Дайджест "Собственост и право", 2017 г., кн. 9, стр. 74 и сл.

ДЛЪЖНОСТНО ЛИЦЕ ПО ЗАЩИТА НА ДАННИТЕ

Бързото технологично развитие, нарастването на мащаба на обмена и събирането на лични данни наложиха по-голяма съгласуваност на нормативната рамка в Европейския съюз /ЕС/. От 25 май 2018 г. защитата на личните данни ще се осъществява по правилата на Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните). Новата уредба е натоварена с очакванията да даде на физическите лица повече контрол върху данните им в дигиталния свят и да намали административната тежест.

Сред новите положения, които въвежда Общият регламент относно защитата на данните /ОРЗД, Регламентът/, е фигурата на **длъжностното лице по защита на данните**. Случаите, в които администраторът и обработващият лични данни[1] задължително определят такова лице, изпълняваните от него функции и задачи са предмет на уредбата в чл. 37-39 от ОРЗД.

1. Досегашната уредба за длъжностното лице по защита на данните в Европейския съюз

Директива 95/46/ЕО, която ще бъде отменена с ОРЗД, не предвижда задължение за назначаване на длъжностно лице за защита на данните, поради което и преобладаващата част от държавите членки не установяват подобно задължение в своето вътрешно законодателство. В националните законодателства или няма изисквания[2], или се прилага на доброволен принцип назначаване на лице по защитата на данните[3]. В българското законодателство доброволният принцип беше предвиден с Наредба № 1 от 30 януари 2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни, приета от Комисията за защита на личните данни в изпълнение на чл. 23, ал. 5 от Закона за защита на личните данни[4].

Само няколко държави членки на ЕС понастоящем изискват задължително назначаване на длъжностно лице по защита на данните при определени условия. Например в Германия задължението произтича в зависимост от броя на постоянно ангажирания с обработването на лични данни персонал (над 9 при автоматизирано обработване на лични данни и над 20 при неавтоматизирано обработване на лични данни). В Хърватия задължението за назначаване на лице по защита на данните зависи от броя на персонала на дадено предприятие (20 и повече служители). В Унгария е задължително назначаване на лице по защита на данните само за определени сектори: за органите, които обработват лични данни в национални регистри, за органите, които обработват данни за трудова заетост и регистри за съдимост; за финансовите институции и за доставчиците на телекомуникационни услуги и комунални услуги. Въпреки че в Испания няма изискване за назначаване на

[1] Понятията „администратор“ и „обработващ“ лични данни се запазват със същия смисъл, който имаха в Директива 95/46/ЕО. Най-общо администратор на лични данни е всеки правен субект, който определя целите и средствата за обработване на лични данни, а обработващ лични данни е правен субект (отделен от администратора), който обработва лични данни от името на администратора.

[2] Липсва уредба в Австрия, Великобритания, Гърция, Дания, Италия, Чехия, Португалия и Румъния.

[3] Този вариант е приложен в редица държави, сред които България, Белгия, Естония, Франция, Литва, Латвия, Ирландия, Люксембург, Малта, Нидерландия, Полша, Словакия, Швеция.

[4] Според чл. 18 от Наредбата администраторът на лични данни може да определи едно или повече лица по защита на личните данни, които да отговарят за координиране и прилагане на необходимите технически и организационни мерки за защита на личните данни.

служител по защита на данните, субектите, които обработват лични данни, изискващи мерки за защита от средно и/или високо ниво, трябва да назначат ръководител по сигурността на данните. Той не отговаря за защитата като цяло, а само за мерките за сигурност, които се прилагат към базите данни.

2. Случаите на задължително определяне на длъжностно лице по защита на данните в новата уредба

Регламент (ЕС) 2016/679 предвижда задължително определяне на длъжностно лице по защита на данните от някои администратори и обработващи данни. Според чл. 37, пар. 1 това са случаите при обработване[5] на лични данни от публични органи (с изключение на съдилищата) и от други администратори/обработващи, които, като основна дейност, извършват редовно и систематично наблюдение на субектите на данни или осъществяват мащабно обработване на специални категории данни. По този начин уредбата въвежда определени материални изисквания, но те не са базирани на точни количествени индикатори, а изискват конкретна преценка за всеки отделен случай. Освен това ОРЗД не изключва възможността и в други случаи да възниква задължение за определяне на длъжностно лице по защита на данните. Те могат да следват от изискванията на правото на ЕС, но е допустимо да произтичат и от правото на държава членка (чл. 37, пар. 4).

