GDPR - ОСНОВНИ ПРИНЦИПИ ПРИ ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

АКТУАЛНО - ЛИЧНИ ДАННИ

GDPR - основни принципи при защита на личните данни

Десислава Кръстева, адвокат
съдружник в Адвокатско дружество „Димитров, Петров и Ко.“ и старши правен експерт във Фондация „Право и интернет“

Актуално към 14. 02. 2018 г.

***Бел. ред.** За разлика от действащия досега режим за защита на личните данни, който масово се възприемаше само като изискване за **еднократна регистрация на администраторите на лични данни**, което изискване **от 25.05. 2018 г. отпада**, вече **всички ще трябва да третират** защитата на личните данни като **постоянен процес**.*

*Адекватната реакция на тази нова ситуация от администраторите на лични данни изисква първо да се потърси **отговор на няколко принципни въпроса**, на пръв поглед може би по-теоретични, но без изясняване на които не биха могли да се предприемат последващите практически действия при разработване на необходимите процедури, свързани със защитата и обработването на лични данни:*

1. ***Обработваме ли лични данни? Ако да, какви?***
2. ***Кои са основните принципи, които следва да съблюдаваме при обработването на лични данни?***
3. ***Какъв е изцяло новият принцип за отчетност, който трябва да се спазва от администратора?***

***Коментарът е първият** от **поредицата коментари**, посветени на новите моменти в защитата на личните данни.*

***В следващия брой на списанието** ще бъдат публикувани **още два коментара** относно новите моменти в защитата на личните данни, а именно **два** отделни **материала** относно **задълженията** на:*

- ***администраторите на лични данни и***
- ***обработващите лични данни.***

Основни аспекти на реформата

Личните данни са ***мощен икономически ресурс*** и са във фокуса на множество класически и нововъзникващи бизнес сектори и пазари.

Тепърва бизнесът открива нови начини за повишаване на ефективността и приходите си чрез обработването на лични данни.

Тяхната **защита**, обаче, е **абсолютна предпоставка за защитата и гарантирането на основните права и свободи гражданите** в съвременния високотехнологичен свят.

Нещо повече, самото **право на защита на личните данни** е признато за ***самостоятелно основно право*** на гражданите на ЕС в **Хартата на основните права на ЕС** (ХОПЕС) (1).

Поради това и режимът на защитата им днес е предмет на една от най-дискутираните и значими законодателни реформи, а санкциите за нарушения в сферата достигат рекордни размери.
Регламент № 2016/679, познат още като ***Общ регламент за защита на личните данни*** (**GDPR**) ще започне да се прилага **от 25 май 2018 г.**

Регламентът изцяло реформира и идва да замени действащите правила и изисквания за защита на личните данни, а при **нарушение** на новите правила предвижда налагането на санкции в размер:

- **до 4% от годишния световен оборот** за **предходната финансова година** на предприятието ***или***
- **20 000 000 евро,**

която от ***двете суми*** **е по-висока**.

Стъпвайки върху концепцията, заложена в ***Директива 95/46/ЕО на Европейския парламент и на Съвета от 24 октомври 1995 година за защита на физическите лица при обработването на лични данни и за свободното движение на тези данни*** (**Директивата**), GDPR надгражда и съществено завишава изискванията към защитата на личните данни.

Основните принципи, свързани със защитата на личните данни, познати от:

- ***Конвенция № 108 на Съвета на Европа от 28 януари 1981*** г. ***за защита на лицата при автоматизираната обработка на лични данни*** и
- ***Директивата***,

са преформулирани, допълнени и **доразвити от GDPR**.

В допълнение макар самата дефиниция на термина „лични данни“ в GDPR да следва тази от Директивата, систематичното тълкуване на тази дефиниция с други текстове (включително от Преамбюла) на GDPR сочи, че **терминът „лични данни“ би могъл да бъде тълкуван *много по-широко*** и съответно да обоснове **далеч по-широко приложно поле на изискванията на GDPR** от това на Директивата.

