НАЙ-ЧЕСТО ДОПУСКАНИ НАРУШЕНИЯ НА ПРАВИЛАТА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ И СРЕДСТВА ЗА ТЯХНОТО ИЗБЯГВАНЕ

Мартин Захариев
Университет по библиотекознание и информационни технологии, Фондация „Право и Интернет“, Адвокатско дружество „Димитров, Петров и Ко.“

Резюме: Изминаха повече от 3 години, откакто Общият регламент за защита на данните започна да се прилага в ЕС. Регламентът съществено завиши изискванията към организациите, които обработват лични данни – администратори и обработващи, и същевременно въведе високи санкции, чиито максимални размери достигат милиони евро. Независимо от факта, че редица организации инвестираха сериозни ресурси в това да приведат процесите си по обработване на данни в съответствие с новите изисквания, все още се наблюдават множество нарушения на тези правила. Настоящият анализ има за цел да систематизира най-разпространените нарушения на правилата за защита на данните и да предложи средства за тяхното избягване.

Ключови думи: нарушения, лични данни, средства за избягване, Регламент 2016/679 (ОРЗД).

Въведение

Изминаха повече от 3 години, откакто Общият регламент за защита на данните (ОРЗД) започна да се прилага в ЕС[1]. ОРЗД съществено завиши изискванията към администраторите (АЛД) и обработващите лични данни и същевременно въведе високи санкции, чиито максимални размери достигат милиони евро. В допълнение, в края на февруари 2019 г. бяха направени изменения в Закона за защита на личните данни (ЗЗЛД)[2], имащи за цел да хармонизират българското законодателство в сферата на защита на личните данни (ЗЛД) с това на ЕС.

Проблематиката на ЗЛД и начините за постигане на съответствие с нея са добре изследвани в българската научна литература. В теорията са разработени методики за прилагането на ОРЗД, както и методики относно специфични случаи на обработване на лични данни в отделни сектори (в дейността на публичните органи; достъпа до обществена информация; преддоговорните и договорните отношения; хотелиерската дейност и др.) [1]. Някои автори предлагат методики и планове за действие при привеждане в съответствие с изискванията на

ОРЗД, както и систематизират различни добри практики, като контролни методики, решения за длъжностните лица по защита на данните, системи за видеонаблюдение и програми за обучение [2]. Разработени са и образци на ключови документи и процедури, изисквани от ОРЗД в различни ситуации – образци на съгласие, на документи за предоставяне на информация по чл. 13 и чл. 14 от ОРЗД, заявления за упражняване на права от субектите на данни и др. [3].

Горните достижения безспорно са с голямо практическо значение за АЛД. Независимо от това към настоящия момент липсва изследване на това какви нарушения на правилата за ЗЛД най-често се допускат на практика. Именно това е основният стимул за изготвяне на настоящия доклад, който **има за цел** да систематизира най-разпространените нарушения на правилата за ЗЛД и да предложи средства за тяхното избягване.

Актуалността на изследвания проблем се обуславя с постоянно нарастващия брой жалби до Комисията за защита на личните данни (КЗЛД) с твърдени нарушения на правилата на ЗЛД. По данни от годишните отчети за дейността на КЗЛД за 2019 г.[3] и 2020 г.[4], в периода 2017 – 2020 г. е налице относително постоянна възходяща тенденция по общ брой подавани до КЗЛД жалби. През 2017 г. КЗЛД е била сезирана с не повече от 480 жалби, през 2018 г. – със 784 жалби, а през 2019 г. – с над 1600 жалби. Наблюдава се спад през 2020 г. и жалбите са над 680, но последният факт може да се обясни с пандемията от COVID-19 и предприетите мерки за социална дистанция, които блокираха за известен период цели сектори от обществения живот. Независимо от това анализът на наличните данни води до обоснованото предположение, че тенденцията към нарастване на броя жалби ще се запази. Това се обяснява с постепенната адаптация на бизнеса, публичния сектор и отделните индивиди към пандемията и нейните социални измерения и повишената чувствителност на тема ЗЛД в обществото.

