СТАТИИ

ОБЩИЯТ РЕГЛАМЕНТ ОТНОСНО ЗАЩИТАТА НА ДАННИТЕ И АДВОКАТСКАТА ПРОФЕСИЯ

Йорданка Иванова*

Много адвокати са вероятно твърде добре запознати с Регламент (ЕС) 2016/679 относно защитата на личните данни[1] (наричан за краткост „Регламентът"), определян от мнозина анализатори като най-мащабната и смела реформа, която се очаква да преобърне режима на защита на личните данни не само в Европейския съюз, но и далеч отвъд неговите граници. Без съмнение правните услуги за привеждането на всички организации на частното и публичното право в съответствие с Регламента са особено актуални след 25 май 2018 г., когато Регламентът се прилага пряко във всички държави – членки на Европейския съюз, в това число и България.

Но дали всички адвокатски кантори и самостоятелно действащи адвокати в страната са също така добре запознати и готови да докажат, че спазват Регламента, когато събират и обработват лични данни на физически лица във връзка с предоставяните от тях правни услуги?

Именно с цел да подпомогне адвокатите в процеса на подготовка за прилагането на Регламента тази статия ще се опита да изведе някои от основните изменения в режима на защита на личните данни, като анализира особености и изключения, които ще са приложими при упражняването на адвокатската професия след месец май 2018 г.[2]

---

* Адвокат от София. Статията е изготвена по възлагане от Фондация „Институт за правна информация".

[1] 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), OJ L 119, 4.05.2016, p. 1–88.

[2] Извън обхвата на анализа ще остане обработването на личните данни на работниците и/или служителите, наети от адвокатските кантори в качеството им на работодател, тъй като това е тема, относима към всички организации, която заслужава сама по себе си отделно изследване.

1. Защо защитата на личните данни е важна за адвокатската професия?

Като за начало е удачно да се кажат няколко думи защо защитата на личните данни е особено важна за адвокатската професия. Освен че новите завишени изисквания на Регламента ще са приложими на общо основание към адвокатите, самото естество на адвокатската работа върви ръка за ръка с редица правни и етични задължения, пряко или непряко свързани със защитата на личните данни. На първо място, адвокатът играе особена роля в обществения живот, като едно от основните му етични задължения е да съдейства за утвърждаване на върховенството на закона, включително като сам дава пример за спазването на българското и европейското законодателство.[3] По-важно в случая обаче е законовото и първостепенно задължение на адвоката да гарантира поверителността и сигурността на информацията, получена във връзка с възложената му работа, като пази тайната на своя клиент без ограничение във времето и изисква опазването ѝ от своя персонал и от всяко лице, с което си сътрудничи в професионалната дейност.[4] Потенциално загубване или нарушаване по друг начин на сигурността на тази информация (включително лични данни) могат сериозно да увредят интересите на клиента, неговите права и свободи. Освен това адвокатът често борави с чувствителна информация, като по закон има право на много широк достъп до информация от праворазадавателни и други държавни органи.[5] Не на последно място, адвокатите може да са специален обект на атаки на сигурността и следва да вземат сериозни мерки за защита на поверителността и интегритета на получената информация, за което новите изисквания на Регламента могат без съмнение да спомогнат.

2. Приложимост на новите изисквания на Регламента към адвокатската професия

Регламентът въвежда редица изменения в сега действащия режим на защита на личните данни съгласно Закона за защита на личните данни и Директива 95/46/ЕО, като значително завишава изискванията за обработването на лични данни от всички организации на частното и публичното право[6] и създава единна европейска правна рамка, директно приложима във всички държави – членки на ЕС. Новите засилени мерки ще имат пряко отношение към отговорността и задълженията на адвокатите, като неспазването им може да доведе до сериозни санкции в размер до 20 млн. евро или 4 % от годишния оборот на адвокатската кантора или адвоката на самостоятелна практика. Основните нововъведения ще бъдат разгледани по-долу, като специално

[3] Член 40 от Закона за адвокатурата.
[4] Член 45 от Закона за адвокатурата и чл. 5 от Етичния кодекс на адвоката.
[5] Член 31 от Закона за адвокатурата.

внимание ще бъде отделено на предвидените изключения, от които адвокатите ще могат да се ползват при упражняване на своята професия.

2.1. По-широка дефиниция на личните данни и специална категория данни

Първата важна промяна е свързана с по-широката **дефиниция на понятието „лични данни“**, която занапред ще обхваща всяка информация, свързана не само с идентифицирано физическо лице, но и с такова, което може да бъде идентифицирано (наричано в Регламента и анализа „субект на данни“). Лицето може да бъде идентифицирано пряко или непряко, по-специално чрез идентификатор (като име, ЕГН, местонахождение, IP адрес), или по един или повече признаци, специфични за неговата физическа, физиологична, генетична, психическа, умствена, икономическа, културна или социална идентичност.[7] Данни, свързани с юридически лица, не попадат в приложното поле на Регламента, доколкото не са свързани с физическо лице.

