Дайджест "Собственост и право", 2017 г., кн. 10, стр. 74 и сл.

ДЛЪЖНОСТНО ЛИЦЕ ПО ЗАЩИТА НА ДАННИТЕ ОПРЕДЕЛЯНЕ, СТАТУТ И ЗАДАЧИ

Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 24 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните) /ОРЗД, Регламентът/ урежда изискванията и задачите на длъжностното лице по защита на данните. Те се прилагат независимо от обстоятелството дали длъжностното лице по защита на данните е определено в изпълнение на задължение на администратора или обработващия данните или доброволно по тяхна преценка.

1. Определяне на длъжностно лице по защита на данните

1.1. Изисквания

1.1.1. Професионални качества

В чл. 37, пар. 5 от ОРЗД е предвидено, че „длъжностното лице по защита на данните се определя въз основа на неговите професионални качества, и по-специално въз основа на експертните му познания в областта на законодателството…“. Съображение 97 на Регламента пояснява, че необходимото ниво на експертни познания следва да се определи в съответствие с извършваните операции по обработване на данни и защитата, която е необходима за тях. Подходът да не се фиксира конкретно ниво на експертиза, а да се поставя в зависимост от чувствителността, сложността и количеството данни, които се обработват, заслужава подкрепа. Администраторите и обработващите данни трябва определят лицето не въз основа на формални критерии, а като отчитат предизвикателствата, които обработваните лични данни поставят пред тях. Наред с това трябва да подберат лице, което има познания в областта на законодателството и практиките за защитата на личните данни.

В Насоките за длъжностните лица по защита на данните[1], приети от Работната група по чл. 29[2], са откроени важни практически изисквания към професионалните качества на тези лица. Те са свързани с познаване на сектора и организацията на администратора, както и разбиране на операциите по обработка, информационните системи, сигурността на данните и необходимостта от тяхната защита. При дейността на публичните органи е препоръчително и добро познаване на административните правила и процедури, които се прилагат от администратора.

Основните минимални изисквания, на които трябва да отговаря длъжностното лице по защита на данните в структурата на администратори или обработващи от държавната администрация, са посочени изрично в Класификатора на длъжностите в

[1] Guidelines on Data Protection Officers (‘DPOs’) 16/EN WP 243 rev.01, приети на 13 декември 2016, последно ревизирани на 5 април 2017

[2] Работната група е създадена въз основа на чл. 29 от Директива 95/46/ЕО на Европейския парламент и на Съвета от 24 октомври 1995 година за защита на физическите лица при обработването на лични данни и за свободното движение на тези данни. Тя има съвещателен статут и действа независимо, а съставът й обхваща представители на надзорните органи на държавите членки, представители на органите по надзор на институциите на ЕС и представител на Европейската комисия.

администрацията[3] – редове 109а, 111а, 178а и 262а. Предвидени са изисквания за образователна степен, ранг и професионалния опит, които лицето трябва да притежава.

1.1.2. Способност за изпълнение на задачите

Длъжностното лице по защита на данните играе ключова роля в насърчаването на културата по защита на данните в рамките на организацията. Поради това, наред с професионалните качества, ОРЗД поставя като кумулативно изискване „способността му да изпълнява задачите, посочени в чл. 39“ (чл. 37, пар. 5). Според Работната група по чл. 29 тази способност трябва да се тълкува като отнасяща се до личните качества и знания на лицето, като се изисква почтеност и висока професионална етика. Способността за изпълнение на задачите се разглежда и в друг аспект, като се отчита позицията на длъжностното лице по защита на данните в структурата на администратора.

1.2. Правни възможности при определяне на длъжностно лице по защита на данните

Дори в случаите, в които изисква задължително определяне на длъжностно лице по защита на данните, ОРЗД открива широки възможности на администраторите и обработващите. Според чл. 37, пар. 6 длъжностното лице по защита на данните може да бъде член на персонала или да изпълнява задачите си въз основа на договор за услуги с администратора или обработващия.

