Deloitte. Legal

Let's Talk Law

Правни акценти

25 Май 2023 г.

Пет години GDPR

Навършват се пет години от датата, на която Общият регламент относно защитата на данните (GDPR) започна да се прилага - 25 май 2018 г. За този период GDPR постави множество изисквания и предизвикателства пред всички организации, обработващи лични данни в публичния и частния сектор, включително и извън границите на Европейския съюз.

В настоящото издание поставяме акцент върху интересни теми, свързани с прилагането на GDPR, а именно:

- *GDPR в цифри*
- *Статистика за България*
- *Наложени санкции в България и Европа*
- *Практика на Съда на Европейския съюз*

GDPR в цифри

През петте години на своето прилагане, GDPR издигна защитата на личните данни до високо ниво и намери отражение, както върху законодателните процеси, дейността на компаниите и обществеността в Европа, така и извън нейните граници.

Според статистиката, представена от Международната асоциация на професионалистите в областта на поверителността на данните (IAPP)[1], за тези пет години от прилагането на GDPR:

- Общият размер на наложените глоби възлиза на над 4 млрд. евро;
- Предприетите действия по прилагане на GDPR от надзорните органи са над 1700;
- Съда на Европейския съюз е постановил 32 решения във връзка с GDPR;
- Назначените длъжностни лица по защита на данните в Европа са над 700,000.

Важен аспект по отношение на прилагането на законодателството за защита на личните данни е и осведомеността на физическите лица – субекти на данни, респективно тяхната бдителност по отношение на обработването на личните им данни. В последните години се наблюдава все по-голяма активност на субектите при упражняване на техните права, което свидетелства и за повишената им информираност. Според статистиката на IAPP, 62% от европейските потребители се безпокоят за поверителността на своите лични данни в онлайн среда, а 52% считат, че изкуственият интелект е значителна заплаха за поверителността.

Статистика за България

Жалби до КЗЛД

През последната година от приложението на GDPR в България се забелязва значителна активност при подаване на сигнали и искания за упражняване на надзорни правомощия до българския надзорен орган - Комисията за защита на личните данни („КЗЛД“). За 2022 г. те са 394, а за сравнение през 2018 г., първата от прилагането на GDPR, са постъпили 290 сигнали и запитвания.

Най-голям брой запитвания и сигнали са получени срещу администратори на лични данни, предоставящи интернет услуги и on-line търговия – 75 бр., както и тези в сектор банково дело и кредитна дейност – 36 бр. Следват ги сигналите за незаконосъобразно обработване на лични данни от органи на държавната администрация – 29 бр., а във връзка с директен маркетинг - 26 бр.

Значителен е броят на постъпилите сигнали, касаещи обработване на лични данни на физически лица от различни интернет сайтове и платформи по отношение неспазване на изискванията на GDPR и Закона за защита на личните данни („ЗЗЛД“), и по-точно на задълженията да се публикуват правилата или политиките за обработване на личните данни на потребителите и политиките за поверителност при използването на т.нар. „бисквитки“ (“cookies”).

През 2022 г. жалбите, подадени до КЗЛД от физически лица с твърдения за нарушения при обработване на лични данни и упражняване на права, продължават да бъдат голям брой - над 770.

[1] IAPP, GDPR at Five, Joe Jones, May 2023 - https://iapp.org/resources/article/gdpr-anniversary/

Сектори на дейност	Брой постъпили жалби през 2022 г.
Видеонаблюдение	178
Банки и кредитни институции	89
Политически субекти	68
Физически лица	66
Телекомуникации	49
Държавни органи	33
Трудови и осигурителни услуги	19
Здравеопазване	18
Медии	17
Застраховане	9
Образование	4

Източник: Годишен отчет на КЗЛД за 2022 г., публикуван на интернет страницата на КЗЛД https://www.cpdp.bg/index.php?p=sub_rubric&aid=279

Контролна дейност на КЗЛД

От 25 май 2018 г. насам КЗЛД провежда разследвания под формата на проверки след постъпил сигнал за нарушения на разпоредбите на GDPR или след решение на КЗЛД по повод разглеждане на жалба или самосезиране.