Особено важно е да се отбележи, че Регламентът по принцип ограничава обработването на **специална категория лични данни**, т.нар. чувствителни данни, разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения или членство в синдикални организации, както и обработването на генетични данни, биометрични данни за целите единствено на идентифицирането на физическо лице, данни за здравословното състояние или данни за сексуалния живот или сексуалната ориентация на физическото лице.[8] Предвидени са обаче някои изключения от общата забрана, на които адвокатите биха могли да се позоват и свободно да обработват такива „чувствителни“ лични данни (което всъщност нерядко им се налага на практика), доколкото обработването е необходимо с цел установяване, упражняване или защита на правни претенции.[9]

Съществуват ограничения при обработването и на **лични данни, свързани с присъди и нарушения** или със свързаните с тях мерки за сигурност, което може да

[6] Задължени да спазват Регламента са всички организации на частното право, включително търговски дружества, кооперации, неправителствени организации, политически партии и други формирования, както и публични органи, органи на местно самоуправление, свободни професии, когато обработват лични данни. Съгласно чл. 2, ал. 2 Регламентът не се прилага само спрямо физически лица в хода на чисто лични или домашни занимания, както и при някои други, изрично изключени хипотези от държавни органи при осъществяване на Общата европейска политика в областта на външните отношения и сигурността, както и за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наложените наказания, включително предпазването от и предотвратяването на заплахи за обществената сигурност.

[7] Член 4, ал. 1 от Регламента.

[8] Член 9, ал. 1 от Регламента.

[9] Член 9, ал. 2, б. „е“ от Регламента.

се извършва само под контрола на официален орган или когато обработването е разрешено от правото на Съюза или правото на държава членка, в което са предвидени подходящи гаранции за правата и свободите на субектите на данни.[10] Би могло да се заключи, че адвокатите могат да боравят свободно с лични данни, свързани с присъди и нарушения, доколкото съгласно чл. 31 от Закона за адвокатурата те разполагат със свободен достъп и могат да правят справки по дела, да получават копия от книжа и сведения с предимство от правораздавателните органи и други служби в страната и навсякъде, където е необходимо.

2.2. Разграничение между „администратор“ и „обработващ лични данни“

Друга съществена промяна, която Регламентът въвежда, е ясното **разграничение** между отговорността и задълженията на **администратор на лични данни** и **обработващ лични данни**.[11] Така например адвокатите ще могат да ограничат своята отговорност и да действат като „обработващ лични данни“, когато действат от името на клиент – „администратор на лични данни“, въз основа на договор, в който се определят предметът и срокът на действие на обработването, естеството и целта на обработването, видът лични данни и категориите субекти на данни, задълженията и правата на администратора, а също така са изпълнени всички изисквания, предвидени в чл. 28, ал. 3 от Регламента.[12] Стандартни клаузи, които да бъдат включени в дого-

[10] Член 10 от Регламента.

[11] Член 24–31 от Регламента.

[12] Например адвокатът трябва да обработва личните данни само по документирано нареждане на клиента „администратор“, освен когато има законово задължение за това. Адвокатът също така следва да гарантира, че лицата, оправомощени да обработват личните данни, са поели ангажимент за поверителност или са задължени по закон да спазват поверителност (например адвокатска тайна). При включване на друго лице, обработващо данни (например друг адвокат), адвокатът трябва да получи преди това съгласието на клиента и да му представи достатъчно гаранции за прилагане на подходящи технически и организационни мерки от подизпълнителя, за неспазването на които адвокатът също носи отговорност. Адвокатът е длъжен още да подпомага клиента при изпълнението на задължението му на „администратор“ да отговори на искания за упражняване на правата на субектите на данни, както и при нарушения на сигурността на личните данни (вж. т. 2.5 по-долу). Доколкото адвокатът има законово задължение да пази книжата по делата в продължение на 5 години от приключването им, той следва да откаже заличаването или връщането на личните данни, ако клиентът поиска това преди изтичането на този срок. Следва да се предвиди възможност клиентът администратор при необходимост да извършва одити, включително проверки, но само за книжата по възложените от него дела, тъй като чл. 33, ал. 1 от Закона за адвокатурата предвижда, че адвокатските книжа, досиета, електронни документи, компютърна техника и други носители на информация са неприкосновени и не подлежат на преглеждане, копиране, проверка и изземване.