Методология на изследването

Резултатите от настоящото изследване бяха получени след прилагане на следните научни методи:

- **Документален метод** – изразява се в анализирането и синтезирането на информация относно различните видове нарушения от документални източници, например от годишните отчети на КЗЛД за 2018 – 2020 г. и от други публично достъпни (включително онлайн) източници, както и в систематизирането и обобщаването на тази информация.

- **Сравнителен анализ** – изразява се в откриване на общото и различното между отделни явления. В настоящия доклад този метод е необходим, за да се направи съпоставка между най-разпространените нарушения на правилата за ЗЛД в България и останалата част на ЕС и да се извлекат изводи относно определени закономерности, като сходство на допусканите нарушения, и респективно да се предложат конкретни способи за тяхното бъдещо избягване.
- **Статистически анализ** – изразява се в извършването на анализ на статистически данни относно относително постоянно нарастващия брой жалби за твърдени нарушения на правилата за ЗЛД, с които годишно се сезира КЗЛД. Изводите, до които се достига чрез този метод, обуславят актуалността и значимостта на изследваната проблематика.
- **Исторически метод** – този метод се използва, за да се проследи динамиката във вида установени от КЗЛД нарушения на правилата за ЗЛД през последните 3 години, откакто се прилага ОРЗД.

Ограничение на изследването

Извън обхвата на настоящото изследване остават нарушенията, констатирани от Инспектората към Висшия съдебен съвет при обработването на лични данни от органите на съдебната власт. Тази проблематика може да бъде предмет на бъдещи изследвания.

Резултати

Анализът на практиката на КЗЛД за 2019 г.[3] и 2020 г.[4] сочи, че може да се очертаят няколко основни групи най-често допускани нарушения на правилата за ЗЛД:

- **Обработване на лични данни без правно основание по чл. 6, пар. 1 от ОРЗД.** Това е сред най-разпространите нарушения и според отчета на КЗЛД за 2018 г.[5], но в контекста на стария режим за ЗЛД – липса на правно основание по чл. 4 от ЗЗЛД (редакция преди 26.02.2019 г). АЛД са длъжни да определят подходящо правно основание за всяка отделна цел на обработването. Нерядко обаче те не се ориентират в приложимата нормативна уредба и не избират правилното основание, на което да базират обработването, например търсят единствено съгласие от субектите на данни, разчитат на легитимен интерес, когато същият няма преимущество над правата, свободите и интересите на субекта на данни, и др. под. Това е в основата на този вид нарушения. **Възможно**

средство за избягване на тези нарушения е доброто познаване на особеностите на всяко правно основание по чл. 6, пар. 1 от ОРЗД. По-долу са коментирани ключови специфики на най-често използваните в практиката основания.

Първо, съгласието не е нито единственото, нито водещото правно основание за обработване на лични данни. В редица случаи, особено когато е налице неравнопоставеност между АЛД и субекта, например в отношенията „публични органи – граждани“ или „работодатели – работници/служители“ (относно основните операции по обработване в контекста на трудовото правоотношение), съгласието не е подходящо основание. Във връзка с това е полезно АЛД да се запознаят с практическите насоки на КЗЛД в кои случаи не е необходимо съгласие[6]. Второ, договорът е годно правно основание за обработването само когато е сключен със субекта на данни, чиито данни се обработват, т.е. субектът трябва да е страна по него. Договори между юридически лица не могат да се ползват като договорно основание за обработването – там следва да се търси друго възможно основание, като легитимния интерес. Трето, когато обработването се базира на легитимния интерес, съществено изискване е дефинирането на съответния интерес и внимателното му балансиране с правата, интересите и свободите на субектите на данните. В теорията и практиката в тази връзка се говори за т.нар. тест за баланс (balancing test) – своеобразна документална оценка на разнопосочните интереси при обработването, обосноваваща преимуществото на съответния легитимен интерес. Така при възражение срещу обработването или жалба АЛД може да докаже, че е оценил всички обстоятелства в съответната ситуация и това обуславя възможността да обработва данните на легитимен интерес. Важно е да се съобрази и забраната на ОРЗД публични органи да използват легитимен интерес за изпълнението на своите задачи. Четвърто, законовото задължение трябва да е установено в правото на ЕС/националното право, приложимо към съответния АЛД. Законодателствата на трети държави (например САЩ), дори да въвеждат задължения към собственика на капитала на съответната организация, не могат да обосноват обработване на основание законово задължение.

