КОМИСИЯ ЗА ЗАЩИТА
НА ЛИЧНИТЕ ДАННИ

ПРАКТИЧЕСКИ ВЪПРОСИ НА ЗАЩИТАТА НА ЛИЧНИТЕ ДАННИ СЛЕД 25 МАЙ 2018 Г.

От 25 май 2018 г. във всички държави-членки на Европейския съюз ще се прилагат нови правила за защита на личните данни. Те са уредени в т.нар. Общ регламент за защита на личните данни (GDPR). Новата правна рамка запазва редица основополагащи принципи и понятия от съществуващата към момента нормативна уредба, но в същото време въвежда по-високи стандарти за защита на данните, разширени права на физическите лица и нови задължения на администраторите на лични данни.

Целта на настоящата брошура е да даде разяснения на някои ключови въпроси, които да подпомогнат практическото прилагане на Общия регламент. Тя е чисто информационен документ и не претендира за изчерпателност.

Комисията за защита на личните данни периодично ще актуализира тази информация и ще включва и допълнителни разяснения по други важни въпроси с практическа насоченост. Най-актуална информация може да бъде намерена на интернет страницата на Комисията www.cpdp.bg

СЪДЪРЖАНИЕ:

Съгласие за обработване на лични данни

Съгласието е едно от алтернативните основания за законосъобразно обработване на лични данни. В случай че администраторът реши да обработва данните на това основание, той следва да е в състояние да докаже, че съгласието е:

- свободно изразено – не е дадено под натиск или заплаха от неблагоприятни последици (напр. по-висока цена на услуга);
- конкретно – отделно съгласие за всяка конкретно определена цел, а когато е относимо - и за конкретна категория лични данни;
- информирано – дадено на основата на пълна, точна и лесно разбираема информация;
- недвусмислено – не се извлича или предполага въз основа на други изявления или действия на лицето;
- дадено с активно действие: чрез изрично изявление или ясно потвърждаващо действие, вкл. онлайн. Мълчанието на лицето или предварително отметнати квадратчета за съгласие не могат да се приемат за валидно съгласие.

Недопустимо е съгласието да бъде обвързано с предварителни условия от страна на администратора или да води до неблагоприятни последици за лицето при отказ да го предостави или ако впоследствие го оттегли.

Съгласието може да не бъде счетено за валидно, ако съществува зависимост или неравнопоставеност между субекта на данни и администратора, напр. в отношенията между гражданин и публичен орган или между работник и работодател.

В съответствие с принципа за отчетност на администраторите на лични данни, съгласието следва да бъде документирано с цел доказване на неговото наличие.

Лицето има право да оттегли своето съгласие по всяко време, като начинът за това следва да бъде толкова лесен и достъпен, колкото начинът, по който съгласието е било дадено.

В случай на пряко предлагане на услуги на информационното общество на дете под 14 години (напр. регистрация в социална мрежа или откриване на електронна поща) администраторът следва да изисква съгласие, респ. потвърждение от носещия родителска отговорност за детето.

Правото да бъдеш забравен

Правото на изтриване (или "правото да бъдеш забравен") дава възможност, когато субектът на данни не желае данните му да бъдат обработвани и не съществуват законни основания за тяхното съхранение, да поиска те да бъдат заличени при едно от следните основания:

- личните данни повече не са необходими за целите, за които са били събрани или обработвани по друг начин;
- субектът на данните оттегля своето съгласие, върху което се основава обработването на данните;
- субектът на данни възразява срещу обработването и няма преимуществено законово основание за продължаване на обработването;
- личните данни са били обработвани незаконосъобразно;
- личните данни трябва да бъдат изтрити с цел спазването на правно задължение;
- личните данни са били събрани във връзка с предлагането на услуги на информационното общество на дете.

„Правото да бъдеш забравен" не е абсолютно право. Съществуват ситуации, в които администраторът има възможност да откаже да изтрие данните, а

именно когато обработването на конкретните данни е необходимо за някоя от следните цели:

- за упражняване правото на свобода на изразяване и информация;
- за изпълнение на правно задължение или на задача от обществен интерес или упражняване на публична власт;
- за целите на общественото здраве;
- архивиране за цели в обществен интерес, научноизследователски исторически изследвания или статистически цели;
- за установяване, упражняване или защитата на правни претенции.