В случай, че длъжностното лице по защита на данните е член на персонала, то може да изпълнява и други задачи и задължения (по аргумент от чл. 38, пар. 6), стига те да не водят до конфликт на интереси. Няма съмнение, че възлагането на задачите на длъжностно лице по защита на данните на служител на администратора или на обработващия, трябва да бъде съобразена с изискванията на трудовото законодателство[4], както и на законодателството за държавните служители. Например възлагането на допълнителни функции може да стане с промени в длъжностната характеристика, но в този случай те трябва да бъдат свързани по характер с изпълняваната от служителя длъжност, а по обем не трябва да надхвърлят възможностите за изпълнение на задачите в рамките на работното време. Ако възлаганите функции са извън кръга на трудовите задължения на служителя, по-удачно би било да се приложат правилата за допълнителен труд при същия работодател.

1.3. Съвместно определяне на длъжностно лице по защита на данните

Регламентът допуска група предприятия (контролиращо предприятие и контролираните от него предприятия) да определят едно длъжностно лице по защита на данните. Условието е всяко предприятие да има „лесен достъп“ до длъжностното лице по защита на данните. Според Работната група по чл. 29 достъпността се отнася до задачите на длъжностното лице като точка за контакт на субектите на данни и надзорния орган, но също и в рамките на организацията, като се има предвид, че една от задачите му е да информира и съветва администратора или обработващия и служителите, които извършват обработване, за техните задължения.

Съвместното определяне на едно длъжностно лице по защита на данните стои като възможност и пред администраторите или обработващите лични данни, които са

[3] Класификаторът на длъжностите в администрацията е приет с Постановление на Министерския съвет № 129 от 26 юни 2012 г. (Обн. ДВ, бр. 49 от 29 юни 2012 г., последно изменение в ДВ, бр. 44 от 2 юни 2017 г.).

[4] Виж Богомилова Ж., Законови възможности за възлагане на допълнителни функции в рамките на трудовото правоотношение, „Труд и право“, кн. 5/2012 г., стр. 17 и следващи.

обществени органи или структури (чл. 37, пар. 3). Изискването е да се отчита организационната им структура и размер, но достъпността на длъжностното лице също трябва се вземе предвид, за да се гарантира ефективното изпълнение на неговите функции.

1.4. Публикуване на данни за контакт с длъжностното лице по защита на данните

Администраторът или обработващият лични данни са длъжни да публикуват данните за контакт с длъжностното лице по защита на данните и да ги съобщят на надзорния орган (чл. 37, пар. 7). Това е своеобразна гаранция, че субектите на данни и надзорните органи могат да се свържат с длъжностното лице пряко, без „посредничеството“ на администратора или обработващия данните. Такива данни за контакт могат да бъдат адрес, телефонен номер, електронен адрес, специален формуляр за контакт на интернет страницата на организацията, адресиран до длъжностното лице по защита на данните и др.

В чл. 37, пар. 7 от ОРЗД не се изисква публикуваните данни за контакт да съдържат името на длъжностното лице. Въпреки че Работната група по чл. 29 оценява публикуването на името като добра практика, оставя на преценката на администратора/обработващия и длъжностното лице да решат дали това е необходимо или полезно при конкретните обстоятелства. Надзорният орган и служителите на администратора или обработващия, обаче, при всички случаи трябва да бъдат информирани за името и данните за връзка с длъжностното лице по защита на данните. Това следва от възложените му задачи и по-конкретно от изискването длъжностното лице да си сътрудничи с надзорния орган (чл. 39, пар. 1, б. „г“ от ОРЗД). Освен това *името* и координатите за връзка с длъжностното лице по защита на данните са част от нормативното съдържание на уведомлението до надзорния орган при нарушение на сигурността на личните данни (чл. 33, пар. 3, б. „б“ от Регламента).