Не на последно място, **за разлика от досегашния режим**, задължени да **спазват изискванията за защита** на личните данни вече са:

- ***не само*** т. нар. **администратори** (*лицата, които определят целите и средствата за обработване на личните данни*), но ***и***
- **обработващите лични данни** (*лицата, обработващи лични данни **от името на администратора***).

Всичко това, наред с **разширените и засилени права на физическите лица**, чиито лични данни се обработват, поставя ***сериозни предизвикателства пред всеки бизнес*** и всяка организация.

Първата и най-ключова стъпка към справянето с тези предизвикателства и към спазването на строгите изисквания GDPR е **осъзнатото обработване на лични данни** и съблюдаването на **основните принципи** предвидени в **чл. 5 от GDPR**.

1. Лични данни

Обработваме ли лични данни?

Ако да, какви?

Това са първите въпроси, на които е необходимо всяка организация да си отговори, за да пристъпи към съобразяване с изискванията на GDPR.

Отговорът на първия въпрос изглежда лесен.

В съвременния свят **няма организация**, която да може да функционира и да реализира бизнес дейностите си **без да обработва лични данни**:

- данни за служители,
- за потребители-физически лица,
- за представителите и служителите на други организации (клиенти, подизпълнители, потенциални партньори и т.н.),
- данните от контрола на достъпа до нашите офиси и помещения,
- видеонаблюдение,
- аудиозаписи на телефонни разговори (напр. при обслужване на клиенти) и т.н., и т.н.

Какви лични данни обработваме?

Далеч **по-сложен и комплексен е въпросът за *определяне на всички данни***, които е необходимо да **се третират като лични данни** и да се **защитават съобразно изискванията на GDPR.**

В този момент е **изключително важно** да се подчертае и изясни, че **обхватът на *понятието лични данни*** е **изключително широко**.

Съгласно дефиницията в GDPR:

- ***Всяка информация*** може да съставлява лични данни.

Не само очевидните идентификационни данни като имена, ЕГН, данни по документ за самоличност и т. н. са лични данни, а **всяка информация**, която може да доведе ***до идентифицирането на определено физическо лице***.

Няма изчерпателен списък на информацията, която е лични данни.

При преценката дали обработваме лични данни е необходимо винаги да се преценяваме обработваната информация в нейната съвкупност.

Така например, един работодател обработва не само идентификационните данни на служителите си, но и:

- *информацията за техните договори,*
- *осигурителен доход,*
- *възнаграждения, удръжки,*
- *бонуси и поощрения,*
- *образование,*
- *опит,*
- *отсъствия,*
- *оценки на представянето,*
- *представяне и постигнати резултати в работата,*
- *подадени жалби и сигнали и д*
- *дори информация, отнасяща се до хобита, интереси, предоставяни допълнителни поощрения като абонаменти за фитнес зала, снимки от фирмени събития и т. н.*

- Условие определена **информация да се счита за лични данни** е ***тя да се отнася до физическо лице.***

Връзката между:

- ***данните*** и
- ***физическото лице***

не е необходима да е пряка и **лесно забележима**.

Така дори информация, например, за функционирането определени „умни“ домакински уреди би могла да съставлява лични данни, ако може да бъде свързана по някакъв начин с физическите лица - ползватели на тези уреди.

Връзката между данните и субекта може да е:

- ***пряка*** или
- ***непряка***.

Не е необходимо данните непосредствено да идентифицират лицето.

Те може да ***опосредстват връзката към други данни*** и по този начин **в съвкупност да довеждат до идентифициране на субекта.**

Например, едно лице може да бъде идентифицирано:

- **пряко** по ***име*** или

- **непряко** по ***телефонен номер, регистрационен номер на автомобил, номер на социално осигуряване, номер на паспорт или чрез комбинация от значими критерии, които позволяват лицето да се разпознае в малка група, към която принадлежи*** (възраст, професия, местожителство и др.).

