЕО относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации (Директива за правото на неприкосновеност на личния живот и електронни комуникации) и Директива 2006/24/ЕО за запазване на данни, създадени или обработени, във връзка с предоставянето на обществено достъпни електронни съобщителни услуги или на обществени съобщителни мрежи и за изменение на Директива 2002/58/ЕО. [1]

Първоначалните договори на Европейските общности не съдържат никакво посочване на правата на човека или на тяхната защита. Когато обаче в тогавашния Съд на Европейските общности бяха заведени дела за предполагаеми нарушения на правата на човека в области, попадащи в обхвата на правото на ЕС, Съдът разработи нов подход. За да предостави защита на физическите лица, той включи основните права в така наречените общи принципи на европейското право. Съгласно Съдът на Европейския съюз тези общи принципи отразяват съдържанието на защитата на правата на човека, установена в националните конституции и договорите за правата на човека, по-специално в ЕКПЧ. Съдът на ЕС заяви, че ще гарантира съответствието на правото на ЕС с тези принципи.

Признавайки, че неговите политики биха могли да окажат въздействие върху правата на човека и за да се чувстват гражданите по-свързани с ЕС, през 2000 г., ЕС провъзгласи **Хартата на основните права на Европейския съюз**. Тази харта включва целия спектър от граждански, политически, икономически и социални права на европейските граждани, като излага в синтезиран вид общите за държавите членки конституционни традиции и международни задължения. Въпреки че първоначално бе само политически документ, с влизането в сила на Договора от Лисабон на 1 декември 2009г., Хартата придоби правно обвързващ характер като първично право на ЕС (член 6 , параграф 1 от Договора за Европейския съюз).

Първичното право на ЕС също така съдържа обща компетентност на ЕС да приема законодателни актове по въпроси, свързани със защитата на данните (член 16 от Договора за функциониране на Европейския съюз) .

Хартата не само гарантира зачитането на личния и семейния живот (член 7), но също така установява правото на защита на личните данни (член 8), като изрично издига тази защита до това на основно право. Институциите на ЕС, както и държавите членки, трябва да спазват и да гарантират това право, което се отнася и за държавите членки, когато те прилагат правото на Съюза (член 51 от Хартата). Формулиран няколко години след приемането на Директивата за защита на личните данни, член 8 от Хартата трябва да се тълкува като израз на съществуващото преди това право на ЕС в областта на защитата на данните. Поради това в Хартата не само изрично се указва правото на защита на данните в член 8 , параграф 1, но също така се посочват основните принципи за защита на данните в член 8 , параграф 2 . Накрая, в член 8 , параграф 3 от Хартата се гарантира, че прилагането на тези принципи ще подлежи на контрол от независим орган.

Договорът от Лисабон (2007 г.), известен като Договор за изменение на Договора за Европейския съюз и на Договора за създаване на Европейската общност, разширява процедурите на съвместно вземане на решения в областта на полицейско и съдебно сътрудничество при наказателни дела, дава по-големи права на националните парламенти в законодателството на ЕС, въвеждането на Инициатива на европейските граждани, увеличаване на компетенциите на Върховния представител за външна политика и политика на сигурност, като всичко това е обвързано с „Хартата на основните права“.

Преди влизането в сила на Лисабонския договор, законодателството в областта на свободата, сигурността и правосъдието бе разделено между защита на данните за лична или търговска цел, и защита на данните за целите на прилагане на закона, на междуправителствено равнище. Оттук и процесът на взимане на решения следваше два различни набора от правила. Различията в структурата изчезна с Договора от Лисабон, което предоставя по-здрава основа за развитието на по-ясна и по-ефективна система за защита на данните, като същевременно предвижда нови правомощия за Европейския парламент , който става съвместен законодател. Член 16 от ДФЕС постановява, че Парламентът и Съветът установяват правилата във връзка със защитата на физическите лица при

обработването на лични данни от институциите, органите, службите и агенциите на ЕС, както и от държавите членки при извършването на дейности, които са в приложното поле на правото на ЕС. [1].

