ОСНОВАНИЯ ЗА ОБРАБОТВАНЕТО НА ЛИЧНИ ДАННИ И ПРАВА НА ГРАЖДАНИТЕ – КЛЮЧОВИ ПРОМЕНИ ПО GDPR

АКТУАЛНО - ЛИЧНИ ДАННИ

Основания за обработването на лични данни и права на гражданите – ключови промени по GDPR

Д-р Мартин Захариев,
адвокат в Адвокатско дружество „Димитров, Петров и Ко.“ и експерт във Фондация „Право и интернет“

Актуално към 14. 02. 2018 г.

***Бел. ред.** За разлика от действащия до сега режим за защита на личните данни, който с **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 з**ащитата на личните данни като **постоянен процес**.*

*За да върне контрола на гражданите върху ползването на личните им данни, новият европейски регламент за защита на личните данни - Регламент 2016/679 (GDPR) **засилва техните права** като:*

- ***разширява обхвата на някои от съществуващите** и*
- ***предвижда някои непознати досега права**.*

*Тъй като **най - високите санкции, предвидени в GDPR**, са за **нарушаване на правата на гражданите и основанията за обработване на личните им данни**, изясняването на промените, свързани със защитата на личните данни, изисква да се започне с изясняване на:*

- *основанията за законосъобразно обработване на личните данни;*
- *новите/променените права на субектите на данни.*

***Коментарът е вторият** 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.***

Общи бележки

В последните месеци изключително популярна тема в целия ЕС, в т. ч. и в България, е предстоящото прилагане на **новия европейски регламент за защита на личните данни *Регламент 2016/679*** (**GDPR**).

Това до голяма степен може да се обясни с безпрецедентно високите санкции, които GDPR предвижда за нарушение на изискванията му, най-високите от които достигат:

- **до 20 милиона евро** *или*,
- в случай на предприятия, **до 4 % от общия световен годишен оборот на предприятието за *предходната година***,

която от двете **е по-висока.**

Санкциите по сега действащия у нас Закон за защита на личните данни (ЗЗЛД) далеч да не са пренебрежими - същите основно варират между 10 000 и 100 000 лева – те обаче са несъизмерими с максималните размери на санкциите по GDPR. Това обуславя все по-голямата чувствителност на пазара по темата за защитата на личните данни.

И макар регламентът да е в сила още от май 2016 г. (1), същият предизвиква по-сериозното внимание на бизнеса и институциите едва напоследък, защото наближава датата, от която **GDPR започва да се прилага** - **25 май 2018 г.**

Приложението на GDPR бе отложено във времето спрямо датата на влизането му в сила поради сериозните промени, които регламентът въвежда в режима за защита на личните данни – идеята на европейския законодател е всички субекти, обработващи лични данни (частни компании, публични институции и други образувания) да приведат дейността си в съответствие с новите изисквания.

Настоящият анализ има за цел да изясни някои ключови промени и нововъведения, които GDPR ще въведе в режима на защитата на личните данни, а именно:

1. ***Основанията за законосъобразно обработване на личните данни***;
2. ***Новите/променените права на субектите на данни***.

Настоящият анализ е без претенции за изчерпателност, защото комплексният анализ на промените, въведени с GDPR, далеч би надхвърлил целите на настоящото изложение (2).

1. Основания за законосъобразно обработване на лични данни

Основанията за обработване на лични данни по GDPR са ***същите***, които са уредени в Директива 95/46 и транспониращият я у нас ЗЗЛД.

Това са:

- **Съгласие на субекта на данните;**
- Договор със субекта на данните/ предприемане на стъпки по сключването на договор по искане на субекта на данните;
- Законово задължение на администратора;
- Жизненоважни интереси на субекта на данните/ на друго физическо лице;
- Задача от обществен интерес или упражняването на официални правомощия на администратора;
- **Легитимните (законни) интереси на администратора/на трета страна, които имат преимущество пред интересите, основните права и свободи на субекта на данните.**

Това са алтернативни основания и е достатъчно едно от тези условия да е налице, за да може администраторът законосъобразно да обработва лични данни (разбира се, при спазване на всички останали правила и принципи на GDPR).