При липсата на легални дефиниции в регламента на понятията „публичен орган или структура“, „основна дейност“, „мащабно наблюдение“, „мащабно обработване“, практиката по прилагане ще бъде изправена пред сериозно предизвикателство. То ще е особено осезаемо в държавите, чието национално законодателство не е изисквало задължително определянето на длъжностно лице по защита на данните. Не е изключено и държавите, които и досега задължават да се определи такова лице, да се изправят пред различия с критериите, които залага ОРЗД. За да улесни този преход, Работната група за защита на лицата при обработването на лични данни (Работната група по чл. 29)[6] прие Насоки за длъжностните лица по защита на данните[7], които дават представа за съдържанието на използваната терминология в ОРЗД. Те имат важно значение при подготовката на дейностите, които ще способстват прилагането на новото европейско законодателство.

2.1. Администратори или обработващи лични данни, които са публични органи или структури

Работната група по чл. 29 счита, че понятието „публичен орган или структура“ в ОРЗД трябва да бъде определено съгласно националното законодателство на държавите членки. Прави впечатление, че ОРЗД не предвижда никаква характеристика за вида на

[5] По смисъла на чл. 4, т. 2 от Регламент (ЕС) № 2016/679 „обработване“ означава всяка операция или съвкупност от операции, извършвана с лични данни или набор от лични данни чрез автоматични или други средства като събиране, записване, организиране, структуриране, съхранение, адаптиране или промяна, извличане, консултиране, употреба, разкриване чрез предаване, разпространяване или друг начин, по който данните стават достъпни, подреждане или комбиниране, ограничаване, изтриване или унищожаване. В сравнение с дефиницията по чл. 2, б. „б“ на Директива 95/46/ЕО се наблюдава разширяване на кръга на действията, които се считат за обработване на лични данни. Например добавени са действия като структуриране, извличане, разкриване чрез начин, по който данните стават достъпни, подреждане, извършвани по отношение на лични данни. Тази по-широка дефиниция трябва да се отчете при определянето на администраторите и обработващите лични данни.

[6] 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 ѝ обхваща представители на надзорните органи на държавите членки, представители на органите по надзор на институциите на ЕС и представител на Европейската комисия. Представители в Работната група по чл. 29 има и Комисията за защита на личните данни, която е независимият държавен орган в Република България, който осъществява защитата на лицата при обработването на техните лични данни, при достъпа им до тези данни и контрола по спазването на Закона за защита на личните данни.

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

обработваните лични данни, а в тази хипотеза на задължително определяне на длъжностно лице по защита на данните издига като единствен критерий качеството на администратора или обработващия данните. Задължението им да определят такова лице изглежда формално, но аргументи за това могат да бъдат намерени в основанията, на които се обработват лични данни в тези случаи. Най-често не се изисква съгласието на субекта на данните (физическото лице, за което се отнасят данните), а обработването произтича от изпълнение на нормативно задължение, от изпълнявана задача в обществен интерес или от упражняване на правомощие на администратора. В тези случаи субектите на данни нямат избор относно това дали и как ще бъдат обработени техните данни. Това налага допълнителната защита, която определянето на длъжностно лице по защита на данните може да им даде. Смятам, че това принципно съображение трябва се отчита и при определяне на обхвата на понятието „публичен орган или структура“ в българското законодателство.

В категорията „публичен орган или структура“ могат да бъдат обхванати следните правни субекти:

- **Държавните органи в Република България**. Без значение в каква сфера се осъществява тяхната дейност, ако се налага извършване на действия по обработване на лични данни, те трябва задължително да определят длъжностно лице по защита на данните. Изключение се прави при обработването на лични данни от „съдилища при изпълнение на съдебните им функции“ и то е проявление на идеята, последователно проведена в ОРЗД, да се гарантира независимостта на съдебната власт при изпълнение на нейните функции. Поради това ОРЗД допуска надзорът на дейностите по обработване на лични данни от съдебните органи да се повери на специални органи в рамките на съдебната система на държавата членка. Този орган следва да осигури спазването на правилата на регламента, да повишава осведомеността сред членовете на съдебното съсловие за техните задължения при обработването на лични данни и да разглежда жалби във връзка с действия по обработване на такива данни. Като се отчита, че една от основните задачи на длъжностното лице по защита на данните е сътрудничеството с надзорния орган, а за съдилищата този надзор се осъществява от друг орган, липсата на задължение за определяне на такова лице намира своето логично обяснение.

