ДЛЪЖНОСТНО ЛИЦЕ ПО ЗАЩИТА НА ДАННИТЕ – ИЗИСКВАНИЯ, СТАТУС И ФУНКЦИИ

*доц. д-р Андрей Александров
Институт за държавата и правото
при Българската академия на науките
Югозападен университет „Неофит Рилски“*

DATA PROTECTION OFFICER – REQUIREMENTS, STATUS AND FUNCTIONS

*Assoc. Prof. Andrey Aleksandrov, PhD
Institute for the State and the Law –
Bulgarian Academy of Sciences
South-West University „Neofit Rilski“*

Резюме: Изследването е посветено на една от най-значимите от практическа гледна точка теми, свързани с прилагането на Общия регламент за защита на данните – този за определянето, статуса и функциите на длъжностното лице по защита на данните. Представени са актуалните тенденции по тези въпроси в европейската и българската практика. Потърсени са отговори на често възникващи в практиката проблеми.

Ключови думи: *длъжностно лице по защита на данните (ДЛЗД), Общ регламент за защита на данните (ОРЗД), изисквания, роля, права и задължения*

Abstract: The study is devoted to one of the most important from a practical point of view topics related to the implementation of the General Data Protection Regulation - that of the definition, status, and functions of a data protection officer. The current trends on these issues in European and Bulgarian practice are presented. Answers to frequently encountered problems in practice are sought.

Key words: *Data Protection Officer (DPO), General Data Protection Regulation (GDPR), requirements, roll, rights and obligations*

DOI: <https://doi.org/10.36997/PPDD2021.44>

Въведение

Вече над три години се прилага Общият регламент за защита на данните (ОРЗД),¹ който бележи началото на мащабна реформа в законодателството по защита на личните данни, а и в развитието на Европейския съюз (Тошкова – Николова, Фети 2019). Като че ли в последно време темата мина донякъде на заден план, изместена от безпрецедентната заплаха на пандемията от COVID-19 и *антикризисните* промени в законодателството, възприети във връзка с извънредното положение и извънредната епидемична обстановка. Тя обаче не е загубила голямата си обществена значимост и не бива да се забравя за нея. Причините са не само и не толкова в големите размери на санкциите при установени нарушения, а в нещо много по-важно: защитата на данните не е самоцел, а средство за предпазване на личната неприкосновеност на лицата, а оттук – и гаранция за основните им права (Кръстева, Александров 2018). Оттук произтича и голямата практическа важност на въпроса кой ще бъде определен за длъжностно лице по защита на данните (ДЛЗД). Удачният избор на такова лице може да се окаже решаващ за сигурността на обработваните данни.

Изложение

I. Хипотези на определяне на ДЛЗД

ДЛЗД е *отговорник* по всички въпроси, свързани със защитата на личните данни в организацията на администратора или на обработващия лични данни. Това е служител на администратора/обработващия или външно за организацията лице, натоварено с консултативни функции в областта на защитата на личните данни, надзор по спазването на регламента в организацията и повишаването на осведомеността и обучението на персонала (Матеева 2019).

Съгласно ОРЗД могат да се обособят две групи случаи на определяне на ДЛЗД: (а) при първата от тях то представлява правно задължение и евентуалното му неизпълнение може да доведе до налагане на санкции на задължените лица; (б) във втората група случаи

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. Той започва да се прилага от 25 май 2018 г.

определянето на ДЛЗД става по избор на съответната организация с цел да се оптимизира защитата на обработваните лични данни (Захариев 2018а, 2018б). Независимо дали определянето на ДЛЗД е било задължително или е предприето от организацията доброволно, неговите статут и функции са еднакви.

По въпросите, свързани с определянето на ДЛЗД, са издадени нарочни указания (насоки) от Работната група по чл. 29 от Директива 95/46/ЕО (след 25.05.2018 г. – Европейски комитет по защита на данните. В тях е дадена препоръка към администраторите и обработващите лични данни, освен ако е очевидно, че дадена организация не е задължена да определя ДЛЗД, 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. 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 на задължително определяне на ДЛЗД (Александров 2018).