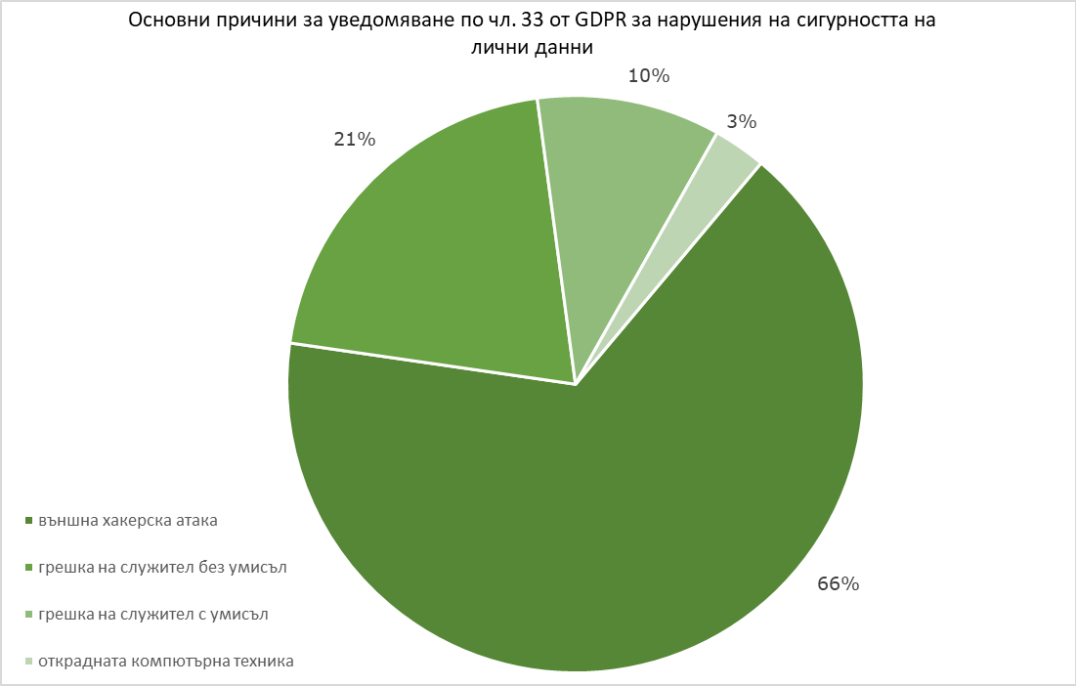
През 2022 г. се наблюдава увеличение на броя на разследванията на КЗЛД във връзка със спазване правилата на GDPR. Най-голям е броят на извършените от КЗЛД проверки във връзка с осъществяване на видеонаблюдение и инсталиране на системи за видеонаблюдение в сгради в режим на етажна собственост и в съседни имоти. Във връзка с политическата обстановка и множество изборни процеси и подписки за референдуми – местни и национални, през отчетния период в сектор политика са извършени 46 проверки.

Източник: Годишен отчет на КЗЛД за 2022 г., публикуван на интернет страницата на КЗЛД – https://www.cpdp.bg/index.php?p=sub_rubric&aid=279

Уведомления за нарушения на сигурността на личните данни

През 2022 г. в КЗЛД са постъпили общо 80 уведомления за нарушения на сигурността на данните, като с високо ниво на риск са оценени 8 уведомления. При 15 от случаите има трансгранично обработване.

Запазва се тенденцията, според която характерът на нарушенията показва, че дигиталните пробиви в сигурността на данните са по-голям брой (45 бр.) от физическите пробиви (24 бр.). В голяма част от случаите се касае за външни злонамерени атаки към системите на организациите.



Източник: Годишен отчет на КЗЛД за 2022 г., публикуван на интернет страницата на КЗЛД - https://www.cpdp.bg/index.php?p=sub_rubric&aid=279

Наложени санкции в България и Европа

През изминалите пет години надзорните органи в държавите членки проявиха голяма активност не само по отношение на даването на насоки и становища, но също така и при реализиране на контролните и санкционните си правомощия. В България и в останалите страни бяха наложени глоби на множество организации, както в частния, така и в публичния сектор за различни по вид нарушения, а някои от санкциите достигнаха многомилионен размер. Част от глобите, наложени през последната година, сме разгледали в изложението по-долу.

Решения на надзорните органи в България

- Български пощи ЕАД е глобена (**500 000 лева**) след хакерска атака. По време на своето разследване КЗЛД установява, че администраторът не е приложил адекватни технически и организационни мерки за защита на личните данни, за да избегне нарушение на данните.
- Политическа партия е глобена (**12 800 лева**), след като няколко лица подават жалба до КЗЛД, защото личните им данни са били добавени в избирателните списъци без тяхното съгласие.
- Транспортна фирма е глобена (**5 000 лева**), защото администраторът е разкрил лични данни на бивш служител на трети лица без валидно правно основание.