Наличието на законово основание за обработването е едно от основните изисквания за обработването на лични данни, неслучайно същото е въздигането като елемент от правото на защита на личните данни по **чл. 8** от Хартата на основните права на ЕС (ХОПЕС) (3).

В контекста на GDPR, ***две от посочените по-горе основания*** заслужават по-специално внимание:

- **съгласието** и
- **законният интерес (4)**.

Съгласието от страна на субекта на данни за обработване на свързани с него лични данни, изразено чрез **писмена декларация, по електронен път или по друг подходящ начин** е едно от най-разпознаваемите основания за обработването на лични данни. **Администраторът** на лични данни следва **да може да докаже,** че ***съгласие е налице***.

Неговото значение е подчертано и в **чл. 8, пар.** 2 ХОПЕС, където то е изведено като пример за легитимно основание за обработването на лични данни.

Независимо от това, за него трябва да се направят няколко **важни предварителни уточнения.**

Често в практиката битува разбирането, че **ако е налице съгласие на субекта на данните за обработването на личните му данни**, това е напълно достатъчно и ***преодолява всякакви законови ограничения пред обработването.***

Това разбиране е **погрешно**.

Действително, в някои хипотези е възможно с помощта на съгласието да се преодолеят определени законови ограничения – напр. при липса на друго основание за предаване на данните в трета държава (т.е. държава извън ЕС), това може да стане със съгласието на субекта на данните. Това обаче както с основание се посочва в теорията, е по-скоро изключение, а не общо правило (5).

Ето защо, важно е да се подчертае, че **съгласието *не се ползва с някаква по-голяма* сила спрямо останалите основания за обработване на личните данни.**

Простото му наличие *не освобождава* администратора от всички **останали изисквания на режима на защита на личните данни**:

- спазване на принципите на защита на личните данни;
- предприемане на подходящи мерки за защита на данните;
- гарантиране на правата на субектите и спазване на задълженията на администратора/ обработващия и други подобни.

Въпреки това, ако съгласието се използва правилно, то може да бъде могъщ инструмент в ръцете на субектите данни, които имат контрол върху обработването (6) и могат да влияят по процесите на обработване на данните им.

Това е така, защото **субектът на данните** е господар на обработването най-малко в **следните аспекти**:

1. Дали да се извърши обработването – **дали въобще да се даде съгласие**, т.е. да съдейства на администратора за осигуряване на правно основание за обработването;

2. В какъв обем да се извърши обработването – **за кои цели субектът да даде съгласието си за обработван**е.

Следва да се отбележи, че с GDPR се изисква **при повече от една цел**, за която се иска съгласие, субектът да има възможност да даде съгласие за всяка **отделна** цел.

3. До кога да се извършва обработването – субектът може **по всяко време да оттегли съгласието за обработване** и ако администраторът не разполага с друго основание, същият следва да прекрати обработването на данните.

Съгласието по GDPR представлява **изявление** или **ясно потвърждаващо действие**, което трябва да бъде:

- **Свободно изразено** – това означава съгласието ***да не е дадено под натиск/ заплаха от неблагоприятни последици за субекта на данните***.

Такъв натиск/неблагоприятни последици може са налице напр. в хипотези, в които цената на дадена стока/ услуга се обвързва от даването/ недаването на съгласие (напр. недаването на съгласие води до предлагането на стоката/услугата на по-висока цена); в които изобщо се отказва предоставяне на услуга при недаване на съгласие и др. под.

Ето защо, ***съгласието не е най-подходящият инструмент за обработване на лични данни в контекста на трудовото правоотношение***.

Фактическата и икономическа неравнопоставеност между работника/служителя и работодателя до голяма степен компрометира изискването съгласието да е дадено „свободно“, т.е. не под натиск.