Физическото лице може вече да е идентифицирано или може да бъде идентифицирано след допълнителни действия. Това означава, че информацията, която до момента е била налична за лицето, може да не е достатъчна за неговото идентифициране, но в съвкупност с конкретни допълнителни данни или допълнително обработване да позволи неговото идентифициране.

- И накрая, физическите лица, за които се отнася информация, е необходимо да са ***идентифицирани или идентифицируеми.***

Не е необходимо информацията, която обработваме да позволява ***сигурна идентификация*** на физическото лице, за което се отнася.

Потенциалната възможност въз основа на информацията, която обработваме ***да идентифицираме*** (*пряко или непряко*) едно физическо лице би означавала, че **обработваме лични данни**.

Съгласно GDPR „**физическо лице, което може да бъде идентифицирано**“, е всяко лице което **може да бъде идентифицирано**, ***пряко*** или ***непряко***, по-специално чрез **идентификатор** като:

- ***име***,
- ***идентификационен номер***,
- ***данни за местонахождение***,
- ***онлайн идентификатор*** или
- ***по един или повече признаци***, специфични за физическата, физиологичната, генетичната, психическата, умствената, икономическата, културната или социална идентичност на това физическо лице“.

Изброените в дефиницията „идентификатори“ и за “специфични признаци“ са примерни и могат да включват и всякакви други типове информация, представляваща идентификатор или специфичен признак.

Ново спрямо дефиницията в досегашния закон е, че в изброяванията за идентификатори са включени изрично и **„онлайн идентификаторите“**.

Такива биха могли да са:

- **IP адресите**,
- „бисквитките“,
- етикетите за радиочестотна идентификация (RFID) и
- други ***идентификатори, предоставени от устройства, приложения, инструменти и протоколи***.

Най-общо **онлайн идентификаторите** са данни, които се получават от използваните устройства, приложения, инструменти и протоколи и ***оставят следи***, които в съчетание с друга информация, получена от сървърите, могат да се използват за **създаването на профили на физическите лица** и за тяхното идентифициране.

Анонимизирани данни

GDPR *не променя* по същество ***дефиницията за лични данни***, която съществуваше:

- в Директивата и съответно
- в Закона за защита на личните данни,

а я **конкретизира чрез по-детайлни примерни изброявания** на ***отделни типове лични данни***.

Запазва се, обаче, **тенденцията към *все по-широко* тълкуване на понятието „лични данни“.**

В тази връзка **специално внимание** следва да се обърне и на въпроса ***кога може да се приеме, че физическото лице не може да бъде идентифицирано***, т.е. че обработваме изцяло анонимни/анонимизирани данни.

Принципите и изискванията на защита на личните данни не следва да се прилагат по отношение на анонимна информация, т.е. информация, която не е свързана с идентифицирано или подлежащо на идентифициране физическо лице, или по отношение на лични данни,

които са анонимизирани по такъв начин, че физическото лице да не може или вече не може да бъде идентифицирано.
GDPR не се отнася за обработването на такава анонимна информация, включително за статистически или изследователски цели.

Новост в уредбата на личните данни са **текстовете на чл. 11** и съответно:

- ***Съображение 26*** и
- ***Съображение 57***

от GDPR, които определят **критериите за тази преценка**.

Съгласно **Съображение 26** от GDPR:

*„За да се определи дали дадено физическо лице може да бъде идентифицирано, следва **да се вземат предвид всички средства**, като например подбирането на лица за извършване на проверка, **с които е най-вероятно да си послужи администраторът или друго лице, за да идентифицира пряко или непряко даденото физическо лице**.*

За да се установи дали има достатъчна вероятност дадени средства да бъдат използвани за идентифициране на физическото лице, следва да се вземат предвид всички обективни фактори, като разходите и количеството време, необходими за идентифицирането, като се отчитат наличните към момента на обработване на данните технологии и технологичните развития.“

Така се налага изводът, че **може да е налице обработване на лични данни**, дори и ако самият администратор, който борави с информацията, не може да идентифицира физическото лице, **стига друго лице, различно от администратора, да може да го идентифицира.**

Цитираните текстове са ясен израз на тенденцията понятието „лични данни“ да се тълкува все по-широко. Те разширяват приложението на GDPR и изискванията към обработването дори към обработването на данни, които сами по себе си не позволяват на администратора да идентифицира физическите лица, за които се отнасят.