Последните две декади са белязани с все по силна и ангажирана позиция на Европейския Парламент в сферата на защитата на личните данни. Той прие различни решения по тези чувствителни въпроси, във връзка с етническото и расово профилиране, Решението на Съвета от Прюм за трансграничното сътрудничество в борбата срещу тероризма и трансграничната престъпност, използването на телесни скенери за увеличаване на сигурността на въздухоплаването, биометричните данни в паспортите и общите консулски инструкции, управлението на границите, интернет и извличането на данни.

Използвайки своите правомощия, през февруари 2010г. Парламентът отхвърли временното прилагане на Споразумението за проследяване на финансирането на тероризма (ППФТ) (известно преди като Споразумение SWIFT) относно предаването на банкови данни на САЩ за целите на борбата с тероризма. През юли 2011г. Комисията прие съобщение относно основните възможни варианти за създаване на Европейска система за проследяване на финансирането на тероризма (СПФТ на ЕС) , във връзка с което Парламентът изрази някои съмнения. През ноември 2013г. Комисията обяви намерението си да не представя предложение за СПФТ на този етап.

Друг въпрос от решаващо значение за защитата на данните е споразумението относно резервационните данни на пътниците (PNR) между ЕС и Съединените щати за обработването и предаването на такива данни от въздушните превозвачи към Министерството на вътрешната сигурност на САЩ. След одобрението на Парламента, получено на 19 април 2012г. , Съветът прие на 26 април 2012г. решение за сключване на новото споразумение, което замести (от юли 2012г.) временно действащото от 2007г. споразумение между ЕС и САЩ за резервационните данни на пътниците.

През февруари 2011г. Комисията внесе Предложение за директива относно използването на резервационни данни на пътниците за предотвратяване, разкриване, разследване и наказателно преследване на престъпления, свързани с тероризъм, и на тежки престъпления (EUPNR) .

Парламентът участва в процеса по одобрението (съгласно съответната процедура) на правно обвързващо рамково споразумение със Съединените щати за обмена на информация и защитата на данните. Целта е да се осигури високо равнище на защита наличната информация, като данните на пътниците или финансовата информация, които се предават в рамките на трансатлантическото сътрудничество в борбата срещу тероризма и организираната престъпност.

На 12 март 2014г. Парламентът прие резолюция относно програмата за наблюдение на Агенцията за национална сигурност на САЩ, органите за наблюдение в различните държави членки и тяхното отражение върху основните права на гражданите на ЕС и върху трансантлантическото сътрудничество в областта на правосъдието и вътрешните работи. С тази резолюция приключи 6-месечното проучване на Парламента относно електронното масово наблюдение на гражданите на ЕС, последвало разкритията от юни 2013г. за предполагаемо шпиониране от страна на САЩ и някои държави – членки на ЕС. В своята резолюция Парламентът призова за прекратяване на прилагането на принципите за неприкосновеност на личния живот („Safe Harbour“ - доброволни стандарти за защита на данните за дружества извън Европейския съюз, които прехвърлят лични данни на граждани на ЕС в САЩ) и на Програмата за проследяване на финансирането на тероризма.

Четвъртият етап от развитието на законодателството в сферата на защитата на личните данни е доминиран от глобализацията и цифровата икономика. Защита на неприкосновеността, ограничена в национални или европейски граници, не е достатъчна. Промени се разбирането за стойността на защитата на личните данни - от изграждане на чувство на лична сигурност се превърна в стратегическо предимство при правеното на бизнес. Доверието на клиента в компанията - доставчик на услуга, стана водещо при персоналния избор.

На 6 юли 2011 г. Парламентът прие резолюция относно всеобхватен подход за защита на личните данни в Европейския съюз. На 25 януари 2012 г. Комисията публикува широкообхватен законодателен пакет за реформа на законодателството на ЕС за защитата на данните. Предложената реформа е насочена към гарантиране сигурността на личните данни в целия ЕС, увеличаване на контрола на ползвателите върху техните собствени данни и намаляване на разходите за предприятията, а през октомври същата година организира междупарламентарно заседание на комисии съвместно с националните парламенти на тема „Реформа на рамката на ЕС за защита на данните“. Утвърди се пакетен подход, с успоредни действия по предложенията на Комисията за общ регламент за защита на данните и директива в сектора на правоприлагането.

На 12 март 2014 г. Парламентът гласува на първо четене реформата, за по- добри гаранции на лицата, подобряване възможностите за стопанска дейност и създаване на силна система за оценяване на съответствието и на 27 април 2016г. е окончателно одобрен като Регламент 2016/679. Като част от пакета документи е приета и Директива 2016/680 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.