Затова такова **съгласие, получено от работниците/служителите**, крие ***риск да бъде прието за невалидно.***

Работодателите в *преобладаващия брой* случаи ***не се и нуждаят от съгласие*** за обработване на лични данни на своите работници/ служители, защото тази **обработка се осъществява на други основания** – **изпълнение на законови задължения** в сферата на трудовото, осигурителното и данъчното законодателство; необходимост за изпълнението на договор; легитимен интерес и др.

- **Конкретно** – това означава съгласие да се получава ***за всяка отделна цел***.

Затова администраторите следва да осигурят подходящ механизъм, чрез който **отделните цели да бъдат диференцирани** и субектът да може да дава **съгласие *само* за някоя/някои от целите**.

Ето защо, **декларации**, в които **само** са изброени **различни цели**, а накрая е предвидено **само *едно поле за подпис на субекта***, няма да отговарят на посоченото изискване и ще дисквалифицират даденото съгласие.

- **Информирано** – съгласно GDPR минималните изисквания съгласието да е информирано е субектът да е получил информация (пълна, точна и лесноразбираема) най-малко за ***самоличността на администратора и целите на обработването*** (7).

Според Работната група по чл. 29 (8) **субектът** трябва **да получи** и ***допълнителна информация*** като:

- описание на **категориите данни**;
- **правото да се оттегли съгласието**;
- **информация за използването на данните** за автоматизирано вземане на решения, ***включително профилиране***;

ако данните ще се трансферират в трети държави (9), за които няма адекватно ниво на сигурността **подходящите гаранции за трансфера** и т.н. (10).

- **Недвусмислено** - съгласието не следва да се извлича/ предполага от други действия/ изявления на субекта на данните, а трябва **да се дава чрез *ясно утвърдителен акт***.

То трябва да се дава чрез ***активно*** поведение.

Ето защо, с GDPR ***мълчанието***, предварително отметнатите полета и липсата на действие няма да представляват валидно съгласие за обработване.

Няма пречка съгласието в електронна среда да се даде чрез подходящи средства, **съобразени с конкретните технологии и платформи** – напр. чрез:

- ***поставяне на отметка в дадено поле***,
- чрез избиране на технически настройки за услуги на информационното общество и други подобни.

Ако **съгласието** се дава чрез ***отметка***, обаче, тази отметка следва **да се постави от субекта на данните**.

Отметката не следва да се появява автоматично/„по подразбиране“, т.е. чрез простото зареждане на дадена интернет страница полето срещу текста със съгласието *„Съгласен съм с ....“* ***не*** трябва да бъде предварително отметнато, а **субектът чрез активно поведение следва да го отметне**.

- GDPR въвежда някои **специални правила за даването на съгласие от деца**.

Децата според GDPR са уязвима категория лица и заслужават засилена закрила, тъй като не винаги са в състояние да осъзнаят рисковете, свързани с обработването на личните им данни.

Според GDPR съгласие при предоставяне на услуги на информационното общество от **деца до 16-годишна възраст** следва да се получи от ***носителя на родителската отговорност на детето***.

Държавите членки могат да снижат тази възраст, но не повече от 13 години. У нас е логично да се очаква тази възраст да бъде снижена **до 14 години** в контекста на общите правила за дееспособност по българското право (11).

Извън контекста на услугите на информационното общество, също е ***препоръчително администраторите да получават съгласие от родители/ настойници/ попечители***, защото съгласието е едностранно волеизявление, което по правило следва да се направи от дееспособно лице.

- **На ясен и прост език** – GDPR изисква ***да не се използват сложни юридически термини, които са неразбираеми за масовия потребител***.

Това е възможно да създаде практически затруднения пред администраторите, защото, както бе посочено по-горе, **информацията, която субектите следва да получат при даване на съгласие**, за да бъде същото информирано, е ***доста детайлна според GDPR.***

- **Оттеглянето му е също толкова лесно като даването** – не е нужно съгласието да се оттегля чрез същия механизъм, чрез който е дадено, но този механизъм трябва да е също толкова лесен колкото механизма за получаване на съгласието.