Може да се постави въпросът дали изключението за задължително определяне на длъжностно лице по защита на данните е допуснато само за съдилищата или следва да се прилага и за други органи в системата на съдебната власт. Необходимо е да се отбележи, че ОРЗД не се прилага за обработване на лични данни за целите на предотвратяването, разкриването или наказателното преследване на престъпления или изпълнение на наложени наказания, за предпазването от и предотвратяването на заплахи за обществената сигурност (чл. 2, пар. 2, б. „г“). Предвид това и другите органи в системата на съдебната власт няма да бъдат задължени по ОРЗД да определят длъжностно лице по защита на данните, защото тяхната дейност по обработване на лични данни остава извън материалния му обхват. С Директива (ЕС) 2016/680 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни от компетентните органи за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания и относно свободното движение на такива данни, и за отмяна на Рамково решение 2008/977/ПВР на Съвета, която трябва да бъде транспонирана до 6 май 2018 г., държавите членки могат да освободят съдилищата и други независими съдебни органи от определянето на длъжностно лице по защита на данните. Освобождаването е предвидено като възможност за случаите, когато органите действат в изпълнение на съдебните си функции (чл. 32, пар. 1 от Директива (ЕС) 2016/680).

- **Органите на местното самоуправление.** Орган на местното самоуправление е общинският съвет, който се избира от населението на съответната община. Необходимо е да се вземе предвид, че дейността на общинския съвет се осигурява от общинската администрация. По силата на чл. 29а, ал. 2 от Закона за местното самоуправление и местната

администрация в нейната структура се създава звено, което подпомага и осигурява работата на общинския съвет. Служителите в звеното се назначават и освобождават от кмета на общината по предложение на председателя на общинския съвет. Няма пречки да се възложи на лице от това или друго звено на общинската администрация да изпълнява функциите на длъжностно лице по защита на данните.

- **Други публичноправни субекти, създадени по силата на нормативен акт за осъществяване на публични функции**. Терминът „публичноправен субект“ е използван в българското законодателство, без да има легална дефиниция на съдържанието му. В Закона за защита на класифицираната информация се допуска организационна единица по смисъла на този закон могат да бъдат публичноправните субекти, създадени със закон или с акт на орган на изпълнителната власт (§ 1, т. 3 от Допълнителните разпоредби). В Закона за достъп до обществена информация публичноправните субекти са включени в кръга на задължените субекти по закона (чл. 3, ал. 2, т. 1). „В съответствие със съдебната практика, това са субекти, извън тези по чл. 3, ал. 1 и извън публичноправните организации по смисъла на § 1, т. 4 от ДР на ЗДОИ, на които правнонормативно са предоставени определен кръг властнически правомощия. Правоотношението възниква между публичноправен субект като орган на власт от една страна и гражданите с техните организации от друга. То е властническо, а не на равнопоставеност, тъй като държавата е създала правилата, регламента на правоотношенията, т.е. тя е упражнила суверенитет, макар и опосредено в защита на обществения интерес“[8].

В практиката на Конституционния съд е използвано понятието „корпорации на публичното право“[9], като е пояснено, че „тези корпорации разполагат с известни публичноправни функции за организиране, контрол и дисциплинарна власт“. Като примери за такива корпорации се сочат адвокатурата, Нотариалната камара, както и съюзите на лекарите и стоматолозите, предвидени в Закона за съсловните организации на лекарите и стоматолозите, по повод на който Конституционният съд е имал възможността да се произнесе по тези въпроси. Според Конституционния съд: „Като поверява на самите лекари и стоматолози чрез управлявани от тях корпорации да ръководят двете професии, атакуваният закон постига най-целесъобразния способ за контрол върху спазването на Кодекса за професионална етика и на Правилата за добра медицинска практика, както и за надлежно управление на професията. Иначе тези функции би следвало да се възложат на държавни служители, които не биха могли да разполагат със същата компетентност и биха стрували не малко средства на държавния бюджет.“