ворите между „администратор“ и „обработващ данни“, предстои да бъдат предложени от Европейската комисия, а междувременно френската Комисия за защита на личните данни (CNIL) вече е предложила примерни такива.[13]

Макар и с по-ниска отговорност и задължения, адвокатите, действащи като „обработващи данни“ от името на свои клиенти – „администратори на данни“, също следва да предоставят достатъчни гаранции за прилагането на подходящи технически и организационни мерки в съответствие с изискванията на Регламента и да осигурят защита на правата на субектите на данни.[14] Предвид правомощията на Комисията по защита на личните данни (КЗЛД) да налага значителни имуществени санкции при неизпълнение на Регламента (до 4 % от годишния оборот)[15], а също и предвид възможността увредени субекти на данни да търсят обезщетение[16], препоръчително е да се предвиди клауза в договора за ограничаване на отговорността до определен размер.

Адвокатите също трябва да прегледат договореностите си с „обработващи лични данни“ от тяхно име (например IT фирми, счетоводни къщи, охрана), за да са сигурни, че ползват услугите на организации, които спазват изискванията на Регламента, и договорите съдържат посочените по-горе специални клаузи и гаранции.

2.3. Принципи, свързани с обработването на лични данни

Регламентът извежда на първостепенно място редица принципи[17], които трябва винаги да се спазват при обработването на лични данни, в това число принципите на законосъобразност, добросъвестност и прозрачност, ограничение на целите[18], ограничение на съхранението[19], свеждане на данните до минимум[20], точност[21], ця-

[13] Достъпни на https://www.cnil.fr/fr/sous-traitance-exemple-de-clauses.

[14] Член 28, ал. 1 от Регламента.

[15] Член 83, ал. 5 от Регламента.

[16] Член 82 от Регламента.

[17] Член 5 от Регламента.

[18] Данните трябва да се събират за конкретни, изрично указани и легитимни цели и да не се обработват по-нататък по начин, несъвместим с тези цели.

[19] Данните трябва да се съхраняват във форма, която да позволява идентифицирането на субекта на данните за период, не по-дълъг от необходимото за целите, за които се обработват личните данни; личните данни може да се съхраняват за по-дълги срокове, доколкото ще бъдат обработвани единствено за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели.

[20] Данните трябва да са подходящи, свързани със и ограничени до необходимото във връзка с целите, за които се обработват.

[21] Данните трябва да са точни и при необходимост да бъдат поддържани в актуален вид; трябва да се предприемат всички разумни мерки, за да се гарантира своевременното изтриване или коригиране на неточни лични данни, като се имат предвид целите, за които те се обработват.

лостност и поверителност на личните данни[22]. Макар тези принципи да са съществували в голямата си част и досега, в Регламента те намират много по-конкретно изражение в задълженията и изискванията, които администраторите и обработващите лични данни трябва да спазват, като някои от основните промени ще бъдат разгледани по-долу в анализа.

2.3.1. Законосъобразност

Принципът на законосъобразност изисква винаги да съществува законово основание, когато се събират и обработват лични данни на физическите лица. Затова основната промяна спрямо сега действащия режим са значително по-строгите изисквания за съгласието, което трябва да е дадено чрез ясно утвърдителен акт, с който да се изразява свободно дадено, конкретно, информирано и недвусмислено заявление за съгласие от страна на субекта на данни.[23] Смята се, че съгласието не е дадено свободно, ако не се предоставя възможност да бъде дадено отделно съгласие за различните операции по обработване на лични данни, макар и да е подходящо в конкретния случай, или ако изпълнението на даден договор, включително предоставянето на услуга, се поставя в зависимост от даването на съгласие, въпреки че това съгласие не е необходимо за изпълнението.[24] Трябва да е предвидена и възможност субектът на данни да оттегли съгласието си по всяко време, като това трябва да става толкова лесно, колкото и даването му, и субектът на данни да е предварително информиран за това.[25]

Всички тези нови изисквания превръщат съгласието в сравнително нестабилна законова основа за обработването на данни. Това, както и необходимостта да се определи точното законово основание за обработването налага задълбочен анализ предвид голямата вероятност адвокатите всъщност да обработват данните въз основа на други законови основания, в това число[26]:

– изпълнението на договор (например при сключен договор за правна защита и съдействие, при който събирането на личните данни е необходимо за защитата на правата и законните интереси на клиента), или

– защитата на жизненоважни интереси на субекта на данните или на друго физическо лице (например когато лични данни се събират за друго физическо лице, което застрашава или е увредило жизненоважни интереси на клиента), или

---

[22] Данните трябва да се обработват по начин, който гарантира подходящо ниво на сигурност на личните данни, включително защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане, като се прилагат подходящи технически или организационни мерки.