Така например, ако **съгласието се даде чрез отмятане на поле**, теоретично няма пречка същото да се оттегля чрез ***натискане на линк*** – отново един ***„клик" на мишката*** е достатъчен, т.е. оттеглянето е също толкова лесно като даването.

Ако обаче **съгласието трябва да се оттегли чрез обаждане на дадена безплатна телефонна линия**, която приема обаждания между 9:00 и 17:00 ч., това изискване няма да бъде спазено, защото обаждането в работни часове е свързано с по-големи затруднения за субекта от натискането на мишката, което може да стане по всяко време в денонощието (12).

Основанието ***законен (легитимен) интерес*** съдържа **два елемента**, които едновременно трябва да са налице, за да има администраторът годно основание за обработването:

- ***даден интерес, припознат от правото като законен*** (напр. упражняване на правни претенции по съдебен и извънсъдебен ред; опазване на имуществото; борба с прането на пари; предотвратяване на измами и др.), и
- този интерес да има ***преимущество*** спрямо правата, свободите и интересите на субекта на данни.

Необходима е преценка за всеки конкретен случай дали интересът на администратора натежава над интересите на субекта на данните.

Идеята на тази преценка е да се осигури **разумен баланс между интересите на администратора и субекта**, така че **субектът да бъде защитен** от ***непропорционално въздействие при обработването*** **(13)**.

Така например, според Работната група по чл. 29, ***интересът на администратора от използването на биометрични данни на субектите за общо опазване на имуществото*** (напр. контрол на достъпа до дадени помещения) би натежал в по-малка степен от основните права и свободи на субектите.

Въпреки това, ***за определени високо рискови дейности*** (напр. работа с вируси в изследователски лаборатории) въвеждането на биометрична идентификация за контрол на достъпа би могла да бъде оправдана, т.е. в тези **случаи интересът на администратора би натежал над интереса на субектите (14)**.

Тъй като задължение на законодателя е да уреди със закон правното основание за обработването на лични данни от публичните органи, според GDPR това правно основание ***не следва да се прилага спрямо обработването на данни от публичните органи при изпълнението на техните задачи***.

Интересно разрешение е разписаната в преамбюла на GDPR (съображение 47) възможност ***обработването на лични данни за целите на директния маркетинг*** да се разглежда като осъществявано поради законен интерес.

Това разрешение не се съдържа в нормативната част на GDPR, а само в преамбюла, който има значение за тълкуването на нормите.

Като цяло трайното разбиране на КЗЛД в последните години е, че **директен маркетинг** може да се осъществява само **при *предварително* изрично съгласие на субекта на данните.**

Затова е ***препоръчително администраторите да не се предоверяват на законния интерес при маркетингови кампании, а да си осигурят съгласието на субектите на данните***.

2. Права на субектите

Една от основните и най-амбициозни задачи на GDPR е **да върне контролът върху личните данни на европейските граждани**.

Един от механизмите за постигане на това е чрез **засилване правата на субектите на данни**.

Затова GDPR доразвива/ модифицира някои от съществуващите права и предвижда някои напълно непознати до този момент права.

Право на информираност съществува и по сега действащия режим. То се изразява в задължението на администратора да предостави определен набор информация на субектите на данни.

В съответствие с въведения принцип на прозрачност GDPR разширява **обема информация, която трябва да се предостави на субекта на данните**.

Администраторите вече трябва да предоставят и следната допълнителна информация:

- ***Координати за връзка с длъжностното лице по защита на данните*** (ако такова е назначено);
- Целите и ***правното основание*** за обработването - това е много съществено изискване, защото предполага ***привързването*** на всяка конкретна цел с конкретното основание за нея – например,

- управление на човешките ресурси – *изпълнение на договор*;
- финансово счетоводна дейност – *законово задължение* и *изпълнение на договор* и т.н.

Администраторите трябва да са в състояние **предварително**:

- да определят целите за обработването и
- да идентифицират правилно кореспондиращото им основание за обработването;

- При основание законен интерес администраторите трябва да посочат ***конкретния законен интерес***.

