



SHUTTERSTOCK

Професия „Пазител на данните“

В кои случаи фирмите трябва да назначат служители за защита на данните и какви са техните задачи

автор
Митко Карушков*

Длъжностното лице по защита на данните не е нова професия. И преди влизането в сила на GDPR в България съществува подобна работна функция – тя се нарича „лице по защита на личните данни“ и е регулирана в Наредба №1 на Комисията за защита на личните данни (КЗЛД). Целта на тези служители е да следят техническите детайли и организацията на работата с лични данни.

Новата длъжност Data Protection Officer (DPO), или длъжностно лице по защита на данните (ДЛЗД), се появява заради развитието на технологиите, порастването на обемите с данни и нуждата от допълнителни компетентности в работата с данни. Регламентът продължава еволюцията в развитието на работата с данни и предвижда, че за определени групи администратори или обработващи данни е задължително определянето на DPO. Неговата функция по същество си не се отличава от познатото в България и други страни „лице за защита на личните данни“ и от

тази гледна точка това няма да представлява съществена новост за една част от компаниите и организациите, работещи с лични данни.

Тъй като регламентът въвежда основни изисквания към тази позиция, нейните функции и други задължения, е необходимо компаниите да съобразят наличните си практики с изискванията на регламента. Към днешна дата немалко компании и организации са определили отделни специалисти, които изпълняват функцията на ДЛЗД. Доколкото при такъв избор страните са съобразили експертността и другите качества, тези ДЛЗД би трябвало спокойно и необезпокоявано да упражняват своята дейност. Все пак при евентуално въвеждане на допълнителни изисквания би могло да е необходимо компаниите и ДЛЗД да проверят дали ДЛЗД отговарят на такива (евентуални) допълнителни изисквания.

Нужните квалификации

Според регламента длъжностното лице по защита на данните трябва да отговаря на изисквания в две основни направления – експертност и професионализъм. DPO специалистите трябва да имат познания и практически опит при прилагането и тълкуването на национални или европейски регулации в областта на защита на личните данни, включително познаване на регламента. GDPR не изисква упражняването на конкретна професия. Тоест не е въведено специфично изискване за юридическа, ИТ, счетоводна или друга професионална квалификация, която да бъде задължителна в това отношение. С цел конкретизиране на изискванията към професионалната квалификация може да се очаква Комисията за защита на личните данни да изработи правила, които внасят допълнителна яснота относно евентуални допълнителни изисквания към специалистите с тази функция.

За тази позиция ще са нужни и умения и познания в операциите по обработване на данни в дадена компания или организация. Свободното боравене с информационни технологии, приложения, ориентацията в използването на различни видове софтуер, познаването на ИТ инфраструктура, сигурността на данните в стандартна,

цифрова и електронна среда са допълнителни практически умения, които биха спомогнали за адекватно упражняване на функцията на DPO.

Знания, умения и опит в определен сектор на бизнеса, икономиката, администрацията, професионалния или обществен живот също биха представлявали конкурентно предимство. Познаването на съответната организация или компания също може да бъде прието като необходимо условие за упражняване на тази функция. Когато се наема външен експерт обаче, това познаване не настъпва автоматично, а също така може да срещне практически ограничения. За подобни случаи GDPR е предвидил определени изисквания към фирмите и институциите за оказване на съдействие към специалистите по защита на личните данни.

Кой не може да бъде ДЛЗД

В тази роля категорично не може да влезе мениджмънтът. Висшият мениджмънт, както и други звена от средното ниво на управление в дадена организация нямат право да съвместяват своите задължения с функцията на DPO. При евентуално комбиниране на такива функции се достига до конфликт на интереси по отношение обработването на данни, тъй като мениджърите определят целите и насоките на обработване на данни, а DPO има за функция да контролира и съветва дали така определените цели и действията по изпълнението им са законосъобразни.

Какво прави егия DPO

Съветва, докладва, информира. Работата на длъжностното лице е да съветва компаниите или институциите, които използват лични данни. Той трябва да докладва директно на висшия мениджмънт по различни групи въпроси, отнасящи се до съответствието на практиките на дадена организация с GDPR и другите регулации в областта на защита на данните, в това число националните закони. DPO има ангажимент да информира и съветва отделните служители, които имат достъп до лични данни в организацията, относно законосъобразността на

дадена практика, процес или действие по обработване на данни.