[23] Член 4, т. 11 от Регламента.

[24] Съображение 43 от Регламента.

[25] Съображение 32 и чл. 7 от Регламента.

[26] Член 6, ал. 1 от Регламента.

– съществуването на законово задължение по българското или европейското право, което задължава адвоката да събира данните (например задължение да се узнае точно самоличността на клиента[27] или задължения, свързани с мерки против изпирането на пари), или

– наличието на легитимни интереси на адвоката или на клиента му, освен когато пред такива интереси преимущество имат интересите или основните права и свободи на субекта на данните, които изискват защита на личните данни, по-специално, когато субектът на данните е дете.

Когато съществува някое от тези други законови основания, адвокатите не трябва да искат съгласието на лицето, когато събират и обработват свързани с него лични данни.

2.3.2. Отчетност

Сред най-съществените промени в режима на защита на личните данни са завишената отговорност и новият принцип на отчетност на всички организации на частното и публичното право, които трябва да са в състояние да докажат, че спазват всички принципи и изисквания при обработването на лични данни.[28] В това отношение Регламентът радикално променя съществуващия досега режим, като прехвърля тежестта на доказване върху самите компании и организации за сметка на много от досегашните административни процедури по регистрация и докладване към надзорния орган, които ще отпаднат занапред. До 25 май 2018 г., откогато Регламентът се прилага, всички организации (включително адвокатите на самостоятелна практика) трябва да са приели съответните организационни и технически мерки, за да гарантират, че спазват Регламента. Такива мерки включват *inter alia* гарантиране на сигурността на данните, приемане на вътрешни процедури и правила за обработване и защита на личните данни, изготвяне на уведомления за поверителност, водене на вътрешни регистри за обработването на лични данни, назначаването при необходимост на длъжностно лице по защита на личните данни, извършване на оценка на въздействието върху защитата на данните и др., част от които ще бъдат разгледани по-нататък в анализа.

2.3.3. Прозрачност

В изпълнение на този принцип адвокатите следва да прегледат като начало цялата информация, която предоставят на физическите лица преди обработването на личните им данни (например уведомления за поверителност, политика за защита на личните данни), винаги когато действат като администратори на лични данни. Важно е да се отбележи, че това задължение съществува независимо от правното основание, въз основа на което се обработват личните данни, т.е. и в случаи, в които не се иска

[27] Член 11, ал. 3 от Етичния кодекс на адвоката.

[28] Член 6, ал. 2 от Регламента.

съгласието на физическите лица. Новите изисквания налагат предоставянето на кратка, прозрачна, разбираема информация в леснодостъпна форма, представена на ясен и прост език[29], която включва всички елементи, посочени в чл. 13, ал. 1 от Регламента. Във връзка с това Насоките на Работна група 29[30] относно принципа на прозрачност[31] допълнително изискват да се избягват сложни, условни и абстрактни формулировки, както и прекалено правна или техническа терминология. Информацията трябва да се предостави безплатно, като адвокатите не могат да събират такси във връзка с това.[32]

2.4. Повече и по-лесни за упражняване права на субектите на данни

Регламентът значително разширява и улеснява упражняването на правата на субектите на данни, посочени в чл. 14–22 от Регламента. Когато действат като „администратор на данни", адвокатите следва да осигурят възможност на субектите на данни да упражняват тези свои права, като разгледат исканията им в срок до 1 месец.[33] По-долу ще бъдат разгледани само някои от посочените права, доколкото съществуват особености при упражняването на адвокатската професия, които предвиждат изключения от общите правила.

Специално внимание следва да се обърне на **правото на информираност**, пряко свързано с принципа на прозрачност, разгледан по-горе. Съществуват две хипотези в зависимост от това дали адвокатът получава информацията пряко от субектите на данни[34] (с тяхно знание или чрез наблюдение през камери, следене на wifi и др.), или опосредствано[35] (чрез други организации, публично достъпни ресурси, други физически лица, в това число клиенти и т.н.). В първата хипотеза на директно събиране на данни адвокатът е длъжен да предостави на субекта на данни информацията във връзка с обработването в подходящ период от време преди самото събиране на данните. Във втората хипотеза на непряко събиране на данни адвокатът отново е длъжен

[29] Член 12, ал. 1 от Регламента.

[30] Това е работна група по защита на личните данни, създадена на основание чл. 29 от Директива 95/46/ЕО, която има за задача да разработва допълнителни указания/насоки по прилагането на европейската правна рамка за защита на личните данни. След влизане в сила на Регламента Работната група ще се нарича Европейски комитет по защита на данните и ще включва ръководителите на надзорните органи на всяка държава членка и на Европейския надзорен орган по защита на данните или съответните им представители. Представител на Европейската комисия участва в дейностите на Комитета без право на глас.