„Правото да бъдеш забравен" в онлайн средата, изисква от администратора, който е направил личните данни обществено достъпни (напр. чрез публикуване в интернет) да уведоми другите администратори, които обработват тези лични данни, да изтрият всякакви връзки към тях или техните копия или реплики. Това се отнася преди всичко за интернет търсачките.

Профилиране

Профилиране е автоматизирано обработване на лични данни, с цел оценяване на определени лични аспекти, свързани с дадено лице, вкл. за анализиране или прогнозиране на поведението му, изпълнението на професионалните му задължения, икономическото му състояние, здраве, лични предпочитания, интереси, надеждност, поведение, местоположение или движение.

В голямата си част профилирането се извършва в онлайн среда. То се използва най-често за целите на директния маркетинг, оценка на кредитоспособността, набиране на персонал и др.

Физическото лице – обект на профилиране, следва да бъде информирано за извършването му и за последствията от него. Тази информация може да бъде

предоставена графично, напр. чрез стандартизирани икони, така че по лесно видим, разбираем и ясно четим начин лицето да се запознае с планираното профилиране. То има право да възрази срещу профилирането по всяко време.

Профилирането не следва да води до дискриминация на лицата въз основа на тяхната раса или етнически произход, политически възгледи, вероизповедание или убеждение, членство в синдикални организации, генетичен или здравен статус или сексуална ориентация. Профилирането не може да се прилага спрямо дете.

Профилирането по правило поражда висок риск за правата и свободите на физическите лица. За тази цел, администраторът следва да извърши оценка на въздействието върху защитата на данните, когато те се обработват с цел профилиране.

Длъжностно лице по защита на данните

Длъжностното лице по защита на данните играе ключова роля за осигуряване на законосъобразното обработване на лични данни в структурата на администратора. То трябва да разполага с професионални качества и експертни познания в областта на защитата на личните данни (законодателство и практика).

Основната задача на длъжностното лице е да информира и съветва администратора и неговите служители по всички въпроси, свързани с обработването и защитата на личните данни. Важно е да се знае, че то не определя целите и средствата за обработване на данни и съответно администраторът не може да прехвърли своята отговорност за неспазване на изискванията на Общия регламент върху него. Поради този причина длъжностното лице по правило не може да заема ръководни позиции, пряко свързани с обработването на лични данни в организацията на администратора, за да се избегне конфликт на интереси. В същото време длъжностното лице следва да разполага с висока степен на независимост, за да изпълнява ефективно своите консултативно-превантив-

ни функции. Администраторът няма право да дава указания или нареждания във връзка с изпълнението на задачите на длъжностното лице по защита на данните, което следва да се отчита директно на висшия мениджмънт в организацията на администратора.

Задължение да определят Длъжностно лице по защита на данните имат следните администратори на лични данни (физически и юридически лица):

- публичен орган или орган на местно самоуправление;
- администратори, които извършват системно и мащабно наблюдение на субектите на данните;
- администратори, които извършват мащабно обработване на специални (чувствителни) лични данни;
- в други, предвидени в закон случаи.

Длъжностно лице по защита на данните може да изпълнява функциите си въз основа на един от следните алтернативни начини:

- назначаване на служител в дружеството или организацията;
- съвместяване с друга длъжност, стига да не се поражда конфликт на интереси;
- по граждански договор/договор за услуга.

Отчетност

Отчетността е ново задължение на администраторите на лични данни и основен инструмент за доказване изпълнението на изискванията на Общия регламент за защита на личните данни. Отчетност на практика е способността във всеки един момент администраторът на лични данни да удостовери и да докаже, че обработва личните данни законосъобразно, добросъвестно, про-

зрачно, за конкретни и пропорционални цели, с подходящо ниво на сигурност и защита.