Хипотезите на задължително определяне на ДЛЗД според регламента са следните: (а) когато обработването се извършва от публичен орган или структура, освен когато става въпрос за съдилища при изпълнение на съдебните им функции; (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; (в) когато основните дейности на администратора или обработващия лични данни се състоят в мащабно обработване на специалните категории данни и на лични данни, свързани с присъди и нарушения.

Така описаните хипотези налагат няколко уточнения, например кога обработването на данни представлява основна дейност на администратора или на обработващия. За *основни дейности* се считат ключовите операции, които са необходими за постигането на целите на администратора или обработващия лични данни. Обработването на данни е основна дейност и в случаите, когато то е неразделна част от останалите дейности на организацията. Казаното може да се она-

гледни със следните примери:

► 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 е нужно да се счита за една от основните дейности на всяка болница и съответно болниците трябва да определят ДЛЗД.

► Частно охранително дружество 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.

► КЗЛД е имала повод да изрази специално становище по отношение на училищата: „Съгласно разпоредбата на чл. 37, пар. 1, б. „а” от Регламент (ЕС) 2016/679 във вр. с пар. 1, т. 17 от ДР на Закона за защита на личните данни, институциите в системата на предучилищното и училищното образование (училища, детски градини и др.), в качеството си на администратори на лични данни, са задължени да определят ДЛЗД.“²

Обратно, следните дейности по обработване на данни не трябва да се считат за основна дейност на администратора/обработващия: (а) обработка на данни на работници и служители с цел изплащане на възнагражденията им; (б) стандартна ИТ поддръжка на фирмени системи; (в) наблюдение на интернет и имейл трафик с цел спазване на изискванията за киберсигурността и др. п. Това са примери за спомагателни функции, които са необходими за основната дейност или основното направление на стопанската дейност на организацията. Въпреки че тези дейности несъмнено са необходими, те обикновено са считани за спомагателни функции, а не за основна дейност.

Що се отнася до хипотезите на *масабно обработване* на данни, липсва точен количествен критерий кога е налице такова обработване. При преценката следва да се вземат под внимание фактори като броят на субектите на данни, обемът или видът данни, които се обработват, продължителността на обработването, географският обхват на обработването. При това е нужно тези критерии да се съобразят

² https://www.cpdp.bg/index.php?p=news_view&aid=1576

кумулятивно (едновременно), а не самостоятелно. Обработването, например, може да се осъществява паралелно в няколко държави членки и да е налице широк географски обхват, но да засяга малко на брой лица и незначителен обем данни. В този случай то няма да се характеризира като мащабно.

Понятието за редовно и систематично наблюдение на субектите на данните също не е изрично дефинирано в регламента. Според тълкуването на Работната група по чл. 29 *редовно* означава: текущо или възникващо на определени интервали за определен период; многократно или повтарящо се на определени интервали; случващо се постоянно или периодично наблюдение. Наблюдението е систематично, когато се осъществява чрез система, организирано е или е част от целенасочен план или стратегия за събиране на данни.

Редовно и систематично наблюдение може да е налице при профилиране и оценяване на субектите 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) и др.п.

II. Изисквания към ДЛЗД

В чл. 37, пар. 5 от регламента 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“. 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. Въпреки че регламентът не поставя конкретни изисквания относно необходимата професионална квалификация и опит на ДЛЗД, то следва да познава добре сектора и организацията на администратора, както и да разбира 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. При частните организации се предполага познаването на специалните закони и процедури, регулиращи тяхната дейност (напр. Закона за кредитните институции и съответните подзаконови актове – по отношение на дейността на банките и т.н.)