Решения на надзорните органи в Европейския съюз

- Три санкции на Meta Platforms Ireland Limited (общо **627 млн. евро**) заради нарушение на задълженията за прозрачност и информиране и липса на валидно съгласие.

- Clearview AI – компания, предлагаща софтуер за разпознаване на лица, е санкционирана в няколко държави членки, след като става ясно, че е прилагала биометрични техники за наблюдение на територията на страните. Компанията притежава база данни с над 10 милиарда изображения на лица от цял свят.

  Глобите са наложени в Италия (**20 млн. евро**), Гърция (**20 млн. евро**), Великобритания (**9 млн. евро**) и Франция (първа глоба от **20 млн. евро** и повторна глоба от **5,2 млн. евро** през 2023 г. поради неизпълнение на насоките на френския надзорния орган).

- Нидерландската данъчна и митническа администрация беше глобена (**3,7 млн. евро**) след като надзорният орган е открил, че администрацията е водила списък в продължение на няколко години, в който е запазвала индикации за измама. Списъкът съдържал информация за над 270 000 лица, включително информацията на непълнолетни.

- В Испания Google LLC е глобена (**10 млн. евро**) след като двама субекти на данни са подали оплакване до надзорния орган, че Google са разкрили техните лични данни на трети страни без разрешение.

- Гръцки телеком е глобен (**6 млн. евро**) за нарушения на принципите на GDPR, след хакерска атака, поради недостатъчни технически и организационни мерки за осигуряване на информационна сигурност.

- Националният статистически институт на Португалия е глобен (**4,3 млн. евро**), след като надзорният орган е установил множество нарушения на GPDR във връзка с преброяването в Португалия през 2021г. Установено е, че администраторът не е информирал субектите на данни, че предоставянето на религиозни и здравни данни е чисто доброволно.

- Рекордна санкция е наложена на Meta (**1,2 млрд. евро**) от Ирландския надзорен орган, поради обработване и съхранение на лични данни в Съединените щати в противоречие с GDPR. Глобата е най-голямата, налагана някога, съгласно GDPR. Предишният рекорд от 746 милиона евро беше наложен на Amazon през 2021 г.

Практика на Съда на Европейския съюз

CEC постанови решение относно понятието „копие" от личните данни по смисъла на GDPR

Съдът на Европейския съюз („CEC") се произнесе с решение по дело C-487/21, постановено по преюдициално запитване, че правото да се получи „копие" от личните данни, закрепено в GDPR, изисква на субекта на данните да се предостави точно и разбираемо копие на всички тези данни. Преюдициалното запитване се отнася до тълкуването на член 15 от GDPR. Запитването е отправено във връзка с отказа на австрийски орган за защита на данните да задължи агенция за търговски консултантски услуги, която предоставя информация за кредитоспособността на трети лица, да изпрати на неин клиент копие от документите и извлеченията от бази данни, съдържащи в частност личните му данни, които са в процес на обработване.

Австрийският съд формулира преюдициалния въпрос до CEC относно тълкуване на понятието „копие", както и дали задължението, предвидено в член 15, параграф 3, от GDPR, че на субекта на данните трябва да се предостави „копие" от личните му данни, които са в процес на обработване, трябва да се тълкува в смисъл, че в него е установено общо право на субекта на данните да му бъде предоставено копие също и на цели документи, в които се обработват лични данни, съответно да му бъде предоставено копие от извлечение от база данни, в случай на обработване на лични данни в такава база данни, или в смисъл, че за субекта на данните е налице само законово право на точно възпроизвеждане на личните данни, до които се иска достъп.

В решението си CEC разяснява, че терминът „копие" се отнася не до документа като такъв, а до личните данни, които той съдържа и които трябва да са пълни и в копието трябва да се съдържат всички лични данни, които са в процес на обработване. Също така се разяснява, че администраторът е длъжен да осигури подходящи мерки, за да предостави на субекта на данните цялата посочена информация в леснодостъпна и разбираема форма. По така поставените преюдициални въпроси, според CEC отговаря, че член 15, параграф 3, от GDPR

трябва да се тълкува в смисъл, че: правото да се получи от администратора копие от личните данни, които са в процес на обработване, изисква на субекта на данните да се предостави точно и разбираемо копие на всички тези данни. Това право предполага правото на получаване на копие от извлечения от документи и дори от цели документи или от извлечения от бази данни, които в частност съдържат посочените данни, ако предоставянето на такова копие е задължително, за да може субектът на данните ефективно да упражни предоставените му с GDPR права, като се подчертава, че в това отношение трябва да се вземат предвид правата и свободите на други лица.