Анализира, проверява, контролира. Той следва да събира информация и да анализира дейностите по обработване на данни в дадена организация, да анализира и проверява изпълнението на дейностите по обработване; да информира, съветва и отправя препоръки към администратора или обработващия лични данни. Тези и други функции са препоръчани като добри практики в становище на Работната група по чл. 29 – орган със съветнически функции в структурата на ЕС.

Дава становище при извършване на оценка на въздействието върху защитата на данните. Според GDPR тази процедура е задължение на администратора на лични данни. DPO предоставя съвети, наблюдава и дава становища при евентуалното извършване на такава процедура. Това подчертава и необходимостта от определено ниво на експертност или много високо ниво на потребителска култура при използване на нови технологии за обработването на данни в дадена компания или организация. В тази хипотеза администраторът не е задължен да приеме съветите на ДЛЗД, но в такива случаи неприемането и причините за него трябва да бъдат документирани.

Съдейства, служи като точка за контакт. Специалистът има задължението да съдейства на надзорните органи, включително да ги уведомява при евентуален пробив и изтичане на лични данни. DPO следва да бъде достъпен и за субектите на данни – клиенти или други граждани, ползващи услугите на дадена компания или организация.

Отчита рискове, води регистри. Наблюдавайки процесите по обработка на данни, DPO следва да отчита евентуалните рискове от неправомерно изтичане на данни и да съобразява естеството, целите и обхвата на обработката. На практика това означава, че специалистът може да повлияе върху начините на обработване на данни в дадена компания или организация. Той може, но не е длъжен, да води различни видове регистри относно дейностите по

За DPO специалистите няма специфично изискване за юридическа, IT, счетоводна или друга професионална квалификация, но те трябва да познават национални или европейски регулации в областта на защита на личните данни.

обработка на данни в дадена организация или компания. Този въпрос може да бъде уточнен с договор между администратора и съответния DPO.

Задължително ли е назначаване на такъв служител

GDPR предвижда три случая, в които задължително трябва да бъде назначено длъжностно лице за защита на личните данни: когато обработването се извършва от публичен орган или структура; когато основната дейност на организацията се състои в обработване на данни, които изискват редовно и систематично мащабно наблюдение на субектите на данни; когато основните дейности на организацията се състоят в мащабно обработване на специални категории данни или на лични данни, свързани с присъди и нарушения.

Определянето дали е задължително назначаване на DPO следва да се извърши при анализ на всяка конкретна организация, като тази преценка следва да се документира и мотивира. Възможно е в ситуации, в които не е задължително

да се назначи DPO, все пак такъв да бъде назначен. Отново преценката за това следва да се извърши при анализ на конкретната организация.

Отговорност на специалистите по защита на данни

Експертите не носят лична отговорност в случай на нарушаване на правилата относно защита на лични данни. Регламентът е предвидил, че такава отговорност носят администраторът и обработващият лични данни. Все пак DPO може да носи отговорност във вътрешните отношения с администратора или обработващия данни - въз основа на договор или друг правен акт. Предвиждат се и такава отговорност в договор е препоръчително да бъде извършено с оглед спецификите на отделните случаи, като е необходимо да се има предвид, че според регламента той има определена самостоятелност и независимост спрямо компанията или институцията, която го е наела. ●

* авторът е от „Камбуров и партньори“

ЧУВСТВТЕЛНИ ЛИЧНИ ДАННИ

сексуална
ориентация



раса и
етнически произход



политически
мнения



По принцип GDPR

забранява събирането на чувствителни лични данни, но има и някои изключения.

Те са: изрично съгласие, законодателството го изисква, защита на жизненоважен интерес и др. Компаниите, които обработват такива данни са длъжни да имат служител по защита на личните данни.

религиозни
и философски
разбирания



членство в
синдикати



генетични
данни



биометрични
данни



здравен статус
и заболявания