Абстрактното позоваване на законен интерес няма да бъде достатъчно – например, целта осъществяване на контрол върху достъпа до помещенията може да се привърже със **законен интерес, свързан с опазване имуществото на работодателя**.

- Когато е приложимо, **намерението на администратора да предаде личните данни на трета държава/** международна организация.

Тук следва да се предостави информация за наличието/ отсъствието на решение на Европейската комисия относно адекватното ниво на защита или, ако няма такова решение и има предаване чрез подходящи гаранции – информация за тези гаранции и средствата за получаване на копие от тях или на информация къде са налични.

- **Срок за съхранение на данните**, а ако такъв срок не може да се посочи – ***критерии за определянето му***.

Тук следва да се обърне внимание, че в практиката често битува разбирането, че данните, събрани в контекста на трудовото правоотношение, трябва да се съхраняват за 50-годишен срок.

Това разбиране е погрешно.

У нас **липсва унифицирана правна уредба, като за различни категории носители се прилагат различни срокове на съхранение**.

Относно посочените 50 години следва да се има предвид, че този срок е законоустановен единствено за съхранението ведомостите за заплати, трудовият договор, допълнителните споразумения към него, заповедите за ползван неплатен отпуск над 30 работни дни, заповедите за прекратяване и неполучените от работниците или служителите трудови книжки, дневниците и екземпляр от издадените удостоверения в инспекциите по труда за трудови книжки, издадени от тях (15).

За останалите носители на информация сроковете са различни и администраторите трябва да съблюдават съответните законови изисквания или, когато законът не предвижда срок, да установят разумен такъв.

- **Право на оттегляне на съгласието** – тук важи казаното по-горе при съгласието.
- **Право на жалба до надзорен орган** – субектите трябва да бъдат информирани ***къде могат да упражнят правата си при нарушение на GDPR***. Това изискване пряко кореспондира с принципа на прозрачност.
- **Информация за автоматизирано вземане на решения**/ профилиране (16) и – субектите трябва да получат определена информация, когато по автоматизиран път (без човешка намеса) ще бъдат вземани решения спрямо тях – например, практики по подбор на персонал или оценка на кредитоспособността. Субектите трябва да получат информация относно използваната логика и значението и предвидените последствия от това обработване.
- ***Правото на изтриване*** по същество **не е ново право**.

И по действащия режим съществува правото на заличаване на личните данни. С GDPR се доразвиват хипотезите, при които това право може да се упражни, както и процедурата по упражняването му.
Най-общо казано, ако е налице „проблем“ със законосъобразността на обработването - ***съгласието е оттеглено, целите са постигнати***, няма правно основание за обработването и др. под. администраторът, при упражнено право на изтриване, следва **да изтрие данните без ненужно забавяне**.

Нещо повече, ако администраторът е направил такива данни публично достояние, той трябва чрез „разумни стъпки“ да уведоми всички други администратори, обработващи данните, че субектът на данните е поискал от тях изтриване на всички връзки, копия или реплики на тези данни.

Правото на изтриване не е абсолютно и неговото упражняване следва винаги да се балансира с други права като правото да се търси и разпространява информация, свободата на словото, установяване, упражняване и защита на правни претенции и др. под.

- ***Право на преносимост на данните*** е **ново и непознато до този момент право**. То е своеобразна еманация на правото на достъп до данните.

То се прилага само при едновременното наличие на **две предпоставки**:

- ***обработването*** се извършва на едно от следните **две основания**:

1. ***съгласието*** и
2. ***изпълнението на договор***.

Тези две основания имат и най-голямо практическо приложение в отношенията бизнес-клиенти; и

- ***обработването*** се извършва по **автоматизиран начин** (т.е. със средствата на информационните и комуникационните технологии). Това право не се прилага при обработването на хартиени носители на лични данни.

В ***обхвата*** на това право се включват ***личните данни на субекта***, които той е ***предоставил*** на администратора.

Всички данни, които са анонимни, или не се отнасят до субекта на данните, не биха попаднали в обхвата на това право.

В обхвата обаче се включват данни за псевдонимите, които ясно могат да бъдат свързани с даден субект на данни (например тъй като той е предоставил съответния идентификатор) (17).