СЕС постанови решение относно обезщетенията за неимуществени вреди, поради нарушение на GDPR

Съдът на Европейския съюз постанови решение (C-300/21) относно обезщетения, произтичащи от нарушения на защитата на личните данните. Според член 82 пар. 1 от GDPR, всяко лице, което е претърпяло материални или нематериални вреди в резултат на нарушение на регламента, има право да получи обезщетение от администратора или обработващия лични данни за нанесените вреди.

Пред СЕС са формулирани следните преюдициални въпроси: дали дадено лице има право да получи обезщетение съгласно член 82 от GDPR само от нарушение на GDPR или дали такъв иск изисква лицето да е претърпяло вреда от това нарушение, както и дали претърпяната вреда трябва да надвишава определена степен на опасност и методите за оценка на размера на щетите. Според СЕС фактът, че са нарушени разпоредбите на GDPR, е недостатъчен, за да се предяви иск за обезщетение, а за да възникне отговорността по член 82 от GDPR се изисква наличието на три условия: (i) нарушение на GDPR, (ii) вреда, претърпяна от субекта на данните и (iii) причинно-следствена връзка между незаконното обработване и вредата. В практиката широко разпространено е възприятието, че член 82, пар. 3 от GDPR освобождава администратора или обработващия лични данни от отговорност, ако се докаже, че не са отговорни за събитието, причинило вредата. Това означава, че администраторът или обработващият лични данни трябва да докажат, че не са действали виновно. СЕС посочва, че вредите, причинно-следствената връзка и нарушението са необходими, за да се установи право на обезщетение. Във връзка с определянето на размера за обезщетение за вреди, СЕС приема, че националните съдилища следва да прилагат националното право за оценка на вредите, като спазват принципите на ЕС за равностойност и ефективност. По отношение на прага за неимуществени вреди, СЕС приема, че той може да варира в различните държави членки. Следователно, дори „емоционални" оплаквания след нарушение на GDPR биха могли да доведат до присъждане на обезщетение за неимуществени вреди. СЕС посочва, че субектът на данни, който претендира обезщетение за неимуществени вреди, все пак ще трябва да докаже, че негативните последици след нарушение на GDPR са довели до неимуществена вреда.

Съдът на Европейския съюз публикува Заключение на генералния адвокат по дело C-340/21 (В.Б. срещу Национална агенция за приходите)

На 15 юли 2019 г., след неоторизиран достъп до информационната система на Националната агенция за приходите (НАП), различна данъчна и осигурителна информация на милиони хора, както български граждани, така и чужденци, е публикувана в интернет. Много лица, включително В.Б., завеждат дела срещу НАП, за да получат обезщетение за неимуществени вреди, които се изразяват в притеснения и опасения, че с личните данни може да бъде злоупотребено в бъдеще.

Според В.Б., НАП е нарушила националното право, както и задължението да приеме подходящи мерки, за да гарантира подходящо ниво на сигурност при обработката на личните данни в качеството си на администратор. Първоинстанционният съд - Административен съд София-град (АССГ) отхвърля иска, като приема, че НАП не е отговорна за разкриването на данните, че доказателствената тежест на подходящия характер на мерките е на В.Б. и че няма неимуществени вреди, които да подлежат на обезщетяване.

Сезиран с жалба, Върховният административен съд (ВАС) отправя няколко преюдициални въпроса до СЕС за тълкуване на GDPR, за да определи условията за обезщетение за неимуществени вреди на лице, чиито лични данни, съхранявани от публична агенция, са били публикувани в интернет вследствие на хакерска атака.

В заключението си генерален адвокат Giovanni Pitruzzella прави уточнението, че администраторът има задължението да прилага подходящи технически и организационни мерки, за да гарантира, че обработването на лични данни е в съответствие с GDPR. Подходящият характер на тези мерки се определя с оглед на естеството, обхвата, контекста и целите на обработването, както и вероятността и тежестта на рисковете за правата и свободите на физическите лица, въз основа на оценка за всеки отделен случай.

На първо място, генералният адвокат приема, че настъпването на „нарушение на сигурността на личните данни" само по себе си е достатъчно, за да се заключи, че прилаганите от администратора техническите и организационни мерки не са „подходящи" за осигуряване на защитата на данните. Когато избира мерките, администраторът трябва да вземе предвид редица фактори, сред които „достиженията на техническия прогрес", което позволява ограничаване на технологичното ниво на мерките до разумно възможното в момента на приемането им, включително с оглед на разходите за прилагане.