[31] Достъпни на http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=615250.

[32] Член 12, ал. 5 от Регламента.

[33] Член 12, ал. 2 и 3 от Регламента.

[34] Член 13 от Регламента.

[35] Член 14 от Регламента.

да уведоми субектите на данни най-късно до един месец след получаване на данните им. Съществуват обаче изключения, които могат да го освободят от задължението за уведомяване, когато:

– получаването или разкриването е изрично разрешено от правото на Съюза или правото на държавата членка[36] – например чл. 31 от Закона за адвокатурата, който предвижда, че адвокатите имат право на много широк достъп до информация с предимство в съда, органите на досъдебното производство, административните органи и други служби в страната и навсякъде, където е необходимо;

– личните данни трябва да останат поверителни при спазване на задължение за опазване на професионална тайна[37], в случая адвокатска тайна. Такъв би бил например случаят, в който клиентът предоставя информация на адвоката си, в която се съдържат лични данни за други физически лица. Позовавайки се на задължението си за поверителност, адвокатът не бива да уведомява тези други физически лица, че разполага с данни за тях, тъй като това би нарушило задължението му да опази адвокатската тайна.

Друго право, което заслужава специално внимание, е най-новото признато право на субектите на данни да искат **изтриването на личните си данни, или т.нар. право да бъдеш забравен**, прогласено от Съда на ЕС[38] и предвидено в чл. 17 от Регламента. То съвсем обаче не е абсолютно и съществуват определени изключения, на които администраторите на данни могат да се позовават. Така например адвокатите могат да откажат изтриването на лични данни, когато обработването на данни е необходимо за установяването, упражняването или защитата на правни претенции[39], а също и на общо основание за спазването на правно задължение, например предвиденото в чл. 47 от Закона за адвокатурата задължение на адвокатите да пазят книжата по делата в продължение на 5 години от приключването им.

Особеност съществува и при новопризнатото **право на прехвърлимост на личните данни**, което при поискване задължава адвоката да предостави на субекта на данни свързаните с него лични данни в „структуриран, широко използван и пригоден за машинно четене формат“, когато обработването е автоматизирано и основано на съгласие или договорно задължение.[40] Докато предоставянето на данните в „широко използван“ и „пригоден за машинно четене формат“ едва ли ще представлява проблем за адвокатите, изискването за „структурираност“ може да се окаже потрудноизпълнимо, тъй като повечето правни документи са неструктурирани по съ-

[36] Член 14, ал. 5, буква „в“ от Регламента.

[37] Член 14, ал. 5, б. „г“ от Регламента.

[38] По дело C-131/12 *Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, ECLI:EU:C:2013:424.

[39] Член 17, ал. 3, б. „б“ и „д“ от Регламента.

[40] Член 20 от Регламента.

държание и в адвокатската практика липсва общоприет формат за предаване на пълни досиета или дела.[41]

2.5. Сигурност на данните

Сигурността на данните е друга ключова област, където Регламентът съществено завишава изискванията, като адвокатите ще трябва занапред да прилагат подходящи технически и организационни мерки за осигуряване на съобразено с оценения риск ниво на сигурност, включително защита срещу неразрешено разкриване или достъп до данни, както и случайно или неправомерно унищожаване, загуба или промяна на данните. Тези мерки може да включват *inter alia* псевдонимизация[42] и криптиране на личните данни, способност за гарантиране на постоянна поверителност, цялостност, наличност и устойчивост на системите и услугите за обработване, способност за своевременно възстановяване на наличността и достъпа до личните данни и процес на редовно изпитване, преценяване и оценка на ефективността на техническите и организационните мерки.[43] До 25 май 2018 г. минималните мерки бяха регламентирани в Наредба № 1 на КЗЛД[44], която ще бъде актуализирана в съответствие с Регламента и трансформирана в методическо ръководство.

Съществена промяна е новото задължение при нарушение на сигурността на данните адвокатът да уведоми без ненужно забавяне и при всички положения не покъсно от 72 часа:

– **клиента**, когато адвокатът действа като „обработващ лични данни" от името на клиента – „администратор на данни" (вж. т. 2.2 по-горе). В този случай, когато установи нарушение на сигурността, адвокатът е длъжен да уведоми клиента, без да преценява вероятността и риска вредите да настъпят[45], или

---

[41] Насоки на Европейския адвокатски съвет относно основните мерки за адвокатите по изпълнение на Общия регламент за защита на данните, 19.05.2017 г., достъпни на http://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/IT_LAW/ITL_Position_papers/EN_ITL_20170519_CCBE-Guidance-on-main-new-compliance-measures-for-lawyers-regarding-GDPR.pdf.