Макар наглед да няма съмнение кога субектът на данните е предоставил данните на администратора – например, при попълване на данни за регистрация на акаунт, при попълване на онлайн декларации и др. подобни.

Работната група по чл. 29 тълкува това понятие разширително. Според нея, данни, предоставени от субекта на данни са още данните, които се генерират в резултат от наблюдението на неговата дейност.

Ето защо, в **понятието „предоставени от“** трябва да се включват също така *„личните данни, които са генерирани при наблюдението на дейностите на потребителите, като първични данни, обработени от интелигентно измервателно устройство или други видове свързани предмети, дневници на дейността, хронология на използването на уебсайтове или търсения“ (18).*

При упражнение на това право субектите могат да получат данните си в структуриран, широко използван и пригоден за машинно четене формат (напр. CSV, JSON, XML (19)).

Ако е технически осъществимо, **субектът може да поиска и прякото прехвърляне на данните от един администратор на друг**.

Оперативната съвместимост между администраторите се насърчава, но не е задължение по GDPR.

Право на преносимост *не се отнася* до обработването, необходимо за ***изпълнението на задача от обществен интерес*** или при упражняването на ***официални правомощия,*** които са предоставени на администратора.

То ***не може да бъде упражнено по начин, който да влияе неблагоприятно върху правата и свободите на други лица*** – например, ако предаването на данни от един администратор на данни към друг, би попречило на трети страни да упражняват техните права като субекти на данни съгласно GDPR (като право на информация, достъп и др. под.).

Например, при прехвърляне на **данните на контактите в уеб-базирана поща** от един администратор на друг по искане на субекта (когато това е възможно), получаващият **„нов“ администратор на данни не може да използва предадените данни** на трета страна за свои собствени цели, например за да предлага продукти и услуги на въпросните субекти на данни — трети страни.

За да се избегне неблагоприятното влияние върху правата и свободите на тези трети страни,
обработването на тези лични данни от другия администратор следва да е разрешено само доколкото данните се съхраняват под пълния контрол на потребителя, отправил искането, и се управляват единствено за лични или домакински нужди **(20)**.

- ***Право на ограничение на обработването*** също е **ново право**, въведено с GDPR. То се прилага при някоя от следните хипотези:

- при **оспорване точността на данните** – за срока, до който администраторът може да провери точността на данните;

- при **неправомерно обработване**, без субектът да желае изтриване, а вместо това изисква ограничаване на използването им;

- ако **данните са ненужни на администратора**, но субектът ги изисква за установяването, упражняването или защитата на правни претенции; или

- **при направено възражение срещу обработването** в очакване на проверка дали законните основания на администратора (обществен интерес, официални правомощия, законен (легитимен) интерес) имат преимущество пред интересите на субекта на данните.

Последиците от упражняването на това право са следните: **допустимо е само съхранение на данните, без друга форма на обработване**.

Всяко такова друго обработване може да се осъществи само със съгласие от субекта на данните.

Отделно субектът на данните трябва да бъде информиран от администратора преди отмяната на обработването.

Администраторите следва да внедрят такива технологични решения, които им позволяват да маркират съответните данни като „ограничени“, така че да се препятства последващото им обработване докато е упражнено разглежданото право.

- ***Права при автоматизирано вземане на решения вкл. профилиране –***профилирането се дефинира от GDPR като *„всяка форма на автоматизирано обработване на лични данни, изразяващо се в използването на лични данни за оценяване на определени лични аспекти, свързани с физическо лице, и по-конкретно за анализиране или прогнозиране на аспекти, отнасящи се до:*

- *изпълнението на професионалните задължения на това физическо лице,*
- *неговото икономическо състояние,*
- *здраве,*
- *лични предпочитания,*
- *интереси,*
- *надеждност,*
- *поведение,*
- *местоположение или*
- *движение*“.

Автоматизираното вземане на решения (***АВР***) не дефинирано изрично в GDPR, но видно от името му, то предполага вземането на решения чрез ИКТ, т.е. без човешка намеса (например, АВР ще е налице, ако камера за скорост автоматично налага глобата на дадено лице).