Основните средства за спазване на принципа на отчетност са:

- поддържането на регистри на дейностите по обработване.
- определяне на длъжностно лице по защита на личните данни, когато такова се изисква.
- извършване на оценка на въздействието при наличие на висок риск за правата и свободите на физическите лица.
- своевременно уведомяване на Комисията за защита на личните данни и субекта на данните при нарушения на сигурността.
- прилагане на доброволни механизми за сертифициране и/или спазването на кодекси на поведение.

Оценка на въздействието

Оценката на въздействието е важен инструмент за отчетност, тъй като помага на администраторите не само да спазват изискванията на Общия регламент за защита на личните данни, но и да демонстрират, че са взети подходящи мерки, за да се гарантира спазването на регламента. Оценката на въздействието е процес, предназначен:

- да опише обработването на лични данни,
- да оцени необходимостта и пропорционалността на обработката и
- да спомогне за избора на най-подходящите технически и организационни мерки за защита.

Оценката на въздействието може да се отнася до единична операция за обработване на данни или до многобройни повтарящи се или сходни операции.

В съответствие с подхода, основан на риска, въведен с Общия регламент за защита на личните данни, извършването на оценка на въздействието върху защитата на личните данни не е задължително за всяка операция по обработване. Тя се изисква само когато обработването на лични данни има вероятност да доведе до висок риск за правата и свободите на физическите лица.

Операции по обработване, които по правило пораждат висок риск, са например извършването на:

- автоматично вземане на решения, включително профилиране;
- мащабно обработване на данни, разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения или членство в синдикални организации, генетични данни, биометрични данни, данни за здравословното състояние или данни за сексуалния живот или сексуалната ориентация, както и данни за предишни осъждания на лицето;
- систематично мащабно наблюдение на публично достъпна зона.

Оценка на въздействието може да бъде извършена от самия администратор, негов служител или от лице, външно за организацията, но отговорността за извършването ѝ остава на самия администратор. Администраторът задължително трябва да потърси съвет от служителя по защита на данните, когато такъв е определен, а взетите решения следва да бъдат документирани.

Общият регламент за защита на личните данни определя минималното съдържание на оценката на въздействието:

- системен опис на предвидените операции по обработване и целите на обработването, включително, ако е приложимо, преследвания от администратора законен интерес;
- оценка на необходимостта и пропорционалността на операциите по обработване по отношение на целите;
- оценка на рисковете за правата и свободите на субектите на данни,

- мерките, предвидени за справяне с рисковете, включително гаранциите, мерките за сигурност и механизмите за осигуряване на защитата на личните данни и за демонстриране на спазването на настоящия регламент, като се вземат предвид правата и законните интереси на субектите на данни и на други заинтересовани лица.

Администраторът задължително провежда предварителна консултация с КЗЛД, ако оценката на въздействието върху защитата на данните покаже, че обработването ще породи висок риск, ако не се предприемат ефективни мерки за ограничаването му.

Защитата на личните данни на етапа на проектирането (privacy by design) и по подразбиране (privacy by default)

Защитата на личните данни на етапа на проектирането и по подразбиране са нови задължения за администраторите на лични данни, въведени за първи път с Общия регламент за защита на данните. Независимо че основната им цел е да се намалят и по възможност елиминират рисковете за личната неприкосновеност, прилагането им от администраторите на практика спомага за намаляване на евентуални последващи разходи за привеждане на информационните системи в съответствие с изискванията на регламента.

Защитата на личните данни на етапа на проектирането се изразява в задължението на администраторите да въведат подходящи технически и организационни мерки преди започването на обработката на лични данни (на етапа определяне на целите и средствата за обработване), като осигурят тяхното прилагане през целия жизнен цикъл на данните. Това задължение е от съществено значение в контекста на новите технологии и предоставянето на услуги на информационното общество. Защитата на етапа на проектиране трябва да бъде взета предвид още от началните етапи на планиране, изграждане и функциониране на всеки бизнес процес, информационна система и/или предоставянето на услуга, продукт или приложение.