Целта, за която с нормативен акт се създават публичноправни субекти, е да се изпълняват различни задължения на държавата. От гледна точка на обработването на лични данни в хода на осъществяваната от тях дейност, това най-често ще произтича по силата на нормативен акт, без да включва като необходим елемент съгласието на субекта на данните. Тази идея вероятно не е чужда и на Работната група по чл. 29, която приема, че „публични органи и структури включва национални, регионални и местни органи, но концепцията, съгласно приложимото национално законодателство, обикновено включва и редица други структури, регулирани от публичното право. В такива случаи определянето на служител по защита на данните е задължително“[10].

По смисъла на чл. 3, ал. 2, т. 1 от Закона за достъп до обществена информация в категорията публичноправни субекти се обхващат и публичноправните организации. Според § 1, т. 4 от Допълнителните разпоредби на ЗДОИ това са юридически лица, за които е изпълнено някое от следните условия: повече от половината от приходите им да се финансират с публични средства; повече от половината от членовете на управителните или

[8] Решение № 2104 от 27.03.2015 г. по адм. д. № 480/2015 г. на Административен съд-София-град, Второ отделение, 28-ми състав.

[9] Решение на Конституционния съд № 29 от 11.11.1998 г. по конституционно дело № 28 от 1998 г. (Обн. ДВ, бр. 135 от 17.11.1998 г.)

[10] Guidelines on Data Protection Officers (‘DPOs’), т. 2.1.1, стр. 6.

контролните им органи да се определят от държавни органи; да са обект на управленски контрол от държавни органи. Дори да отговарят на някой от изброените критерии, не е задължително те да осъществяват публични функции. Обстоятелството, че като задължени субекти по ЗДОИ са обхванати в категорията „публичноправен субект“, не дава основание тази постановка автоматично да се пренесе в материята на защитата на личните данни. Достъпът до обществена информация и защитата на личните данни преследват диаметрално противоположни цели, поради което позоваването на аналогията на закона в този случай ще е изключено. Предвид това дори даден субект да е публичноправна организация, за него не следва да произтича задължение да определяне на длъжностно лице по защита на данните само на това основание, а да се преценява дали упражнява властнически правомощия. При липсата на такива правомощия задължението за определяне на длъжностно лице по защита на данните би могло да произтича единствено от обработването на лични данни като основна дейност при условията на чл. 37, пар. 1, б. „б“ или „в“ от ОРЗД или от друга специална норма. Смятам, че този извод може да намери подкрепа и в насоките на Работната група по чл. 29, която отчита, че обществени функции могат да се осъществяват не само от публичните органи, но и от други физически или юридически лица, регулирани от законодателството на държавата членка. Това могат да бъдат случаите на предоставяне на административни услуги, водоснабдяване, дисциплинарни органи на регулирани професии и др. Работната група по чл. 29 препоръчва като добра практика частноправните субекти, изпълняващи обществени задачи, да определят такова лице. Неговите функции следва да обхващат всички операции по обработване на лични данни, включително тези, които не са свързани с изпълнение на задачата в обществен интерес.

2.2. Администратори или обработващи лични данни, чиито основни дейности изискват редовно и систематично мащабно наблюдение на субектите на данни

Тази хипотеза на задължително определяне на длъжностно лице по защита на данните е предвидена в чл. 37, пар. 1, б. „б“ от ОРЗД. За да бъде точно определено дали произтича задължение за даден администратор или обработващ лични данни на това основание да определи длъжностно лице по защита на данните, е необходим прецизен анализ, който да обхваща: определяне на основните им дейности; как се съотнася с тези основни дейности обработването на лични данни; дали се извършва наблюдение на субектите на данни; дали това наблюдение може да се квалифицира като „редовно“, „систематично“ и „мащабно“.