[42] Съгласно чл. 4, ал. 5 „псевдонимизация" означава обработването на лични данни по такъв начин, че те не може повече да бъдат свързвани с конкретен субект на данни, без да се използва допълнителна информация, при условие че тя се съхранява отделно и е предмет на технически и организационни мерки, с цел да се гарантира, че личните данни не са свързани с идентифицирано физическо лице или с физическо лице, което може да бъде идентифицирано.

[43] Член 32 от Регламента.

[44] Наредба № 1 от 30 януари 2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни (отм.).

[45] Член 33, ал. 2 от Регламента.

– **КЗЛД**, когато адвокатът действа като „администратор на лични данни“ – винаги когато съществува вероятност нарушението на сигурността на личните данни да породи *риск* за правата и свободите на физическите лица[46], и

– **засегнатите субекти на данни**, когато адвокатът действа като „администратор на данни“ – винаги когато съществува вероятност нарушението на сигурността на личните данни да породи *висок риск* за правата и свободите на физическите лица.[47]

При оценката на риска е важно да се отбележи, че съгласно Съображение 75 и 85 от Регламента висок риск за субектите на данни ще има винаги когато нарушението може да доведе до физически, имуществени или неимуществени вреди за лицата, чиито данни са били засегнати, като например нарушаване на поверителността на личните данни при разкриване на професионална тайна, дискриминация, кражба на самоличност или измама, имуществени загуби или засягане на репутацията. Когато нарушението на сигурността се отнася до „чувствителни данни“ или данни, свързани с присъди и нарушения, също трябва да се счита, че такива вреди е вероятно да настъпят.

Така повишаването на сигурността се оказва от изключително значение за адвокатите като ключова мярка в привеждането на дейността им в съответствие с Регламента, тъй като допуснато нарушение на сигурността на данните на клиента е много вероятно да породи висок риск за неговите права и да наложи съответно той и КЗЛД да бъдат уведомени за нарушението, в случай че адвокатската тайна е била разкрита или нарушението засяга чувствителна информация. Допускането на такива нарушения следователно може не само сериозно да навреди на репутацията на адвоката, но и да породи допълнителна проверка от КЗЛД, за да се установи дали нарушението не е резултат от неспазване на изискванията за сигурност на Регламента. Това може да доведе и до допълнителни административни санкции, за които ще стане дума по-нататък в статията.

Една от препоръките, които може да се направят с цел да се предотвратят тези нарушения, е повишаването на сигурността на информационните системи, които адвокатите ползват, използването само на доставчици на информационни услуги, които спазват Регламента, ограничаването на достъпа до информационните системи на служителите и криптиране на базите данни, служебните пощи и мобилните устройства, на които адвокатите съхраняват лични данни и поверителна информация. Такова криптиране на данните например би направило нечетима информацията за неоторизирания получател, като в този случай, дори да има допуснато нарушение на сигурността, няма да е необходимо уведомяване на КЗЛД и субектите, доколкото няма да съществува риск за правата и свободите на засегнатите клиенти.[48]

---

[46] Член 33, ал. 1 от Регламента.
[47] Член 34 от Регламента.
[48] Член 34, ал. 3, б. „а“ от Регламента.

2.6. Длъжностни лица по защита на данните

Едно от най-съществените и първостепенни нови задължения на администраторите и обработващите данни е да имат длъжностно лице по защита на данните (ДЛЗД) винаги когато основните им дейности се състоят в операции по обработване, които изискват редовно и систематично мащабно наблюдение на субектите на данни, или се състоят в мащабно обработване на „чувствителни данни" и на лични данни, свързани с присъди и нарушения.[49] Докато адвокатите на самостоятелна практика са изрично освободени от задължението да имат ДЛЗД[50], уточнението „мащабно" е много важно в случая, тъй като не е ясно дали малки адвокатски кантори (например от двамачетирима съдружници) също са длъжни да назначат такова длъжностно лице, тъй като липсва установен минимален праг или практика по въпроса. Работна група 29 все пак посочва някои критерии, които да служат за ориентир при преценката дали посочените данни се обработват „мащабно" (например брой физически лица; обем и обхват на личните данни, които се обработват; продължителност на съхранението; географски обхват).[51] Проектозаконът за изменение и допълнение на Закона за защита на личните данни, който беше обявен за обществено обсъждане до 30 май 2018 г.[52], предвижда още една хипотеза на задължително назначаване на ДЛЗД, когато организацията обработва данните на повече от 10 000 субекти. Това ненужно допълнително задължение, което не се налага по силата на Регламента, не само допълнително ще затрудни българския бизнес, но и ще доведе до неясноти, тъй като не всяка организация знае точно броя на лицата, чиито данни обработва.