Фразата *съответен опит* не следва да се чете и разбира изрично като опит, придобит като длъжностно лице по защита на данните – това би могъл да е опит в изготвянето и прилагането на политики в съответната организация (или подобна организация) или в съответните област като ИТ, разработване на продукти и т.н. Достатъчно е да се спомене, че позицията не следва да бъде възлагана на сравнително млад, неопитен човек или на лице, което не е запознато с конкретния (тип) организация, за която става въпрос. (Наръчник за длъжностните лица по защита на данните, публикуван на интернет страницата на КЗЛД).³

Длъжностното лице по защита на данните играе ключова роля в насърчаването на културата по защита на данните в рамките на организацията. Затова, наред с професионалните качества, регламентът поставя като изискване и „способността му да изпълнява задачите, посочени в чл. 39“. 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. „То е в деликатна позиция: трябва да е готово да каже „не“ на своите началници в редки случаи, но по-често да бъде в състояние да помага за намирането на решение на въпроси, което трябва както да бъде приемливо за организацията, така и изцяло да бъде в съответствие със закона (и, ако не друго, да следи и защитава неприкосновеността).“ (цитирания по-горе наръчник).

III. Статус на ДЛЗД

Според регламента ДЛЗД може да бъде както служител на предприятието, така и да изпълнява задълженията си по договор за услуги. Няма пречка служителът, определен от администратора за лице по защита на данните, да изпълнява и други функции в рамките на организацията (т.е. вече назначен на друга длъжност служител да поеме и функциите на длъжностно лице по защита на данните по вътрешно съвместителство).

Възможно е и съвместно определяне на ДЛЗД в група предприятия. Условието е всяко предприятие да има *лесен достъп* до длъжностното лице по защита на данните. Достъпността се отнася до задачите на длъжностното лице като точка за контакт на субектите на

³ [https://www.cdpd.bg/userfiles/file/Documents_2019/T4DATA-MANUAL-2019-BG\(1\).pdf](https://www.cdpd.bg/userfiles/file/Documents_2019/T4DATA-MANUAL-2019-BG(1).pdf)

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. В многонационалните групи предприятия улесняването на достъпа до ДЛЗД би включвало и възможността с него да се комуникира на език, какъвто владеят служителите и в останалите държави, в които компанията има структури.

Предвид възможността длъжностното лице по защита на данните да изпълнява и други задачи, регламентът въвежда изискването те да не водят до конфликт на интереси. Работната група по чл. 29 приема, че ДЛЗД 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, ръководители на звената за човешките ресурси и информационните технологии) могат да създадат такъв конфликт, т.е. такива лица не следва да се определят за ДЛЗД. Противното би означавало тези лица да съчетаят в едно качествата на контролиращ и контролиран, т.е. да осъществяват контрол над собствените си действия, което е логически неиздържано, а оттук – и юридически недопустимо.

Пряко свързан с правилото за предотвратяване на всеки възможен конфликт на интереси е и принципът на независимост на ДЛЗД. Администраторът/обработващият трябва да гарантират, че това лице не получава никакви указания във връзка с изпълнение на своите задачи. Това означава не само те да се въздържат от указания как да се реши конкретен въпрос или жалба, но да важи и за всички други техни служители. Работната група по чл. 29 препоръчва да се даде възможност на ДЛЗД да изразява несъгласие с решения на администратора или обработващия, които са несъвместими с неговите препоръки.

ДЛЗД се отчита пряко пред най-висшето ръководно ниво на администратора или обработващия лични данни. Това е проявление на неговата независимост от други ръководни нива в структурата.

Според чл. 38, пар. 3 от регламента ДЛЗД не може да бъде осво-

бождавано от длъжност, нито санкционирано от администратора или обработващия лични данни за изпълнението на своите задачи. Дадените от Работната група по чл. 29 насоки в тази връзка изясняват, че санкциите са забранени, само ако са наложени във връзка с изпълнението на задълженията като ДЛЗД. Например няма да е допустимо налагане на наказание от страна на администратора, ако той не е съгласен с дадената от ДЛЗД оценка на въздействие за дадена операция по обработване на лични данни. ДЛЗД не може да бъде уволнено за даване на този съвет.