Според Работната група по чл. 29 има **два режима за профилирането** по GDPR:

- профилиране, при което **има човешка намеса на даден етап.** Тогава се прилагат общите правила и принципи на GDPR;

- **АВР,** включително профилиране, което се осъществява изцяло **без човешка намеса**.

Тъй като **вторият процес е по-рисков** поради отсъствието на човешкия фактор, GDPR въвежда по-строги правила при тази обработка. GDPR въвежда **принципна забрана за подобен вид обработване.**

Изключения от забраната са налице, ако са налице някои от посочените **три основания** (т.е. останалите основания за обработване по GDPR ***не*** се прилагат):

- ***изрично съгласие*** – то не е изрично дефинирано в GDPR. За да бъде съгласието „**изрично**“, то трябва да бъде манифестирано по още по-ясен, категоричен и недвусмислен начин от „обикновеното“ съгласие – напр. чрез *подписване на изявление*, *чрез попълване на електронна форма*, *чрез пращане на имейл*, *прикачване на сканиран документ с подписа на субекта на данните, чрез електронен подпи*с и други подобни (21);

- ***необходимост за сключването/ изпълнението на договор*** – обработването трябва да е необходимо за самия предмет на договора – напр. услуги Smart Home;

- ***разрешение от правото на ЕС***/държава членка – към момента **у нас няма изрични правила** в тази насока, Затова в бъдеще може да се очаква някакво на законодателната уредба.

Също така, **администраторите** трябва да прилагат и **подходящи гаранции за защита правата и интересите на субекта**, като:

- ***Право да изрази гледната си точка*** – съществува и по действащия режим;
- ***Право на човешка намеса*** - **ново право**, уредено с GDPR. То предполага намесата на човек, който има възможността да преразгледа решението, и да се ангажира по подходящ начин в преразглеждането на решението, т.е. не следва рутинно и механично решението на ИКТ;
- ***Право да оспори решението*** – пред човек, който да преразгледа решението на ИКТ.

GDPR ограничава възможността за обработване на чувствителни данни с цел АВР, включително профилиране (само при изрично съгласие или важен обществен интерес на основание правото на ЕС/ държава членка).

- ***Право на възражение.*** GDPR дава на субектите на данни и **правото на възражение**.

То позволява на субекта на данните, по всяко време и на основания, свързани с неговата конкретна ситуация, да възрази срещу обработване на лични данни, отнасящи се до него, което се основава на обществен интерес, официални правомощия или легитимен интерес, включително профилиране, базирано се на посочените основания. Администраторът прекратява обработването на личните данни, освен ако не докаже, че съществуват убедителни законови основания за обработването, които имат предимство пред интересите, правата и свободите на субекта на данни, или за установяването, упражняването или защитата на правни претенции.

Възражение срещу обработване за целите на директния маркетинг е ***абсолютно***, т.е. обработването на личните данни за тези цели се прекратява, а администраторът няма възможност да докаже съществуването на убедителни законови основания за обработването, които имат предимство пред интересите, правата и свободите на субекта на данни.

Субектът трябва да бъде изрично уведомен за това право най-късно в момента на първото осъществяване на контакт с него.

То му се представя по ясен начин и отделно от всяка друга информация. В контекста на използването на услугите на информационното общество субектът на данните може да упражнява правото си на възражение чрез автоматизирани средства, като се използват технически спецификации.

Заключение

Датата, от която GDPR ще започне да се прилага, наближава.

В контекста на българското европредседателство темата за GDPR все по-голяма популярност у нас. В същото време, доколкото евентуални нарушения на разпоредбите относно правните основания и правата на субектите на данни са от т.нар. „тежки“ нарушения, т.е. за тях се предвиждат най-високите максимални размери (20 милиона евро или 4% от световния годишен оборот), за администраторите е от първостепенно значение да повишат своята информираност по тези въпроси.