Режимът за назначаване на длъжностното лице е относително гъвкав – адвокатските кантори могат например да назначат такова длъжностно лице само на тази позиция или да определят работник/служител, който да изпълнява задълженията на ДЛЗД по съвместимост, доколкото няма конфликт на интереси с другите му функции. Във връзка с това е важно да се отбележи, че на тази позиция не може да се назначи друг адвокат, ако той също обработва лични данни, защото в този случай неминуемо би възникнал конфликт на интереси и адвокатът не би могъл ефективно и безпристрастно да упражнява функциите си като ДЛЗД. ДЛЗД може да бъде и външно за кантората лице, което да изпълнява тази функция въз основа на договор за услуги.[53]

Каквато и форма от посочените по-горе да се избере, длъжностното лице трябва да бъде независимо предвид възложените му важни задачи и сериозните правомощия, с които разполага, като участва по подходящ начин и своевременно във всички въпроси, свързани със защитата на личните данни, информира и съветва относно за-

[49] Член 37, ал. 1 от Регламента.
[50] Съображение 91 от Регламента.
[51] Вж. бел. под линия 58.
[52] Достъпен на https://www.cpdp.bg/?p=news_view&aid=1226.
[53] Член 37, ал. 6 от Регламента.

дълженията при обработката на лични данни; контролира спазването на правните задължения и вътрешноорганизационните политики по защита на личните данни; участва в обучения на персонала и одити; действа като точка за контакт с надзорния орган по защита на личните данни и др.).[54] То трябва да докладва на най-високо управленско ниво, а освен това да разполага и с достатъчно време и ресурси, за да изпълнява функциите си.[55] Адвокатските кантори са длъжни да уведомят КЗЛД за назначението и да публикуват данни за ДЛЗД, към което всеки субект на данни трябва да има възможност да се обърне при необходимост.

Накрая е важно да се отбележи и възможността някои адвокати да са приели да упражняват функциите на ДЛЗД по договор за услуги със свои клиенти. В такъв случай Европейският адвокатки съвет изрично препоръчва да не се смесват двете функции на адвокат и ДЛЗД, тъй като вероятността да възникне конфликт на интереси е много голяма, когато адвокатът трябва да действа като лице за контакт с надзорния орган (което може да изисква докладване на надзорния орган, дори това да е против интересите на клиента) и защитник на правата и интересите на клиента като негов адвокат.[56]

2.7. Оценка за въздействието върху защитата на данните

Когато съществува вероятност определен вид обработване (по-специално при използването на нови технологии) да породи *висок риск* за правата и свободите на физическите лица, „администраторите на лични данни“ ще са длъжни да изготвят оценка за въздействието върху защитата на данни (ОВЗД), преди самото обработване да е започнало. В една оценка може да бъде разгледан набор от сходни операции по обработване, които представляват сходни високи рискове.[57]

По-конкретно, за адвокатската професия ОВЗД ще е задължителна винаги когато се обработват мащабно „чувствителни данни“ или лични данни, свързани с присъди и нарушения.[58] Докато адвокатите на самостоятелна практика са изрично освободени от това задължение[59], всяка – дори и малка – адвокатска кантора би могла да попадне в обхвата, доколкото обработва такива данни „мащабно“, като при преценката за това се прилагат същите критерии както при необходимостта от ДЛЗД (вж. т. 2.6

[54] Член 39 от Регламента.

[55] Член 38, ал. 2 и 3 от Регламента.

[56] Вж. бел. под линия 45 по-горе.

[57] Член 35, ал. 1 и 10 и съображения 90 и 93. Когато обработването се осъществява изцяло или отчасти от адвокат като „обработващ данни“, съгласно чл. 28, ал. 3, б. „е“ от Регламента той следва да подпомогне клиента – „администратор на данни“, и да му предостави всякаква необходима информация за изготвянето на оценката.

[58] Член 35, ал. 2, б. „б“ от Регламента.

[59] Съображение 91 от Регламента.

по-горе). Уязвимостта на групата клиенти, които канторите по принцип обслужват, също може да предполага извършването на ОВЗД (например деца, възрастни хора, жертви на престъпления, психично болни, бежанци, кандидати за убежище и др.).[60] Очаква се КЗЛД да внесе повече яснота кога такава оценка се налага, като състави списък на видовете операции по обработване, за които ОВЗД се изисква, като може да състави списък и на операциите, за които не се изисква.[61] За съжаление, такава яснота не е въведена с проекта за изменение и допълнение на Закона за личните данни, за сметка на някои други спорни предложения (вж. т. 2.6 по-горе).