ДЛЗД е обвързано със задължение да спазва конфиденциалност при изпълнение на неговите задачи. 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 регламента. Задължението за поверителност е установено по отношение на конкретните обстоятелства, станали известни на длъжностното лице при или по повод изпълнение на неговите задачи.

ДЛЗД не са лично отговорни в случай на неспазване на правилата на регламента. Администраторът или обработващият лични данни е този, който е длъжен да гарантира и да е в състояние да докаже, че обработването се извършва в съответствие с предвидените в него разпоредби (чл. 24, пар. 1). Спазването на разпоредбите за защита на данните е отговорност на администратора на данни или на обработващия лични данни.

IV. Основни задачи на ДЛЗД

На длъжностното лице по защита на данните могат да се възлагат редица задължения, по-важните от които са: (а) да информира и съветва администратора или обработващия лични данни и служителите, които извършват обработване, за техните задължения по силата на нормативните актове за защита на личните данни; (б) да наблюдава спазването на правилата за защита на личните данни и на политиките на администратора или обработващия лични данни по отношение на защитата на личните данни, включително възлагането на отговорности, повишаването на осведомеността и обучението на персонала, участващ в операциите по обработване, и съответните одити; (в) да си сътрудничи с надзорния орган и да действа като точка за контакт за надзорния орган по въпроси, свързани с обработването

на данните; (г) при поискване да предоставя съвети по отношение на оценката на въздействието върху защитата на данните и да наблюдава 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: (аа) да извърши, или не, оценка на въздействието върху защитата на данните; (бб) по каква методология да се извършва оценката на въздействието върху защитата на данните; (вв) дали оценката на въздействието върху защитата на данните да се извърши в организацията, или да се възложи на външен изпълнител; (гг) какви гаранции (включително технически и организационни мерки) да се прилагат, за да се намалят рисковете за правата и интересите на субектите на данни; (дд) дали оценката на въздействие върху защитата на данните е извършена коректно и дали нейните заключения са в съответствие с регламента.

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.

Задължение на администратора и на обработващия лични данни е да гарантират участието на ДЛЗД по всички въпроси, свързани със защитата на личните данни. Това трябва да става по *подходящ начин и своевременно*, т.е. като се отчитат конкретните обстоятелства при организиране на защитата и операциите по обработване на лични данни, извършвани в структурата на администратора или обработващия, и се осигури запознаване с тях на ДЛЗД. 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 изиска и негово предварително становище.

В чл. 38, пар. 2 от регламента са посочени някои задължения на администратора и обработващия личните данни за подпомагане на ДЛЗД при изпълнение на неговите задачи. Те са свързани с осигуряването на необходимите ресурси, достъпа до личните данни и операциите по обработване и поддържане на експертните познания на длъжностното лице по защита на данните. Тук се включват активната подкрепа на функцията на ДЛЗД от висшето ръководство, осигуряването на достатъчно време за изпълнение на задълженията му и осигуряването на финансови ресурси, инфраструктура и персонал към длъжностното лице по защита на данните, ако е необходимо и т.н.

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. Това е 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. На интернет страницата на КЗЛД е публикуван образец на Уведомление за определено длъжностно лице по защита на данните. Указания относно попълването се съдържат в самото уведомление. Администраторът или обработващият имат задължението да информират за всяка настъпила промяна на обстоятелствата/данните от уведомлението. Указаните са и начините, по които може да се подаде уведомлението – на място в деловодството на Комисията, чрез автоматизирана информационна система на КЗЛД и т.н. КЗЛД публикува данните в Регистъра на администраторите/обработващите лични данни, определили ДЛЗД.

Заклучение

Ако накратко трябва да се обобщи всичко казано по-горе, несъмнено се налага изводът за съществената роля, която играе ДЛЗД в процесите на обработване на данните във всяка организация. Затова към определянето на такова лице не следва да се пристъпва лекомислено, прибързано или с мотив, че трудно се намират желаещи да се нагърбят с подобна отговорност и затова тя ще бъде вменена на този, който не е в позиция да откаже. Подобен подход обрича администратора или обработващия на едно формално присъстващо в организацията ДЛЗД, което не проявява никаква инициативност и само маркира изпълнението на възложените му функции. Едва ли е необходимо специално да се обоснова какви рискове крие подобна ситуация за сигурността на данните и, разбира се, за защитата на правата на субектите на тези данни.