На първо място е необходимо да се определи какво означава „**основни дейности**“ на администратора или обработващия. Според съображение 97 на ОРЗД „в частния сектор основните дейности на администратора се отнасят до неговите първични дейности, а не до обработването на лични данни като вторични дейности“. Работната група по чл. 29 разглежда като „основни дейности“ ключовите операции за постигане на целите на администратора или обработващия. Те включват и всички дейности, при които обработването на данни представлява неделима част от дейността на администратора или обработващия. Тези насоки водят до няколко извода. За да се приема обработването на лични данни като основна дейност, то не трябва да се осъществява единствено защото способства другите задачи на администратора/обработвания. Това е важно уточнение, защото едно работодател, който има персонал, обработва личните данни на своите работници или служители. Това не означава непременно основна дейност по смисъла на ОРЗД, тъй като е възможно целта да е съвсем различна, например производство на автомобилни части. Обработването на личните данни на персонала в случая е необходимо с оглед изпълнение на специфични задължения, произтичащи от трудовото законодателство, но не би могло да се разглежда като основна дейност, а като вторична дейност или спомагателна функция.

Обработването на лични данни е основна дейност, когато има ключово значение за постигане на целите на администратора или обработващия. Такъв например би бил случаят на обработване на лични данни от дружество с предмет охранителна дейност, от болница или

от кредитна институция. Действително може да се твърди, че целта им е да гарантират сигурността на охранявания обект, да предоставят ефективни здравни услуги или да привлича влогове и да предоставя кредити, но изпълнението на тези цели не може да стане изолирано от обработването на лични данни. Обработването в такива случаи се явява необходимо условие за постигането им, поради което следва да се разглежда като основна дейност.

Съвсем очевидно обработването на лични данни ще е основна дейност, когато това е целта на администратора/обработващия. В тази група например могат да бъдат отнесени т.нар. „банки кадри“, агенциите за запознанства и др. подобни. Разликата с посочените по-горе случаи е в обстоятелството, че при тях обработването на лични данни следва от целите, а тук обработването на лични данни може да доведе до постигане на целите на такива администратори/обработващи. Независимо каква е причинно-следствената връзка, ако обработването на лични данни е от решаващо значение за целите на администратора или обработващия, това следва да се разглежда като тяхна основна дейност.

Какво означава „**наблюдение**“ по смисъла на чл. 37, пар. 1, б. „б“ от ОРЗД? Работната група по чл. 29 приема, че понятието наблюдение включва всички форми на проследяване и профилиране в интернет, включително за целите на поведенческата реклама. Това съответства на съображение 24 на ОРЗД, според което „с цел да се определи дали дадена дейност по обработване може да се смята за *наблюдение на поведението* на субекта 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“. Работната група по чл. 29 изяснява също, че понятието за наблюдение не се ограничава само до онлайн средата и проследяването в интернет е само един пример за наблюдение на поведението на субектите на данни. Този извод заслужава подкрепа, защото при дефиниране на дадено явление трябва да се изхожда от неговата същност, а не от технологията, по която тя може да се проявява. Освен това съображение 24 има предвид наблюдението на поведението на субектите, което може да води до тяхното профилиране, а наблюдението по чл. 37, пар. 1, б. „б“ е формулирано в много по-широк контекст, който не изисква евентуално последващо използване на техники за обработване на лични данни.

Не всякакво наблюдение на субектите на данни е релевантно за приложението на чл. 37, пар. 1, б. „б“ от ОРЗД, а се изисква то да бъде квалифицирано като „редовно“, „систематично“ и „мащабно“. Според Работната група по чл. 29 „**редовно**“ означава една или повече от следните хипотези: текущо или случващо се на определени интервали за определено време; случващо се или повтарящ се в определени срокове; постоянно или периодично провеждано. За „**систематично**“ се приема една или повече от следните хипотези: възникващо в съответствие със система; предварително подредено, организирано или методично; състоящо се като част от общ план за събиране на данни; предприето като част от стратегия. Като примери за дейности, които могат да представляват редовно и систематично наблюдение на субекти на данни, Работната група по чл. 29 посочва: експлоатация на телекомуникационна мрежа, предоставяне на телекомуникационни услуги, профилиране и оценяване с оглед преценка на риска (например при кредитен рейтинг, установяване на застрахователни премии), проследяване на местоположението от мобилни приложения, програми за лоялност, поведенческа реклама и др.