Изборът на конкретни технически и организационни мерки зависи изцяло от администратора, който следва да отчита достиженията на техническия прогрес, разходите за прилагане, естеството, обхвата, контекста и целите на обработването, както и породените от обработването рискове с различна вероятност и тежест за правата и свободите на физическите лица. Такива подходящи мерки биха могли да бъдат псевдонимизация и/или криптиране на данните, залагане на функционалности за автоматизирано отчитане на сроковете за съхранение и автоматичното им изтриване след изтичането им и др.

Защита на личните данни по подразбиране изисква администраторите да прилагат механизми, които по подразбиране гарантират изпълнението на следните изисквания:

- Само минималното количество лични данни и операции по обработване, които са абсолютно необходими за постигането на всяка специфична цел, биват обработвани.
- Данните са съхранявани за минималния срок, абсолютно необходим за постигане на целите на обработване (например, за периода необходим да се предостави съответния продукт или услуга) и след това заличени при спазване на съответните правила и процедури;
- Всеки достъп, предаване или споделяне на данни е допустим, само при наличие на валидно правно основание за това (например, съгласието на субекта на данни или правни задължения на администратора).

В интернет средата, най-често социалните мрежи, защитата на данните по подразбиране изисква активиране по подразбиране на най-стриктните настройки за поверителност, които не позволяват автоматично споделяне на данни. Напр. информация за дадено лице, публикувана в социалните мрежи, не трябва да бъде достъпна и видима за неограничен кръг лица по подразбиране, освен ако самото лице, за което информацията се отнася, не го разреши със свое активно утвърдително действие.

Административно-наказателна отговорност по Общия регламент за защита на личните данни

Един от основните механизми за гарантиране спазването на високите стандарти на регламента от всички администратори, които са задължени да прилагат Регламент 2016/679, е възможността надзорните органи по защита на личните данни да налагат значителни по размер административни наказания – до 20 млн. евро или до 4% от общия годишен световен оборот, която от двете суми е по-висока.

За осигуряване на ефективност, пропорционалност и възпиращ ефект регламентът въвежда следните критерии при определяне на вида административно наказание (парична санкция или друга корективна мярка) и неговия размер.

Обстоятелствата, които се оценяват са следните:

а) естеството, тежестта и продължителността на нарушението, като се взема предвид естеството, обхватът или целта на съответното обработване, както и броят на засегнатите субекти на данни и степента на причинената им вреда;

б) дали нарушението е извършено умишлено или по небрежност;

в) действията, предприети от администратора или обработващия лични данни за смекчаване на последиците от вредите, претърпени от субектите на данни;

г) степента на отговорност на администратора или обработващия лични данни като се вземат предвид технически и организационни мерки, въведени от тях;

д) евентуални свързани предишни нарушения, извършени от администратора или обработващия лични данни;

е) степента на сътрудничество с КЗЛД с цел отстраняване на нарушението и смекчаване на евентуалните неблагоприятни последици от него;

ж) категориите лични данни, засегнати от нарушението;

з) начина, по който нарушението е станало известно на КЗЛД, по-специално дали и до каква степен администраторът или обработващият лични данни е уведомил за нарушението;

и) когато на засегнатия администратор или обработващ лични данни преди са налагани мерки, във връзка със същия предмет на обработването, дали посочените мерки са спазени;

й) придържането към одобрени кодекси на поведение или одобрени механизми за сертифициране; и

к) всякакви други утежняващи или смекчаващи фактори, приложими към обстоятелствата по случая, като пряко или косвено реализирани финансови ползи или избегнати загуби вследствие на нарушението.

При леки нарушения или ако глобата, която може да бъде наложена, представлява несъразмерна тежест за администратор-физическо лице, вместо глоба може да бъде приложена друга корективна мярка.

КОМИСИЯ ЗА ЗАЩИТА
НА ЛИЧНИТЕ ДАННИ

Комисия за защита на личните данни
бул. "Проф. Цветан Лазаров" № 2
1592 София
Електронна поща: kzld@cpdp.bg
Интернет страница: www.cpdp.bg