2. Статут на длъжностното лице по защита на данните

В чл. 38 от ОРЗД са предвидени основните елементи от правното положение на длъжностното лице по защита на данните. Те са предпоставка за ефективното изпълнение на неговите задачи и очертават статута, който той има в организацията на администратора или обработващия.

2.1. Участие във всички въпроси, свързани със защитата на личните данни

Задължение на администратора и на обработващия лични данни е да гарантират участието на длъжностното лице по защита на данните във всички въпроси, свързани със защитата на личните данни. Според чл. 38, пар. 1 от ОРЗД това трябва да става по „подходящ начин“ и „своевременно“. Това означава да се отчитат конкретните обстоятелства при организиране на защитата и операциите по обработване на лични данни, извършвани в структурата на администратора или обработващия и да се осигури запознаване с тях на длъжностното лице по защита на данните. Удачно е участието му в решаването на всички въпроси, свързани със защитата на личните данни, да става на възможно най-ранен етап, включително да се изисква и негово предварително становище. Това може да се окаже решаваща стъпка в практическото прилагане на защитата на данните на етапа на проектирането (чл. 25 от ОРЗД).

Работната група по чл. 29 отправя следните препоръки във връзка с изискванията на чл. 38, пар. 1 от ОРЗД:

- длъжностното лице по защита на данните да бъде редовно канено да участва в срещи на висшето и средното ръководство;

- длъжностното лице по защита на данните да присъства при вземане на решения, свързани със защитата на данните и цялата относима информация да му бъде предадена своевременно, за да може да предостави адекватни съвети;
- становищата на длъжностното лице по защита на данните да се отчитат с нужната тежест, а в случай на несъгласие с тях да се документират причините за тяхното неспазване;
- длъжностното лице по защита на данните да бъде консултирано своевременно при нарушение на защитата на данните или при друг инцидент;
- ако преценят, че е подходящо, администраторът или обработващият могат да разработят насоки или програми за защита на данните, които да определят кога трябва да се направи консултация с длъжностното лице по защита на данните.

2.2. Необходими ресурси

В чл. 38, пар. 2 от ОРЗД са обхванати няколко задължения на администратора и обработващия личните данни за подпомагане на длъжностното лице по защита на данните при изпълнение на неговите задачи. Те са свързани с осигуряване на необходимите ресурси, достъп до личните данни и операциите по обработване и поддържане на експертните познания на длъжностното лице по защита на данните. Това означава да се има предвид един по-широк контекст в ресурсното обезпечаване на длъжностното лице по защита на данните и този подход намира потвърждение в Насоките за длъжностните лица по защита на данните, приети от Работната група по чл. 29. Тя препоръчва обхващането на следните елементи:

- активна подкрепа на функцията на длъжностното лице по защита на данните от висшето ръководство;
- осигуряване на достатъчно време за изпълнение на задълженията на длъжностното лице по защита на данните. Това е особено важен аспект в случаите на определяне на длъжностното лице чрез възлагане на допълнителни функции на служител от персонала или по договор за услуги с външно за структурата на администратора или обработващия лице. Работната група приема за добри практики определяне на част от времето за функцията длъжностното лице по защита на данните, когато тя не се изпълнява на пълно работно време, изготвяне на работен план за длъжностното лице по защита на данните, подходящо ниво на приоритет на задълженията;
- финансови ресурси, инфраструктура (помещения, съоръжения, оборудване) и персонал към длъжностното лице по защита на данните, ако е необходимо;
- достъп до други звена в структурата на администратора или обработващия (човешки ресурси, правен отдел, звено за сигурност, информационно обслужване) с оглед получаване на нужното съдействие от тяхна страна;
- непрекъснато обучение за повишаване на нивото на експертиза. Длъжностното лице по защита на данните следва да бъде насърчавано да участва в курсове за обучение по защита на личните данни и в други тематики, които имат отношение към професионалното му развитие. Отчитайки необходимостта от обучение и хармонизиране на стандартите и практиките в сферата на защитата на личните данни, Комисията за защита на личните данни планира да изгради национален обучителен център, който да осигури нужното обучение за лицата по защита на личните данни. Очаква се центърът да стартира своята дейност през 2018 г., непосредствено преди прилагането на Общия

регламент[5];

- според размера и структурата на организацията може да се създаде екип на длъжностното лице по защита на данните. Това налага ясно формулиране на вътрешната структура, задачите и отговорностите на членовете на екипа.