Използвана литература

Александров, А. (2018). Статус и функции на длъжностните лица по защита на данните. // Труд и право, № 9, с. 49 – 57.

Aleksandrov, A. (2018). Status i funktsii na dlazhnostnite litsa po zashtita na dannite. // Trud i pravo, № 9, s. 49 – 57.

Захариев, М. (2018а). Задължение за назначаване на ДЛЗД и уведомление за него в КЗЛД. // Данъци ТИТА, №104, 2018 (<https://www.tita.bg/free/commercial-law/553>, 27.09.2021).

Zahariev, M. (2018a). Zadalzhenie za naznachavane na DLZD i uvedomlenie za nego v KZLD. // Danatsi TITA, №104, 2018 (<https://www.tita.bg/free/commercial-law/553>, 27.09.2021).

Захариев, М. (2018б). Автоматизираното профилиране и защитата на личните данни. Анализ на GDPR. София: За буквите (О писменехъ), с. 206 – 210.

Zahariev, M. (2018b). Avtomatiziranoto profilirane i zashtitata na lichnite dannii. Analiz na GDPR. Sofia: Za bukвите (O pismenehy), s. 206 – 210.

Кръстева, Д., А. Александров (2018). Защита на личните данни. Мисия възможна. София: Резон България ЕООД.

Krasteva, D., A. Aleksandrov (2018). Zashtita na lichnite dannii. Misia vazmozhna. Sofia: Rezon Bulgaria EOOD.

Mateeva, Z. (2019). Specific Nature of the New Profession „Data Protection Officer” in the Context of Digitalization. // Международни клъстерни политики: Българо-китайски форум. Сборник с доклади от международна конференция. Варна: Наука и икономика, с. 112 – 122.

Mateeva, Z. (2019). Specific Nature of the New Profession „Data Protection Officer” in the Context of Digitalization. // Mezhdunarodni klasterni politiki: Balgaro-kitayski forum. Sbornik s dokladi ot mezhdunarodna konferentsia. Varna: Nauka i ikonomika, s. 112 – 122.

Тошкова-Николова, Д., Н. Фети (2019). Защита на личните данни. София: Труд и право.

Toshkova-Nikolova, D., N. Feti (2019). Zashtita na lichnite dannii. Sofia: Trud i pravo.

Наръчник за длъжностните лица по защита на данните ([https://www.cdpd.bg/userfiles/file/Documents_2019/T4DATA-MANUAL-2019-BG\(1\).pdf](https://www.cdpd.bg/userfiles/file/Documents_2019/T4DATA-MANUAL-2019-BG(1).pdf), 27.09.2021).

Narachnik za dlazhnostnite litsa po zashtita na dannite. ([https://www.cdpd.bg/userfiles/file/Documents_2019/T4DATA-MANUAL-2019-BG\(1\).pdf](https://www.cdpd.bg/userfiles/file/Documents_2019/T4DATA-MANUAL-2019-BG(1).pdf), 27.09.2021).

Определяне на длъжностно лице по защита на данните в сферата на предучилищното и училищното образование (разяснение на КЗЛД). (https://www.cdpd.bg/index.php?p=news_view&aid=1576, 27.09.2021).

Opredelyane na dlazhnostno litse po zashtita na dannite v sferata na preduchilishtnoto i uchilishtnoto obrazovanie (razyasnenie na KZLD). (https://www.cdpd.bg/index.php?p=news_view&aid=1576, 27.09.2021).

За контакти: доц. д-р Андрей Александров
ИДП при БАН, ЮЗУ „Н. Рилски“
e-mail: a.alexandrov@kambourov.biz