С оглед на горното и предвид динамично развиващите се технологии за автоматизирано обработване на информация и профилиране, както и нарастващия обем информация, достъпен в онлайн пространството, **пълната анонимизация се оказва все по-трудно осъществима**.

В редица случаи, в които се твърди, че се обработва анонимизирана информация, поради широкия обхват на дефиницията, може да се окаже, че е налице обработване на лични данни по смисъла на GDPR и съответно ще е необходимо да се съблюдават принципите и изискванията му. **Особено рискови** в този контекст са, например, т. нар. ***статистически, обобщени или агрегирани*** лични данни, които, макар и несъдържащи преки идентификационни данни, могат да позволят идентифицирането на физическите лица (особено в случаи, когато се обработват ***данни, отнасящи се до тесен кръг от физически лица***).

2. Основни принципи, съблюдавани при обработването на лични данни

Кои са основните принципи, които следва да съблюдаваме при обработването на лични данни?

Чл. 5 на GDPR дефинира **основните принципи**, които е задължително да бъдат съблюдавани при обработването на лични данни. Тези принципи са най-съществените и ключови изисквания, чрез които се цели да се гарантира правото на защита на личните данни.

Личните данни **трябва:**

- **Да бъдат обработвани *законосъобразно, добросъвестно* и по *прозрачен* начин по отношение на субекта на данните *(„законосъобразност, добросъвестност и прозрачност*“)**

Този принцип означава преди всичко личните данни задължително да бъдат обработвани въз основа на ***поне едно*** от **правните основания** предвидени в **чл. 6 от GDPR:**

- ***законово задължение**;*
- ***съгласие на субекта**;*
- ***договор**;*
- ***обществен интерес**;*
- ***официално правомощие**;*
- ***защита на жизненоважни интереси на субекта или на друго физическо лице**;*
- ***легитимен интерес на администратора или на трета страна**.*

На следващо място ***законосъобразността на обработването*** изисква същото да е в **съответствие с *цялото действащо законодателство***, а не само това за защита на личните данни.

Добросъвестното обработване от своя страна изисква преди всичко **извършваното обработване** да не засяга неоправдано ***по негативен начин физическите лица***, чиито данни се обработват, да не противоречи на морала и добрите нрави.

Пряко, свързан с принципа за добросъвестност, е ***принципът за прозрачност***, които изисква обработването на личните данни да се осъществява по ***прозрачен за физическите лица***, чиито данни се обработват, начин.

Това означава **физическите лица да са информирани по ясен, прост, лесен за разбиране и достъпен начин за извършваното обработване спрямо техните данни**, както и за правата, които имат във връзка със защитата на личните им данни.

Принципът за прозрачност пряко кореспондира и е **доразвит** с:

- **правото на информация и** на достъп на субектите на лични данни и

- със **задълженията** на ***администраторите за предоставяне на информация*** по **Глава III, Раздели I и II** от GDPR.

- **Да бъдат събирани за конкретни, изрично указани и легитимни цели и не се обработват по-нататък по начин, несъвместим с тези цели**; ***(„ограничение на целите“)***;

Принципът за ограничение на целите изисква личните данни винаги да бъдат обработвани за ***конкретни и предварително определени цели***.

Обработването за последващи цели, различни от и несъвместими с първоначалните цели за събирането на данните, ***принципно е недопустимо***.