Работна група 29 препоръчва разработването на методологии за ОВЗД, които са специфични за отделните сектори, като се отчитат спецификите на дейността по обработването и вида данни, както и възможният риск за правата и свободите на физическите лица.[62] При липсата на специфична методология за адвокатската професия следва да се спазват общите изисквания на Регламента[63] и Насоките на Работна група 29, като в някои държави надзорните органи вече са разработили специални насоки или софтуери, които да подпомогнат организациите в този процес.[64]

Макар че възлага ново административно задължение, ОВЗД ще има като цяло положителен ефект, тъй като ще спомогне за установяването на рискове, които иначе адвокатските кантори може би не биха отчели, като по този начин избегнат евентуални нарушения на сигурността. Публикуването на ОВЗД не е задължително, но публикуването на част, резюме или заключението от нея е препоръчително, тъй като ще повиши доверието в извършваните от кантората дейности и ще допринесе за повече отчетност и прозрачност спрямо субектите на данни.

2.8. По-силни правомощия на КЗЛД

Накрая следва да се отбележи и една от най-съществените промени спрямо досегашния режим, която цели да гарантира изпълнението на Регламента и значително стимулира организациите да започнат да обръщат сериозно внимание на защитата на личните данни. Това са именно много по-силните правомощия на надзорните органи по защита на личните данни в държавите членки, включително правото им да налагат административни санкции в размер до 20 млн. евро или 4 % от годишния световен оборот на организациите. За да може да установи тези нарушения, КЗЛД ще разпола-

[60] Съображение 75 от Регламента.

[61] Член 35, ал. 4 и 5 от Регламента.

[62] Насоки на Работна група 29 относно оценката за въздействието върху защитата на данни, с. 17, достъпни на http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236.

[63] Член 37, ал. 7 от Регламента.

[64] Например софтуер, разработен от Комисията за защита на личните данни във Франция (CNIL), достъпен на https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment.

га с изключително широки разследващи и разпоредителни правомощия, включително с правото да разпорежда предоставянето на всякаква информация за изпълнение на задачите си; правото да провежда разследвания под формата на одити и да получава достъп до цялата информация и всички лични данни, както и до всички помещения на администратора или обработващия личните данни.[65]

Интересно е да се анализира как тези засилени разследващи и разпоредителни правомощия се съотнасят спрямо адвокатската тайна и неприкосновеността на помещенията, книжата и техниката, с която се ползва адвокатът. Член 90 от Регламента предвижда, че държавите членки могат да приемат специални правила за администратори/обработващи лични данни, обвързани със задължение за опазване на професионална тайна или с други равностойни задължения. За съжаление обаче, такива специални правила не се предвиждат в публикувания за обществено обсъждане Проектозакон за изменение и допълнение на Закона за защита на личните данни[66], мнения по който можеше да се изпращат до 30 май 2018 г. Член 12а от проектозакона единствено гласи, че наличието на търговска, производствена или друга защитена от закона тайна не може да бъде основание за отказ от съдействие от страна на администратора при осъществяване на задачите и правомощията на КЗЛД. *De lege ferenda* се предлага да се въведат по-конкретни правила за неразкриване на професионалната тайна, които да отчитат спецификите на адвокатската професия и необходимостта да се гарантира нейната независимост.

3. Предложение вместо заключение

Едно възможно решение, за да се гарантира спазването на Регламента, докато се отчитат спецификите на адвокатската професия, е да се изготви специален кодекс за поведение, каквато възможност е изрично предвидена в Регламента.[67] Разработването на единни и прозрачни правила под формата на кодекс ще спомогне значително за правилното изпълнение на Регламента от всички адвокати и адвокатски кантори в страната, като съществено ги улесни в този процес. В същото време кодексът ще отчита особеностите и нуждите на адвокатската професия, включително задължението за опазване на адвокатска тайна и неприкосновеността на адвокатската кореспонденция и книжа, като например уточни механизмите за наблюдение от страна на надзорния орган.

Изработването на такъв кодекс може да бъде инициирано например от Висшия адвокатски съвет, като проектът за кодекс следва да се представи за одобрение на КЗЛД. Като част от проекта би могло да се разработи и специална за адвокатската професия методология за оценка на въздействието върху защитата на данните.

---

[65] Член 58, ал. 1, б. „а“, „б“, „д“, „е“ от Регламента.

[66] Достъпен на https://www.cpdp.bg/?p=news_view&aid=1226.

[67] Член 40 от Регламента.