Регламент 769/2016 г. 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) е правно обвързващ документ, променящ глобално условията на играта в световен мащаб.

Технологичният напредък и глобализацията промениха начините, по които се събират и използват данните, както и достъпа до тях. Към момента на приемането 28-те държави членки прилагат правилата от 1995 г. по различен начин, въведен от транспонирането на Директива 95/46 в техните национални законодателства. Единното право премахва съществуващата към този момент фрагментация и високите административни разходи. Регламентът търси укрепване на доверието на потребителите в онлайн услугите и даване на така необходимия тласък на растежа, заетостта и иновациите в Европа. В анонсирания пакет освен предложение за общ регламент за осъвременяване на принципите за защита на данните, е включено и предложение за специфична директива относно обработването на личните данни в областта на полицейското и съдебно сътрудничество по наказателно-правни въпроси и доклад за прилагането на Рамковата директива от 2008 г. [1]

Може би най-значимата промяна, въведена от Регламента е обхвата на действие – доста просто, но перфектно като норма е посочено, че всеки, който обработва данни за граждани на Европейския съюз, следва да го спазва.

Макар и не изчерпателно, но Регламента разширява понятието за лични данни, добавяйки IP адрес, геолокация и позиционира биометричните данни като специални лични данни.

Въвежда нов принцип при обработката „отчетност“ с акцент върху прозрачността на процеса и най-важното - изграждане на доверие от страна на компаниите към клиенти и партньори.

До голяма степен контролът върху обработката на данните е превърнат в права на субектите. Последните получават пълен достъп до данните си, условията на тяхната обработка и имат механизми, с които могат да наблюдават обработката и дори да я управляват.

Акцент върху даване на изрично съгласие за обработка на лични данни, но и ясно разписани правила на възможността за неговото оттегляне по всяко време. В допълнение, трябва да бъде дадено пълно обяснение за целта на събирането на данни, както и намеренията за използването и предоставянето им, с възможност за отказ от страна на субекта на данни.

Задълженията на администратора на лични данни са степенувани на основа оценка на риска, възникващ при обработката на личните данни. Защитата се превръща в процес от анализирани заплахи и оценено бъдещо въздействие на операциите по обработката.

В чисто административен аспект Регламентът въвежда завишен надзор и санкции, но и възможност за бизнеса за по лесна комуникация с надзорните органи. Въвеждането на принципа за обработка на едно гише позволява на администратора на лични данни, договаряйки се с един надзорен орган на една от страните членки, да се договори с целия Европейски съюз.

Познатите механизми за сертифициране, маркиране и кодекси на поведение освен средство за демонстрация на съответствие с Регламента се превръщат в мощен механизъм за трансфер на данни към трети страни, дори и извън Европейския съюз.

За първи път са разписани като норма технически и организационни мерки за защита на данните при изграждане на информационни системи – защита по подразбиране, защита при проектирането, псевдоанонимизация и т.н.

Право и задължение на информираност при пробив – потребителите трябва бъдат информирани до 72 часа за изтичането на каквато и да било лична информация. Като този срок се определя на администратора с презумпцията за максимално бързо минимизиране на последствията от пробива или за неговото отстраняване.

Защитата на личните данни в България.

На национално ниво развитието на нормативната уредба за защита на личните данни следва обичайния път, като осезаем тласък получава при синхронизиране на законодателството ни с общоевропейските норми.

Приетата през 1948 г. Всеобща декларация на правата на човека е препоръчана като задължителна за всички членове на организацията на Обединените нации и днес тя е съставна част от обичайното международно право. По силата на членството си в организацията (България е член на ООН от 1955г.) Народното събрание на Република България приема декларация, в която заявява своята категорична подкрепа. Конституционният съд на Република България приема Конвенция за защита на правата на човека и основните свободи. Всеобщата декларация се посочва в редица документи на български институции, включително и от омбудсмана на Република България в неговото становище относно участието на българските граждани с двойно гражданство в управлението на страната.

Конвенцията за защита правата на човека и основните свободи е правен инструмент на Съвета на Европа и влиза в сила от 1953 г. за страните учредителки, като новите държави членки се задължават да я подпишат до една година от присъединяването си. България ратифицира със закон Конвенцията през юли 1992 година.