Налага се изводът, че колкото по-сложни (заради обема или вида) или чувствителни (заради характера на информацията) са операциите по обработване на личните данни, толкова повече ресурси трябва да се предоставят на длъжностното лице по защита на данните.

2.3. Неполучаване на указания и независимост при изпълнение на задълженията

От разпоредбата на чл. 38, пар. 3 и съображение 97 на ОРЗД следват изискванията пред администратора и обработващия да гарантират, че длъжностното лице по защита на данните не поучава никакви указания във връзка с изпълнение на своите задачи и ги изпълнява независимо. Това означава не само те да се въздържат от указания как да се реши конкретен въпрос или жалба, но това да важи и за всички други техни служители. Работната група по чл. 29 препоръчва да се даде възможност на длъжностното лице по защита на данните да изразява несъгласие с решения на администратора или обработващия, които са несъвместими с неговите препоръки.

Длъжностното лице по защита на данните се отчита *пряко* пред най-висшето ръководно ниво на администратора или обработващия лични данни. Това е важно проявление на неговата независимост от други ръководни нива в структурата.

2.4. Отговорност на длъжностното лице по защита на данните

Автономията на длъжностното лице по защита на данните е гарантирана не само с независимостта му при изпълнение на задачите, но и от забраните за освобождаване от длъжност и санкциониране, предвидени в чл. 38, пар. 3. Дадените от Работната група по чл. 29 насоки в тази връзка са с особена практическа стойност. Те изясняват, че санкциите са забранени само ако са наложени във връзка с изпълнението на задълженията като длъжностно лице по защита на данните. Например няма да е допустимо налагане на наказание от страна на администратора, ако той не е съгласен с дадената от длъжностното лице оценка на въздействие за дадена операция по обработване на лични данни. В такава ситуация длъжностното лице по защита на данните не може да бъде освободено за даване на този съвет.

Забраната за освобождаване от длъжност не трябва да се абсолютизира. Длъжностното лице по защита на данните може да бъде правомерно освободено на основанията, предвидени в трудовото законодателство и правилата за държавната служба. Колкото по-стабилно е правоотношението му, обаче, толкова по-голяма е вероятността да действа по независим начин и Работната група по чл. 29 би приветствала усилията на организациите в тази насока.

2.5. Конфиденциалност

Длъжностното лице по защита на данните е обвързано със задължение да спазва конфиденциалност при изпълнение на неговите задачи (чл. 38, пар. 5). Това е важна гаранция за субектите на данни, които могат да се обръщат към него по всички въпроси, свързани с обработването на лични данни и с упражняването на техните права съгласно

[5] По данни от сайта на Комисията за защита на личните данни, секция „Бъдете информирани“, Информационно-разяснителни материали по Регламент (ЕС) 2016/679, Длъжностно лице по защита на данните, https://www.cpdp.bg/?p=element&aid=1044

Общия регламент относно защитата на данните. В този контекст задължението за поверителност е установено по отношение на конкретните обстоятелства, станали известни на длъжностното лице при или по повод изпълнение на неговите задачи. Неговото спазване, обаче, не изключва възможността за контакт и търсенето на съдействие от надзорния орган, тъй като това е част от задачите на длъжностното лице по защита на данните.