- **Обработване на личните данни в нарушение на принципите по чл. 5, пар. 1 от ОРЗД.** Принципите са своеобразните стандарти при обработването на лични данни, основните и най-важни изисквания, на които то трябва да отговаря. Сред най-често нарушаваните принципи по данни

на КЗЛД за 2019 – 2020 г. са „законосъобразност и добросъвестност“, „свеждане на данните до минимум“, „цялостност и поверителност“, „точност“ и „ограничение на целите“ [3, 4]. Както се посочва в теорията, принципите ***„следва да бъдат спазвани през целия „жизнен цикъл“ на данните*** *– от създаването им до тяхното изтриване или унищожаване на техните носители“* [3]. Поради това е трудно да се дефинира общ набор от средства за избягване на нарушаването им. Все пак **може да се очертаят следните най-общи насоки към АЛД**: внимателно да изследват всеки процес по обработване; да формулират ясно какви цели искат да постигнат и какъв набор данни им е нужен за това; да не обработват първоначално събраните данни за други цели, без да са оценили това обработване, да са информирали за това субектите и да са документирали надлежно този процес; да не събират ненужни за съответните цели данни; да поддържат данните точни и защитени с подходящи мерки за сигурност; да не предприемат нечестни, непропорционални и неочаквани за субектите на данни операции по обработване; да спазват приложимата нормативна уредба – обща по ОРЗД и ЗЗЛД и специална в съответния сектор, в който АЛД осъществява дейността си (банки, застрахователи, работодатели, телекоми, публични органи и др.). Независимо че не е споменат от КЗЛД, от съществено значение остава принципът на отчетност – надлежно документиране на всички операции по обработване и осигуряване на документална следа, че изискванията за ЗЛД се спазват в съответната организация (например изготвяне на политики, правила, инструкции и др.).

- **Нарушения, свързани със сигурността на данните и предприетите технически и организационни мерки за защита на данните (ТОМ).** Това са сред най-честите нарушения, констатирани и в отчета на КЗЛД за 2018 г.[5] За съжаление, този тип нарушения често са тежки и засягат голям набор данни относно множество субекти. Резултат са от непредприемане на подходящи ТОМ, небрежност на персонала на АЛД/обработващия и/или злоумишлени действия на трети лица. Най-големите глоби, налагани към момента в България, са именно по повод нарушения на сигурността на данните – глобата на Националната агенция за приходите с 5,1 млн. лева и на една от водещите

български банки с 1 млн. лева[7]. **Като основни средства за избягване на тези нарушения може да се посочат:** осъзнаването, че няма универсален набор от ТОМ за сигурност и че подходящите ТОМ зависят от контекста и естеството на обработването; обучение на персонала на АЛД относно рисковете при обработването на лични данни и заплахите за информационната сигурност; приемането на вътрешни правила, съдържащи конкретни ТОМ – Наредба № 1 от 30.01.2013 г. на КЗЛД[8], макар и отменена, е много добър ориентир за АЛД относно типовете ТОМ, които могат да се прилагат; уговаряне на конкретни ТОМ в отношенията на АЛД с обработващи и др.

- **Непроизнасяне по подадени от субекти на данни заявления за упражняване на права или произнасяне извън нормативно определените срокове.** Нарушения относно правата на субектите са констатирани и в отчета на КЗЛД за 2018 г.[5]. В тази категория може да се обособят два основни вида нарушения – липса на каквото и да е произнасяне по искане за упражняване на права или произнасяне след нормативноустановените за това срокове. Във връзка с това е важно да се знае, че ОРЗД изисква от АЛД да предоставят на субекта на данни информация относно действията, предприети във връзка с исканията за упражняване на права без ненужно забавяне и в срок 1 месец от получаване на искането. С оглед сложността и броя на исканията този срок може да бъде удължен с още 2 месеца. АЛД е длъжен да информира за това удължаване субекта на данните в посочения 1-месечен срок, както и да посочи причините за забавянето. Тези две групи нарушения се обясняват с няколко основни фактора: неглижиране на правилата за ЗЛД и игнориране на получена комуникация от субектите с искане на упражняване на права; непознаване в достатъчна степен на приложимата нормативна уредба; лоша организация в структурата на съответния АЛД при обработването на получените искания, ненавременното им свеждане до знанието на компетентните органи и звена в предприятието, които да се произнесат по тях, и пр. С оглед на тези фактори може да се формулират **следните средства за избягване на посочените нарушения**: обучаване на персонала на АЛД и придобиване на знания относно правилата за ЗЛД и в частност относно правата на субектите