Това означава, че от **администраторите** се очаква и изисква ***предварително, ясно*** и ***изчерпателно*** **да дефинират целите**, за които им е необходимо да обработват лични данни.

Макар и този принцип да не е нов, той поставя едни от **най-съществените предизвикателства пред администраторите**, тъй като изисква **още в най-началните етапи *да планират целите*, за които ще обработват личните данни**.

Всяко допълване *на тези* цели след като данните са събрани, е свързано с необходимост от:

- **допълнително уведомяване на физическите лица**, събиране на тяхното съгласие ***или***

- осигуряване на ***друго правно основание за законосъобразното обработване за новите цели*** (напр. предоговаряне) и промени в съдържанието на водените регистри и документи.

Така **самият факт, че един администратор разполага с определен набор от данни**, ***не означава***, че свободно и необезпокоявано може ***да ги обработва за всички цели***, за които прецени и ***да добавя нови и нови цели*** към първоначално предвидените.

По същия начин в редица случаи е ***недопустимо използването на публично достъпни лични данни*** (напр. част от публичен регистър) за **цели, различни от тези, за които съответните данни са направени достъпни.**

- **Да са подходящи, свързани със и ограничени до необходимото във връзка с целите, за които се обработват *(„свеждане на данните до минимум“)***

Принципът за свеждане на данните до минимум е пряко свързан с принципа за ограничение на целите.

Този принцип изисква да се обработват **само и единствено лични данни**, които са ***необходими за и съответстващи на конкретните цели***, за които тези данни се обработват.

Два са основните аспекти, за които трябва да се държи сметка при преценка дали съблюдаваме ***принципа за свеждане на данните до минимум***:

- **необходимостта** им за (дали данните действително са необходими за постигане на целта на обработването) и

- **пропорционалността** им спрямо преследваната цел (дали обработваните данни са адекватни, съответстващи и пропорционални спрямо конкретната цел).

Така например, **информацията, която събира и обработва една банка** или **небанкова финансова институция** за целите на ***идентификация на нов клиент*** при встъпване в договорни отношения с него, е напълно **различна като обем и обхват** от информацията, която би била необходима за ***идентификацията на нов потребител*** при регистрацията му **в онлайн форум** на един стандартен новинарски уебсайт.

В случай, че преследваната цел може да бъде постигната чрез обработването на по-малко данни, останала част от данните не следва да бъде събирана или обработвана.

Тук е изключително важно да се подчертае, че **несъответствието с изискванията на този принцип са задължителни** и ***не могат да бъдат преодолени*** дори и със съгласието на засегнатите физически лица.

Така в дадения по-горе пример **дори и при наличие на изрично съгласие** от страна на **потребителите**, регистриращи се във форума на новинарския сайт, ***събирането и обработването на данни за техния осигурителен доход и платежоспособност*** не би било пропорционално на целите по администриране и управление на форума и съответно **би нарушило изискванията на GDPR.**

- **Да бъдат точни и при необходимост да бъдат поддържани в актуален вид *(„точност“)***

Този принцип изисква от администраторите да 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.

На този принцип кореспондират правата на физическите лица да поискат коригиране на своите данни и съответно уведомяване на третите лица, на които тези данни са разкрити за извършените корекции.

- **Да бъдат съхранявани 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 *(„ограничение на съхранението“)***

Принципът за ограничение на съхранението е пряко свързан с принципите за ограничение на целите и за свеждане на данните до минимум.

На конкретна цел съответства и е допустимо да се обработва определен конкретен набор от данни, които могат да бъдат обработвани (вкл. съхранявани) единствено до постигането на целите, за които данните са били събрани.

По този начин **обработването/ съхранението на данни за неограничен период от време** е ***недопустимо и противоречи на изискванията на GDPR***.