2.6. Конфликт на интереси

Предвид възможността длъжностното лице по защита на данните да изпълнява и други задачи, при това не само в структурата на администратора или обработващия, но и извън тях, ОРЗД въвежда изискването те да не водят до конфликт на интереси (чл. 38, пар. 6). Работната група по чл. 29 приема, че длъжностното лице по защита на данните не може да заема позиция в организацията, която е свързана с определяне на целите и средствата за обработка на личните данни. Поради специфичната организационна структура във всяка организация, конфликтът на интереси трябва да се преценява конкретно за случая. Работната група дава примерни насоки, като посочва, че висшите ръководни позиции (например главен изпълнителен директор, главен оперативен директор, главен финансов директор, ръководителите на звената за човешките ресурси и информационните технологии) могат да създадат такъв конфликт. Като пример за конфликт на интереси, когато външно за структурата на администратора или обработващия лице е определено за длъжностно лице по защита на данните, е посочено представителството, осъществявано от това лице на администратора или обработващия, пред съдилищата по въпроси, свързани със защитата на личните данни.

Управлението на конфликта на интереси предполага ясно дефиниране на длъжностите, които биха били несъвместими със задачите на длъжностното лице по защита на данните. Несъмнено изводът на Работната група по чл. 29 относно висшите ръководни позиции следва да бъде споделен, защото ако има сливане на правни качества между администратора и длъжностното лице по защитата на данните, това би обезсмислило определянето на такова лице. Декларирането на обстоятелства, които имат отношение към конфликта на интереси, също би било добра практика, особено в съчетание с надлежни гаранции, предвидени във вътрешни правила за работата или при провеждане на конкурси за длъжностно лице по защита на данните. Липсата на конфликт на интереси при осъществяване на неговите задачи е важна гаранция за независимост.

Видно от уредбата на ОРЗД и интерпретациите, които дава Работната група по чл. 29, понятието за конфликт на интереси е разгледано в контекста на задачите на длъжностното лице по защита на данните. Независимо от това трябва да се държи сметка и за българската уредба, по-специално Законът за предотвратяване и установяване на конфликт на интереси, който ще намери приложение, когато длъжността попада в категорията публични длъжности по смисъла на чл. 3. Например ако задачите на длъжностно лице по защита на данните се изпълняват от служители в държавната администрация, с изключение на служителите, които заемат технически длъжности, към изискванията на ОРЗД ще се добавят и произтичащите от ЗПУКИ.

3. Задачи на длъжностното лице по защита на данните

В чл. 39 от ОРЗД е предвиден определен минимум от задачи на длъжностното лице по защита на данните. При изпълнението им то трябва да отчита рисковете, свързани с операциите по обработване, като се съобразява с естеството, обхвата, контекста и целите на обработването. Този подход, базиран на риска, позволява да се съсредоточат усилията

върху въпроси, които са оценени като по-рискови, без да се пренебрегват и операциите по обработване, които са съпроводени с по-малък риск.

3.1. Информиране и консултиране на администратора, обработващия и служителите, които извършват обработване

Тази задача има за цел да разясни на администратора, обработващия и служителите, които извършват обработване, техните задължения, произтичащи от ОРЗД и от други разпоредби за защита на данните в Европейския съюз или държава-членка. Именно поради това се изискват експертни познания в областта на правото и практиките за защита на данните. Длъжностното лице по защита на данните има възможността не само да представи уредбата, но и да даде съвет как да бъдат изпълнени задълженията в конкретния случай.

3.2. Мониторинг на спазването на ОРЗД

Наблюдението на спазването на регламента и на други разпоредби за защита на данните на ниво ЕС или държава-членка и на политиките на администратора или обработващия, което се възлага на длъжностното лице по защита на данните, не отменя задължението на администратора или обработващия да контролира спазването на ОРЗД. От съображение 97 на ОРЗД става ясно, че ролята на длъжностното лице по защита на данните е да подпомага администратора или обработващия в тази му дейност.