На второ място, когато проверява подходящия характер на мерките, националният съд трябва да извърши проверка, която обхваща конкретен анализ, както на съдържанието на тези мерки, така и на начина, по който са били приложени и на техните практически ефекти. Съдебният контрол следователно ще трябва да вземе предвид всички фактори, съдържащи се в GDPR.

На трето място, доказателствената тежест относно подходящия характер на мерките е на администратора. В съответствие с принципа на процесуална автономия, вътрешният правен ред на всяка държава членка определя допустимите методи за доказване и тяхната доказателствена стойност, включително следствените действия.

На четвърто място, фактът, че нарушението на GDPR е извършено от трето лице, сам по себе си не представлява причина за освобождаване на администратора от отговорност. За да бъде освободен от отговорност, администраторът трябва да докаже с „висок стандарт на доказване", че по никакъв начин не е отговорен за събитието, причинило вредата.

На последно място, вредата, състояща се в страх от потенциална бъдеща злоупотреба с личните данни, чието съществуване заинтересованата страна е доказала, може да представлява неимуществена вреда, която дава право на обезщетение. Това при условие, че става въпрос за реална и сигурна емоционална вреда, а не просто за безпокойство или неудобство.

Заключение

Практиката по прилагане на GDPR през изминалите пет години сочи, че основно предизвикателство пред организациите е да поддържат изградените си системи за управление и защита на личните данни в съответствие с нормативните изисквания, предвид динамиката около тях – законодателни промени, становища и насоки на компетентните органи, практика по прилагане. Тази задача става още по-сложна на фона на навлизащите нови технологии, като например изкуствен интелект.

В заключение, осигуряването на съответствието с GDPR е жив процес, който изисква непрекъснат мониторинг и актуализация. Служителите и експертите във всяка организация, ангажирани със защитата на личните данни, е необходимо на регулярна база да се запознават с новостите в областта и да подлагат на анализ дейностите в организацията.

Делойт Лигъл ще продължи да следи за вас промените в сферата на защитата на личните данни и да ви информира периодично.

За Делойт Лигъл

Адвокатско дружество „Делойт Лигъл" има богат опит при консултирането на местни и международни клиенти в областта на защитата на личните данни, включително във връзка с Общия регламент относно защитата на данните (GDPR).

Тясното сътрудничество на Делойт Лигъл със специалисти в мрежата на Делойт, притежаващи опит в управление на риска и информационна сигурност, осигурява мултидисциплинарен подход и комплексна експертиза при предоставяне на нашите услуги, включително:

- Анализ и оценка на съответствието
- Изготвяне на рамка за съответствие (вкл. политики, оценка на въздействието и др.)
- Договори с обработващи и съвместни администратори
- Съдействие при трансграничен трансфер на данни
- Изпълняване функцията на длъжностно лице по защита на данните
- Уебинари и обучения на персонала
- Сертификационни курсове по програмите на IAPP (CIPP/E, CIPM)
- Съдействие при проверки и др.

Нашият екип по защита на личните данни:

адв. Миглена Мичева
Мениджър
mmicheva@deloittece.com

Миглена има магистърска степен по Право от Софийския университет „Св. Климент Охридски" и е член на Софийската адвокатска колегия. Специализациите й включват диплома по правна практика от College of Law (Международни съвместни предприятия, Международно търговско право и т.н.). Тя е признат специалист по законодателството за защита на личните данни (CIPP/E, CIPM, FIP).

Ирена Колева
Старши адвокат
ikoleva@deloittece.com

Ирена е завършила Юридическия факултет на Софийския университет „Св. Климент Охридски" с магистърска степен по Право и е член на Софийската адвокатска колегия от 2017 г. Тя също така е член на Международната асоциация на професионалистите в областта на поверителността на данните (IAPP), притежава сертификат CIPP/E и е в ръководния състав на IAPP KnowledgeNet Chapter за България.

Кристиан Немцов
Адвокат
knemtsov@deloittece.com

Кристиан има магистърска степен по „Право" (2017 г.) и бакалавърска степен по „Международните отношения" от Софийския университет „Св. Климент Охридски" (2013 г.), вписан в Софийска адвокатска колегия през 2019 г. Той е специализирал в рамките на програмата „Еразъм" в Юридическия факултет на Автономния университет в Мадрид, Испания (2014 г.).