От решаващо значение за преценката дали да се определи длъжностно лице по защита на данните по чл. 37, пар. 1, б. „б“ от ОРЗД ще бъде квалифицирането на редовното и систематично наблюдение на субектите на данни като „**мащабно**“. Няма точни количествени измерители в Регламента, но съображение 91 съдържа важни насоки, в които да се извърши преценката. При мащабните операции по обработване целта е обработване на значителен обем лични данни на регионално, национално и наднационално равнище. Те могат да

засегнат голям брой субекти на данни и е вероятно да доведат до висок риск (поради чувствителност на данните или поради използваната при обработването технология). Не на последно място мащабните дейности по обработване на лични данни могат да затрудняват субектите да упражнят правата си.

Работната група по чл. 29 не изключва възможността с течение на времето да се развие стандартна практика за обективно, количествено определяне на мащабното обработване, като планира да допринесе за това развитие чрез споделяне и публикуване на примери за съответните прагове, при които е наложително определяне на длъжностно лице по защита на данните. В Насоките за длъжностните лица по защита на данните Работната група по чл. 29 препоръчва във всеки конкретен случай да се вземат под внимание следните фактори при определяне дали обработването е мащабно:

- Броят на засегнатите субекти на данни - като конкретен брой или като съотношение на населението;
- Обемът на данните и/или обхватът на различните обработвани данни;
- Продължителността или честотата на дейността по обработване на данни;
- Географският обхват на дейността по обработване.

Като примери за мащабно обработване се дават: обработването на данните за пациентите в нормалния ход на работа на болница; обработване на данни за клиентите в обичайната работа на застрахователни компании или банки; обработване на лични данни за поведенческа реклама от търсачки; обработване на данни (съдържание, трафик, местоположение) от доставчици на телефонни или интернет услуги и други. Практически е много полезен подходът на Работната група по чл. 29 да представи и примери, които не представляват мащабно обработване на лични данни, по-конкретно обработването на данните за пациентите от отделен лекар, обработването на данни за клиентите на отделен адвокат.

2.3. Администратори или обработващи лични данни, чиито основни дейности се състоят в мащабно обработване на специални категории данни и на лични данни, свързани с присъди и нарушения

Понятията „основни дейности“ и „мащабно“ са изяснени по-горе. В същия смисъл те следва да бъдат употребени и в тази хипотеза на задължително определяне на длъжностно лице по защита на данните, предвидена в чл. 37, пар. 1, б. „в“ от ОРЗД. Улеснението тук е наличието на легални дефиниции на другите използвани понятия, както и изричното препращане към разпоредбите на чл. 9 и 10 от Регламента.

За разлика от правилото на чл. 37, пар. 1, б. „б“, в настоящата хипотеза на задължително определяне на длъжностно лице по защита на данните е необходимо не „мащабно наблюдение“, а „мащабно обработване“ на лични данни. Терминът „обработване“, както вече беше споменато, е с много широко съдържание и се отразява на приложното поле на чл. 37, пар. 1, б. „в“ от ОРЗД. Логиката зад това законодателно решение е, че задължителното определяне на длъжностно лице по защита на данните е компенсаторна реакция на мащабното обработване на специални категории лични данни, извършвано като основна дейност. Специалните категории лични данни са изброени в чл. 9, пар. 1 от ОРЗД. Това са 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[11]. Приема се, че

[11] В сравнение с чл. 8, пар. 1 от Директива 95/46/ЕО, респ. чл. 5, ал. 1 от Закона за защита на личните данни, има промяна в понятието. От една страна в него са обхванати обработването на генетични данни, биометрични данни за целите единствено на идентифицирането на физическо лице, както и данните за сексуалната ориентация. От друга страна отпада квалификацията като специална категория на данните, свързани с членство в професионални съюзи и остава само членството в синдикални организации. В резултат на

контекстът на тяхното обработване може да създаде значителни рискове за основните права и свободи на физическите лица. Това налага и поставянето им под специален режим, който включва и определянето на длъжностно лице по защита на данните, когато обработването им е основна дейност и се извършва в голям мащаб.