В Конституция на Република България са записани основните права на гражданите. Според нея тези основни права са правото: на гражданство, на убежище, на живот, **на лична свобода и неприкосновеност**, на адвокатска защита при необходимост, на личен живот и неприкосновеност, на избор на местожителство, на изучаване и ползване на български език, както и на майчиния език, на свобода на съвестта, свободата на мисълта и изборът на вероизповедание, на мнение, на информация, да участват в избори, на мирни събрания, стачки, манифестации, на сдружаване, на брак и семейство, на жалби, на труд при здравословни и безопасни условия и при съответно трудово възнаграждение и заплащане, на обществено и на здравно осигуряване и социално подпомагане, на здравеопазване и образование, на ползване на националните и общочовешките културни ценности, както и правото на човека да развива своята култура, на здравословна и благоприятна околна среда, на защита, когато са нарушени или застрашени негови права или законни интереси (Конституция на Република България, 1991, изм.2007).

Като най-основното от всички права се признава правото на живот, „защото само ако човекът е жив, може да упражнява останалите права и свободи“. Правото на лична свобода /чл.30/ е основно лично право и негово производно право е: Правото на зачитане на личния и семеен живот /чл.32, ал.1/. Неприкосновеността на личния живот е защитена чрез забрана за следене, фотографиране,

филмиране, записване или други подобни действия без знание или въпреки изричното несъгласие на лицето / чл.32, ал.2/. Друга гаранция за защита на правото на личен живот е неприкосновеността на жилището /чл.33, ал.1, изр.1/. Конституцията чрез /чл.34/ обявени за неприкосновени свободата и тайната на кореспонденцията и на другите съобщения

От 01.01.2002 г. в Република България е в сила Закон за защита на личните данни, чиято цел е гарантиране на неприкосновеността на личността и личния живот, чрез осигуряване на защита на физическите лица при неправомерно обработване на свързаните с тях лични данни в процеса на свободното движение на данните - чл.1, ал.2 от ЗЗЛД.

Съобразно този закон, всяко физическо лице има право на достъп до отнасящи се за него данни, като производни на това му право са правото да получи информация за категориите лични данни които се обработват за него, получателите на данните, съдържанието на данните, а така също физическото лице има право да поиска заличаване, коригиране или блокиране на данни, обработването на които не отговаря на изискванията на закона. Със закона се предвижда и възможност за достъп на трето лице до лични данни на друг субект, като са регламентирани предпоставките и механизмът за това. Съдържа механизъм за защита на физическите лица при нарушаване на правата им по него.

Създаден е независим, специализиран държавен орган - Комисията за защита на личните данни, чиято основна функция е защита на лицата при обработването на техните лични данни и при осъществяването на достъпа до тези данни, както и контрол по спазването на закона.

Като процесуална гаранция за спазване правото на защита на личните данни е предвидената възможност за съдебно обжалване на решенията на Комисията за защита на личните данни пред Върховния административен съд или директно обжалване на актовете на администраторите на лични данни пред съответните административни съдилища.

Чрез произнасянето си по жалби срещу решенията на Комисията за защита на личните данни, Върховният административен съд осъществява контрол за спазването на правото на защита на личния живот и личността на гражданите чрез недопускане на неправомерно обработване на свързаните с тях лични данни.

В Закона за адвокатурата /чл.33/, Закона за здравето /чл.27/, Закона за радиото и телевизията /чл.2/; Закона за държавния служител /чл.17 [2] също се съдържат, правни гаранции за защита на личните данни.

Литература

[1] Справочник за Европейския съюз - 2014

[2] Съдебно прилагане на основните права

[3] Годишник Софийски университет том 109, Правата на човека като социално завоевание на човечеството и социална отговорност на гражданите и правителствата, Вяра Гюрова

[4] Origins and historical content of data protection law

Комисия за защита на личните данни
Председател: Венцислав Караджов
Членове: Цанко Цолов
Цветелин Софрониев
Мария Матева
Веселин Целков

Информационен бюлетин № 3 (72) 2018 г.
Издава се съгласно чл. 10, ал. 3 от ЗЗЛД
Отговорник на броя: Надежда Борисова

Разпространява се в електронен вид

ISSN 2367-7759