Така например, ***автобиографиите на кандидати за работа***, кандидатствали по конкретна обява за конкретна позиция, би било ***недопустимо*** **да бъдат съхранявани за неограничен срок или за прекалено дълъг срок** (напр. 2-3 години) след приключване на процеса по избор на подходящ кандидат, тъй като целта за събирането и обработването им е приключила с назначаването на избрания кандидат.

- **Да бъдат обработвани 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 ***(„цялостност и поверителност“***).

Принципът за цялостност и поверителност е **нов принцип**, въведен с GDPR, макар по същество изисквания за осигуряване на защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане чрез прилагане на подходящи технически или организационни мерки да са налице и в действащата до сега уредба в Директивата и Закона за защита на личните данни.

По отношение на този принцип е изключително важно да се подчертае, че **GDPR не въвежда конкретни задължителни мерки за защита на личните данни**, които обработваме.

В текстовете на GDPR, посветени на сигурността на личните данни, са **дадени насоки за подходящи мерки за защита** (като например, ***криптиране***), но какви конкретно мерки да бъдат прилагани следва **всеки администратор да прецени самостоятелно на база на конкретните рискове**, свързани с нарушаването на сигурността на обработваните данни (например, голям брой засегнати лица, риск от кражба на самоличност и др. под.).

3. Отчетност (Accountability)

За да **гарантира съблюдаването на посочените по-горе принципи** GDPR предвижда ***не само посочените по-горе парични санкции***, но и въвежда един **изцяло нов принцип** – ***принципът за отчетност***.

Съгласно този принцип **администраторът носи отговорност** и ***трябва да е в*** **състояние да докаже** ***спазването на всички изброени по-горе принципи***.

Безспорно този принцип поставя **тежестта на доказване** при възникване на спорове с физическо лице – субект на данни, относно нарушения на изискванията за защита на личните данни **върху администратор**.
Извън това, обаче, принципът за отчетност може да се тълкува и много по-широко като изискване **администраторът** ***по всяко време*** **да може да демонстрира и доказва, че** ***съблюдава посочените принципи***.

Този принцип пряко кореспондира с **редица** ***конкретни задължения*** **за администраторите**, въведени в GDPR като:

- ***Задължението за водене на регистриотносно дейностите по обработване на лични данни по чл. 30 от GDPR;***
- Изискванията по чл. 28 от GDPR ***отношенията между администратор и обработващ да са уредени писмено*** и обработването на данните да се извършва само съобразно **документираните нареждания**на администратора;
- Изискванията ***оценката за въздействие да бъде изготвяна в писмена форма*** и други.

Принципът за отчетност цели да гарантира, че обработването на личните данни се осъществява по осъзнат, прозрачен, документиран и съответно лесно проследим начин.

Заключение

В заключение може да се посочи, че спазването на принципа за отчетност на практика ще изисква от администраторите да планират и **предварително да определят в пълнота и конкретика**:

- ***Какви лични данни ще обработват***;
- ***За какви конкретни цели ще обработват данните***; и
- ***Сроковете, в които ще е необходимо обработването*** или критерии за определянето им (ако не може да се определи предварително конкретен срок).

Единствено въз основа на такова планиране и **предварително определяне на данни, цели и срокове** за постигането им биха могли да се изпълнят и изискванията за отчетност като документират по надлежен начин осъществяваните от дейности по обработване и **уреждането по надлежен начин** на отношенията със:

- ***субектите (физическите лица, чиито данни се обработват) и***

- ***администраторите и***

- ***обработващите, с които се осъществява обмен на лични данни.***

Харта на основните права на ЕС

…….

Член 8

Защита на личните данни

1. Всеки има право на защита на неговите лични данни.

2. Тези данни трябва да бъдат обработвани добросъвестно, за точно определени цели и въз основа на съгласието на заинтересованото лице или по силата на друго предвидено от закона легитимно основание. Всеки има право на достъп до събраните данни, отнасящи се до него, както и правото да изиска поправянето им.

3. Спазването на тези правила подлежи на контрол от независим орган.

…….