Работната група по чл. 29 обръща внимание на редакцията на чл. 37, пар. 1, б. „в“ от ОРЗД. Въпреки че в нея обработването на специални категории данни и данни за престъпления и нарушения са дадени със съюза „и“, не съществува причина, поради която двата критерия трябва да се прилагат кумулативно. Предвид това мащабното обработване като основна дейност на специални категории данни *или* мащабното обработване като основна дейност на данни за присъди и нарушения ще води до задължително определяне на длъжностно лице по защита на данните. Във втория случай трябва да се отчита, че ОРЗД лимитира обработването на лични данни, свързани с присъди и нарушения. Според чл. 10 обработването следва да се извършва само под контрола на официален орган или когато обработването е разрешено от правото на ЕС или правото на държава членка, в което са предвидени подходящи гаранции за правата и свободите на субектите на данни. Пълен регистър на присъдите по наказателни дела, обаче, може да се поддържа единствено под контрола на официален орган. Несъмнено при поддържането на такъв пълен регистър ще сме изправени пред мащабно обработване на лични данни и ако то се извършва като основна дейност, ще се наложи определяне на длъжностно лице по защита на данните на основание чл. 37, пар. 1, б. „в“, предложение второ от ОРЗД. Това поставя въпроса дали бюрата за съдимост към районните съдилища и Централното бюро за съдимост при Министерството на правосъдието попадат в тази хипотеза. Несъмнено обработването на лични данни за съдимост е тяхна основна дейност, определена в нормативен акт[12] и същата може да се квалифицира и като мащабно обработване, предвид географския обхват на дейността. Централното бюро за съдимост изпълнява задълженията на централен орган, който обменя информация с централните органи на други държави членки относно влезлите в сила присъди на български и чужди граждани, вписани в регистрите за съдимост. За предаването и получаването по електронен път на тази информация Министерството на правосъдието създава и поддържа информационна система „Централна база данни „Съдимост“. При липса на правосубектност на Централното бюро за съдимост, администратор на личните данни ще се яви юридическото лице, в чиято структура то се намира, а именно Министерството на правосъдието. На основание чл. 37, пар. 1, б. „а“ от ОРЗД в Министерството на правосъдието трябва да има определено длъжностно лице по защита на данните, което няма пречки да осъществява и функциите си спрямо регистъра на личните данни, обработвани от Централното бюро за съдимост.

По-сложен от организационна гледна точка изглежда въпросът с бюрата за съдимост при районните съдилища. Те обработват данни за съдимост на лицата, родени в района на съда, които са осъдени от български съдилища, освободени от наказателна отговорност от български съдилища и са им наложени административни наказания по чл. 78а от Наказателния кодекс, както и за български граждани, осъдени от чуждестранни съдилища с влязъл в сила съдебен акт по наказателни дела, приет на изпълнение по реда на чл. 453-470 от Наказателно-процесуалния кодекс. Бюра съдимост се разкриват към всеки районен съд и са част от специализираната администрация, съгласно чл. 16, ал. 2, т. 9 във връзка с чл. 76 от Правилника за администрацията в съдилищата[13]. Съдилищата не са задължени да определят длъжностно лице по защита на данните на основание чл. 37, пар. 1, б. „а“ от ОРЗД. Изключението за тях, обаче, не е общо за всякакъв вид обработване на лични данни, а

това няма да се третират като чувствителни данните за членството в политически партии или организации, в сдружения с религиозни, философски и политически цели. Обработването им ще се осъществява на общите основания, приложими за личните данни.

[12] Уредбата се съдържа в разпоредбите на чл. 77, ал. 3 и 4, чл. 386 от Закона за съдебната власт и Наредба № 8 от 26 февруари 2008 г. за функциите и организацията на дейността на бюрата за съдимост

[13] Обн. ДВ, бр. 68 от 22 август 2017 г.

установено „при изпълнение на съдебните им функции“. Точното му разбиране е от изключително важно значение, защото определя и компетентността на надзорните органи (чл. 55, пар. 3 от ОРЗД). Според съображение 20 „компетентността на надзорните органи не следва да обхваща обработването на лични данни, когато съдилищата действат при изпълнение на своите съдебни функции, за да се гарантира независимостта на съдебната власт при изпълнението на съдебните й задължения, включително вземането на решения.“ Видно от този контекст и по аргумент от чл. 129, ал. 1 от Конституцията на Република България изразът „при изпълнение на съдебните им функции“, употребен в чл. 37, пар. 1, б. „а“ и в чл. 55, пар. 3 от ОРЗД, следва да се разбира в смисъл, че при осъществяване на правораздавателната си дейност съдилищата не подлежат на контрол от надзорния орган на държавата членка и не са задължени да определят длъжностно лице по защита на данните. Това не изключва задължението им на друго основание за определят длъжностно лице по защита на данните. В случая ще е приложима разпоредбата на чл. 37, пар. 1, б. „в“ от ОРЗД, когато сред основните дейности на районните съдилища се включва мащабно обработване на лични данни, свързани с присъди.

