РАБОТНА ГРУПА ЗА ЗАЩИТА ЗА ЛИЧНИТЕ ДАННИ ПО ЧЛЕН 29

16/BG
WP 243 rev.01

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

Приети на 13 декември 2016 г.

Последно преразгледани и приети на 5 април 2017 г.

Тази Работна група е създадена в съответствие с член 29 от Директива 95/46/ЕО. Тя е независим европейски консултативен орган за защита на личните данни и неприкосновеността на личния живот. Нейните задачи са описани в член 30 от Директива 95/46/ЕО и член 15 от Директива 2002/58/ЕО.

Секретариатът се осигурява от Дирекция C (Основни права и върховенство на закона) на Генерална дирекция „Правосъдие и потребители“ на Европейската комисия, B-1049 Brussels, Belgium, Office No MO59 05/35.

Уебсайт: http://ec.europa.eu/justice/data-protection/index_en.htm

РАБОТНАТА ГРУПА ЗА ЗАЩИТА НА ЛИЦАТА ПРИ ОБРАБОТВАНЕТО НА ЛИЧНИ ДАННИ

създадена по Директива 95/46/ЕО на Европейския парламент и на Съвета от 24 октомври 1995 г.,

като взе предвид членове 29 и 30 от нея,

като взе предвид Правилника за дейността си,

ПРИЕ НАСТОЯЩИТЕ НАСОКИ:

Съдържание

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

[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.

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 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].

[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“*.

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]

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,

---

[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.

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.

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

[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).

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.

[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 *„[о]бработването 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.

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;
- 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.

[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.

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 СПЕЦИАЛНИ КАТЕГОРИИ ДАННИ И ДАННИ, СВЪРЗАНИ С ПРИСЪДИ И НАРУШЕНИЯ

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 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:

[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.

- 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

[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*

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.

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

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“*.

[25] Вж. член 3 от ОРЗД относно териториалния обхват.

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.

- **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

[26] Глава II.
[27] Глава III.
[28] Член 25.
[29] Член 30.
[30] Член 32.
[31] Членове 33 и 34.

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 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).

[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.

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.

[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

[34] Член 5, параграф 2.

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.

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“*.

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

---

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 *„[к]ато 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“*.

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 отгов[а]ря“* 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.

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

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, 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 свързват 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 организацията;
- способност за насърчаване на културата на защита на данните в рамките на организацията.

Източник: член 37, параграф 5 от ОРЗД

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 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 на 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

Съставено в Брюксел
на 13 декември 2016 година.

За Работната група
Председател

Isabelle FALQUE-PIERROTIN

Последно преразгледано и прието на 5 април 2017 г.

За Работната група
Председател

Isabelle FALQUE-PIERROTIN