на данни и сроковете за разглеждане и произнасяне по искания за упражняване на права; определяне на отговорен служител/и или звено за разглеждане на такива искания; разработване на вътрешна процедура за разглеждане на искания. Подходяща стъпка за ограничаване на потенциалните жалби е подобряването на комуникацията със субектите на данни при получено искане за упражняване на права, например бързо потвърждаване (включително генериране на автоматичен отговор при искания, отправени с електронни средства), че искането е получено и предстои да се разгледа в нормативноустановения месечен срок; ако ще се стига до отказ или искането е непълно и АЛД се нуждае от допълнителна информация, за да се произнесе по него (например за идентифициране на субекта), това по чисто психологически съображения да се комуникира възможно най-бързо към субекта и препоръчително – много преди изтичане на месечния срок, и др.

Горните изводи и типове най-често допускани нарушения се потвърждават и от сравнителен анализ в другите държави членки от ЕС. По данни от GDPR Enforcement Tracker[7] – онлайн база данни, поддържана от международната кантора CMS, съдържаща информация за налаганите в ЕС глоби за нарушения на ОРЗД, водещите 4 типа нарушения, за които са налагани най-висок брой глоби, са: 1) липса на правно основание за обработването – 278 глоби на обща стойност 176 162 312 евро; 2) неспазване на принципите на обработване на данните – 160 глоби на обща стойност 780 416 864 евро; 3) неприлагане на достатъчни ТОМ за сигурност на данните – 159 глоби на обща стойност 67 434 519 евро; 4) недостатъчно изпълняване на исканията на правата на субектите на данни – 71 глоби на обща стойност 16 166 025 евро (данните са актуални към 23:30 ч. на 13.08.2021 г. – бел. авт.). В този смисъл може да се направи изводът, че очертаните в този доклад основни типове нарушения, допускани в България, са най-разпространените и в целия ЕС. Това в още по-голяма степен подчертава важността на средствата, предложени за тяхното избягване, и тяхното практико-приложно значение не само в национален, а и в международен план.

Изводи/Дискусия

В резултат на направеното изследване може да се направи извод, че независимо от инвестираните през последните 3 години време, средства и усилия от страна на АЛД, все още се наблюдават множество нарушения на правилата за ЗЛД. Това доказва тезата, че

постигането на съответствие с правилата за ЗЛД е сложен и най-вече продължителен процес. Постигането на съответствие не е еднократно усилие по изготвяне на „основен пакет от документи по ОРЗД“. Тъкмо напротив, както воденето на текуща счетоводна отчетност предполага постоянно отчитане според приложимите стандарти на всяка стопанска операция, така и отговарянето на изискванията за защита на личните данни предполага постоянна грижа в организацията и комплекс от действия: сформирането на компетентен екип по ЗЛД; внимателното анализиране на всеки процес по обработване на лични данни през призмата на приложимите правила; надлежното му документиране; предприемането на подходящи ТОМ за защита на данните; осигуряването на адекватна комуникация със субектите на данни по повод искания за упражняване на права и др. под.

Заключение

В заключение може да се открояят няколко основни групи най-често допускани нарушения на правилата за ЗЛД: обработване без правно основание, нарушения на основните принципи на обработването, необезпечаване на сигурността на данните и на подходящи ТОМ, непроизнасяне или ненавременно произнасяне по искания на субекти за упражняване на техни права. Настоящият доклад предлага различни способи за тяхното избягване в зависимост от спецификите на съответното нарушение. Изследваните проблеми е добре да се наблюдават в динамика, а тяхното развитие да се проследи във времето, включително в рамките на бъдещи научни изследвания и разработки. По този начин може да се проследи колко адекватно и законосъобразно се прилагат правилата за ЗЛД и как може да се ограничат най-често допусканите нарушения в тази област.