При практическото прилагане на задължението за определяне на длъжностно лице по защита на данните по чл. 37, пар. 1, б. „в“ от ОРЗД ключово ще се яви квалифицирането на обработването на данните като мащабно и едновременно с това като част от основните дейности на администратора или обработващия. Ако за функционирането на бюрата за съдимост обработването на лични данни за влезлите в сила присъди на лицата е основна дейност, то същото не може да се твърди в случая със събирането на такива данни от един работодател, когато за заемането на дадена длъжност се изисква чисто съдебно минало. Дори числеността на неговия персонал да е значителна, обработването на такива лични данни единствено способства другите му задачи, като доказва изпълнението на специфични нормативни изисквания, а не е основна негова дейност.

3. Определяне на длъжностно лице от обработващия лични данни

Изискванията по чл. 37, пар. 1 от ОРЗД се отнасят както до администраторите, така и до обработващите лични данни. Според съответствието с предвидените критерии, длъжностно лице по защита на данните ще трябва да определи не само администраторът, но и обработващият лични данни, за когото също са изпълнени тези критерии. Работната група по чл. 29 изрично посочва, че дори администраторът да отговаря на критериите за задължително определяне на длъжностно лице по защита на данните, не е задължително неговият обработващ данните да определи такова лице, но това може да бъде добра практика. При отчитане на тази насока, се налага изводът, че задължението по отношение на обработващия ще се преценява според неговата правноорганизационна структура или според особеностите на дейността му по обработване на лични данни. Ако тя попада в изискванията на чл. 37, пар. 1 от ОРЗД, определянето на длъжностно лице по защита на данните ще произтича като задължение за обработващия. В този смисъл задължението за определяне на длъжностно лице по защита на данните произтича на самостоятелно основание за администратора и за обработващия.

Напълно възможно е и примерът, който Работната група по чл. 29 дава, потвърждава, че е възможно за администратора да не произтича задължение за определяне на длъжностно лице по защита на данните, но такова да произтича за обработващия, на когото този администратор е възложил обработването на данните. Примерът се отнася до малък семеен бизнес, който се занимава с разпространение на домакински уреди в един град. При дейността си той използва услуги на обработващ данни, чиято основна дейност е да предоставя услуги за анализ на уебсайтове и съдействие за целенасочена реклама и маркетинг. Дейността на семейния бизнес и неговите клиенти не генерират мащабно обработване на данни, като се има предвид малкия брой клиенти и относително ограничените дейности. Независимо от това, дейността на обработващия, който има много клиенти като това малко предприятие, взети заедно, води до мащабно обработване. В този

случай Работната група по чл. 29 прави извод, че обработващия е длъжен да определи длъжностно лице по защита на данните по силата на чл. 37, пар. 1, б. „б“, а за семейния бизнес не произтича такова задължение.

Необходимо е да се отчита, че не може да има сливане на правните качества „администратор“ или „обработващ“ по отношение на един и същи регистър лични данни (структуриран набор от лични данни). Това е така, защото именно възлагането от страна на администратора на друг правен субект извън неговата структура да обработва тези лични данни, води до придобиването на правното качество обработващ и обработването става от името на администратора. Това, обаче, не изключва възможността един и същи правен субект да е едновременно обработващ (за личните данни, които обработва по възлагане от администратор) и администратор (за личните данни, за които той определя целите и средствата за обработване). Видно е, че това ще е възможно за различни регистри на личните данни. В случая с примера на Работната група по чл. 29 обработващият може да е администратор на личните данни за своя персонал. В този контекст смятам, че е от особено значение да се отчита добрата практика, която Работната група по чл. 29 препоръчва, а именно длъжностното лице, определено от обработващия личните данни, да наблюдава и дейностите по обработване, които той извършва и в качеството си на администратор. Това е в интерес на защитата на данните, а и има потенциал да оптимизира дейностите по тяхното обработване.

Д-р Невин Фети, юрист