Помощта от лице с експертни познания, каквито са очакванията към длъжностното лице, може да допринесе за повишаване на защитата на личните данни. Това може да стане например чрез идентифициране на операциите по обработване, анализ и проверка за съответствието на обработването с установените изисквания, информиране и даване на конкретни препоръки до администратора или обработващия. Повишаването на осведомеността и обучението на персонала, ангажиран с операциите по обработване, също е инструмент, с който разполага длъжностното лице по защита на данните. Това е механизъм с мощно превантивно действие, който може да даде своевременна информация за рисковете пред защитата на данните и да води до усъвършенстване на прилаганите мерки за защита.

3.3. Участие в процеса на оценката на въздействие

Ролята на длъжностното лице в процеса на оценката на въздействие върху защитата на данните е важна и полезна, но следва да се открои като помощна и консултативна. Според чл. 35 от ОРЗД извършването на оценка на въздействието върху защитата на личните данни е задължение на администратора, а когато е определено длъжностно лице по защита на данните, администраторът трябва да поиска неговото становище. В чл. 39, пар. 1, б. „в“ задачите на длъжностното лице по защита на данните отчитат това правило, като предвиждат и възможността за наблюдение на процеса по извършването на оценката.

Работната група по чл. 29 препоръчва администраторът да потърси съвет от длъжностното лице по защита на данните най-малко по следните въпроси:

- да извърши или не оценка на въздействието върху защитата на данните;
- по каква методология да се извършва оценката на въздействието върху защитата на данните;
- дали оценката на въздействието върху защитата на данните да се извърши в организацията или да се възложи на външен изпълнител;
- какви гаранции (включително технически и организационни мерки) да се прилагат, за да се намалят рисковете за правата и интересите на субектите на данни;
- дали оценката на въздействие върху защитата на данните е извършена

коректно и дали нейните заключения са в съответствие с ОРЗД.

Ако администраторът не е съгласен с препоръките на длъжностното лице по защита на данните, е препоръчително да обоснове конкретно и в писмена форма причините, поради които не ги взема предвид.

3.4. Сътрудничество с надзорния орган

Сътрудничеството с надзорния орган, освен като общо задължение, е предвидено и с изискването длъжностното лице по защита на данните да действа като точка за контакт за надзорния орган по различни въпроси. Те могат да бъдат свързани с обработването на лични данни, с предварителната консултация[6], а по целесъобразност консултирането може да обхваща и всякакви други въпроси.

В контекста на сътрудничеството с надзорния орган е особено важно задължението на администратора да съобщи данните му, включително името на лицето. Въпреки че не е предвидено изрично, администраторът следва да информира своевременно и за всички промени в обстоятелствата.

3.5. Други функции

На длъжностното лице по защита на данните могат да се възлагат и други задачи. Например Работната група по чл. 29 не намира пречки администраторът или обработващият да възложат на длъжностното лице по защита на данните задачата да поддържа регистър на дейностите по обработване, за които отговаря. Регистърът съдържа информацията по чл. 30, пар. 2 от ОРЗД и воденето му от длъжностното лице се разглежда от Работната група по чл. 29 като един от инструментите, който му позволява да изпълнява задачите си по наблюдение на спазването, информиране и съветване на администратора или обработващия.

Може да се изведе по-генералният извод, че възможността за възлагане на допълнителни задачи, която чл. 39, пар. 1 от ОРЗД допуска, трябва да бъде използвана, без да води до конфликт на интереси, а да е в унисон с другите задължения на длъжностното лице по защита на данните.

Д-р Невин Фети, юрист

[6] Предварителната консултация е уредена в чл. 36 от ОРЗД и се изразява в получаването на мнението на надзорния орган преди обработването на данни, което ще породи висок риск за правата и свободите на физическите лица. Наличието на такъв риск се преценява въз основа на извършената оценка на въздействието по правилата на чл. 35 от ОРЗД. Заслужава отбелязване разпоредбата на чл. 36, пар. 4, адресирана до държавите, която изисква да се консултират с надзорния орган по време на изготвянето на предложения за законодателни или регулаторни мерки, които се отнасят до обработването на лични данни.