Представеният анализ няма характера на правен съвет или консултация и не следва да бъде възприеман като достатъчен за разрешаването на конкретни правни проблеми, казуси и др. Мненията, изразени тук, са единствено на автора и не отразяват непременно тези на УниБИТ, Фондация „Право и Интернет“, Адвокатско дружество „Димитров, Петров и Ко.“, техните филиали или служители. Материалът е съобразен с действащото българско законодателство и законодателство на ЕС към 13.08.2021 г.

Бележки

[1] **Reglament** (ES) 2016/679 na Evropeyskiya parlament i na Saveta ot 27 april 2016 godina otnosno zashtitata na fizicheskite litsa vav vrazka s obrabotvaneto na lichni danni i otnosno

svobodnoto dvizhenie na takiva danni i za otmyana na Direktiva 95/46/EO (Obsht reglament otnosno zashtitata na dannite) (Tekst ot znachenie za EIP), Obn. OJ L 119, 4.05.2016, s. 1 – 88.

[**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) (Текст от значение за ЕИП), Обн. OJ L 119, 4.05.2016, с. 1 – 88.]

[2] **Zakon** za zashtita na lichnite danni. Obn. DV, br. 1 ot 4 yanuari 2002 g., posl. izm. DV, br. 93 ot 26.11.2019 g. s Reshenie № 8 ot 15.11.2019 g. na KS na RB po k.d. № 4/2019 g.

[**Закон** за защита на личните данни. Обн. ДВ, бр. 1 от 4 януари 2002 г., посл. изм. ДВ. бр. 93 от 26.11.2019 г. с Решение № 8 от 15.11.2019 г. на КС на РБ по к. д. № 4/2019 г.]

[3] **Godishen** otchet na Komisiyata za zashtita na lichnite danni za deynostta y prez 2019 g., s. 15, 17. <https://www.cpdp.bg/?p=element&aid=1236> (13 avg. 2021).

[**Годишен** отчет на Комисията за защита на личните данни за дейността ѝ през 2019 г., с. 15, 17. <https://www.cpdp.bg/?p=element&aid=1236> (13 авг. 2021).]

[4] **Godishen** otchet na Komisiyata za zashtita na lichnite danni za deynostta y prez 2020 g., s. 13, 16. <https://www.cpdp.bg/?p=element&aid=1281> (13 avg. 2021).

[**Годишен** отчет на Комисията за защита на личните данни за дейността ѝ през 2020 г., с. 13, 16. <https://www.cpdp.bg/?p=element&aid=1281> (13 авг. 2021).]

[5] **Godishen** otchet na Komisiyata za zashtita na lichnite danni za deynostta y prez 2018 g., s. 19 – 20. <https://www.cpdp.bg/?p=element&aid=1181> (13 avg. 2021).

[**Годишен** отчет на Комисията за защита на личните данни за дейността ѝ през 2018 г., с. 19 – 20. <https://www.cpdp.bg/?p=element&aid=1181> (13 авг. 2021).]

[6] **Prakticheski** nasoki na KZLD v koi sluchai ne e neobhodimo saglasie za obrabotvane na lichni danni. <https://www.cpdp.bg/index.php?p=element&aid=1163> (13 avg. 2021).

[**Практически** насоки на КЗЛД в кои случаи не е необходимо съгласие за обработване на лични данни. <https://www.cpdp.bg/index.php?p=element&aid=1163> (13 авг. 2021).]

[7] **GDPR Enforcement Tracker.** <https://www.enforcementtracker.com/?insights> (13 Aug. 2021).

[8] **Naredba № 1** ot 30.01.2013 g. za minimalnoto nivo na tehnicheski i organizatsionni merki i dopustimiya vid zashtita na lichnite danni. Obn. DV, br. 14 ot 12.02.2013 g.; otm. br. 43 ot 25.05.2018 g., v sila ot 25.05.2018 g.

[**Наредба № 1** от 30.01.2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни. Обн. ДВ бр. 14 от 12.02.2013 г.; отм. бр. 43 от 25.05.2018 г., в сила от 25.05.2018 г.]

References/Литература

1. **Feti**, N., D. **Toshkova-Nikolova**. Prilagane na zashtitata na lichnite danni. Sofiya: Trud i pravo, 2020.

[**Фети**, Н., Д. **Тошкова-Николова**. Прилагане на защитата на личните данни. София: Труд и право, 2020.]

2. **Tselkov**, V., D. **Petkov**, G. **Sredkov**, P. **Georgiev**. Zashtita na dannite. Printsipi i praktiki. Sofiya: Za bukvite – P pismeneh, 2019.

[**Целков**, В., Д. **Петков**, Г. **Средков**, П. **Георгиев**. Защита на данните. Принципи и практики. София: За буквите – О писменехь, 2019.]

3. **Toshkova-Nikolova**, D., N. **Feti**. Zashtita na lichnite danni. Sofiya: Trud i pravo, 2019.

[**Тошкова-Николова**, Д., Н. **Фети**. Защита на личните данни, София: Труд и право, 2019.]

За автора

Мартин Захариев завършва специалност „Право“ с отличие, като се дипломира в Юридическия факултет на Софийския университет „Св. Климент Охридски“ през 2014 г. Притежава образователната и научна степен „доктор“ от Университета по библиотекознание и информационни технологии (УниБИТ), а от 2021 г. е доцент към катедра „Национална сигурност“, Факултет „Информационни науки“ на УниБИТ. Работи като старши адвокат в една от водещите български кантори – Адвокатско дружество „Димитров, Петров и Ко.“, като старши правен експерт във фондация „Право и Интернет“, а също така е член на Софийската адвокатска колегия и Сдружението за международни състезания по право. Автор е на две монографии в областта на защитата на личните данни – „Автоматизираното профилиране и защитата на личните данни. Анализ на GDPR“ (2018) и “Data Protection in Commercial Arbitration: In the Light of GDPR” (2019), на учебник „Режим на информацията: Същност и значение на информацията. Защита на личните данни. Примерни тестове“ (2020), както и на множество статии и анализи в областта на защитата на личните данни, търговския арбитраж, трудовото и търговското право. Преподавател е по различни дисциплини в областта на правото и информационните технологии.

За контакт с автора: m.zahariev@unibit.bg

THE MOST COMMON VIOLATIONS OF THE RULES FOR THE PROTECTION OF PERSONAL DATA AND MEANS OF AVOIDING THEM

Martin Zahariev
University of Library Studies and Information Technologies, Law and Internet Foundation, Dimitrov, Petrov & Co. Law Firm

Abstract: It has been more than 3 years since the General Data Protection Regulation (GDPR) became applicable in the European Union. The Regulation has significantly increased the requirements for organizations processing personal data – controllers and processors, while also introducing high sanctions, with maximum amounts reaching millions of euros. Although a number of organizations have invested significant resources in bringing their data processing processes in line with the new requirements, there are still many violations of these rules. This analysis aims to systematize the most common violations of the data protection rules and to propose means of avoiding them.

Keywords: violations, personal data, means of avoidance, Regulation 2016/679 (GDPR).

About the author

Martin Zahariev, Assoc. Prof. PhD, graduated with honors from Sofia University "St. Kliment Ohridski", Faculty of Law (LL.M.) in 2014. He has an educational and scientific degree "doctor" at the University of Library Studies and Information Technologies (ULSIT) and since 2021 has been appointed as "Associate Professor" with the Department National Security, Faculty Information Sciences at ULSIT. He is a senior associate in one of the leading Bulgarian law firms – "Dimitrov, Petrov and Co." He is a senior legal expert in the "Law and Internet" Foundation, and is also a member of the Sofia Bar Association and the International Moot Court Competitions Association. Assoc. Prof. Zahariev is the author of two monographs in the field of personal data protection – "AUTOMATED PROFILING AND THE PERSONAL DATA PROTECTION. Analysis of GDPR" (2018) and "Data Protection in Commercial Arbitration: In the Light of GDPR" (2019), of the textbook "REGIME OF INFORMATION: Nature and significance of information. Personal data protection. Sample tests" (2020). He has written numerous articles and analyses in the field of personal data protection, commercial arbitration, labor and commercial law. He is a lecturer in various courses in the field of law and information technologies.

To contact the author: m.zahariev@unibit.bg