Компаниите следва да извършат подробни вътрешни „**инвентаризации**“ на процесите по обработване на лични данни, да идентифицират ***правните основания за основните си бизнес процеси*** и да обмислят **създаването на механизми и процедури за гарантиране и упражняване правата на субектите на данните**.

Само по този начин българският бизнес ще може да остане конкурентоспособен на всички останали европейски предприятия, които от години са посветили съществено внимание и инвестиции на защитата на личните данни.

1. Съгласно чл. 99, пар. 1 от GDPR, регламентът влиза в сила 20 дни след обнародването си, т.е. е регламентът е в сила от 25 май 2016 г.
2. Вж. примерно систематизиране на най-съществените нововъведения в GDPR в Захариев, М. Коментар на специалиста: Готов ли е бизнесът за GDPR?, URL: <http://computerworld.bg/51638_komentar_na_specialista_gotov_li_e_biznesat_za_gdpr> и <computerworld.bg/51639_komentar_na_specialista_gotov_li_e_biznesat_za_gdpr_chast_2> (04.02.2018 г.).
3. Чл. 8, пар. 1 и 2 от Хартата гласят:
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.*
4. Защитата на личните данни и новите европейски регулации. *// Научна конференция с международно участие „Облачните структури и защитата на информацията“, Сборник научни трудове.* Шумен, 2016, с. 67.
5. Александров, А. Защита на личните данни на работниците и служителите, ИК „Труд и право“, София, с. 47.
6. Guidelines on Consent under Regulation 2016/679 (project), p. 4.
7. Вж. в този смисъл и т. 5 от материала „Съгласието” според новия Общ регламент относно защитата на данните, достъпен на уебсайта на КЗЛД, URL: <https://www.cpdp.bg/?p=element&aid=1046> (04.02.2018 г.).
8. Работната група по чл. 29 е консултативен орган на ниво ЕС, създаден по силата на Директива 95/46 (актът на ЕС, уреждащ защитата на личните данни преди GDPR). Тя се състои от представители на надзорните органи на всяка една държава членка по защита на личните данни и даваща тълкувания на основни понятия и концепции, свързани с режима на защитата на личните данни, в т.ч. и с GDPR.
9. Повече за най-актуалното състояние на механизмите за трансфер на лични данни в трети държави (извън ЕС) вж. Кръстева, Д., Ракшиева, Св., Делото "Шремс": Ще бъдат ли забранени трансферите на данни от ЕС?, Капитал Daily, ноември 2017 г., URL<https://www.capital.bg/biznes/konsult/2017/11/02/3070186_deloto_shrems_shte_budat_li_zabraneni_transferite_na/?#comments> (05.02.2018 г.).
10. Guidelines on Consent under Regulation 2016/679 (project), p. 13-14.
11. Според т. 6.5. от ДЕСЕТ ПРАКТИЧЕСКИ СТЪПКИ ЗА ПРИЛАГАНЕ НА ОБЩИЯ РЕГЛАМЕНТ ЗА ЗАЩИТА НА ДАННИТЕ (актуализиран и допълнен вариант), публикуван на уебсайта на КЗЛД, съгласие за предоставяне на услуги на информационното общество следва да бъде дадено или разрешено от носещия родителска отговорност за детето, в случай че детето е **под 14 години (а не както по GDPRпод 16 години)**, URL: <https://www.cpdp.bg/?p=element&aid=1109> (05.02.2018 г.).
12. Guidelines on Consent under Regulation 2016/679 (project), p. 21.
13. Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, p. 41.
14. Ibid, p. 38-39.
15. Александров, А. Защита на личните данни на работниците и служителите, ИК „Труд и право“, София, с. 138-139.
16. Детайлен анализ за профилирането вж. Захариев, М. Организация и управление на автоматизираното профилиране в контекста на защитата на личните данни. Дисертация за присъждане на образователна и научна степен „доктор“. Защитена на 11.10.2017 г., София, УниБИТ, 269 с.
17. Насоки относно правото на преносимост на данните, с. 10-11.
18. Пак там, с. 11.
19. Пак там, с. 21.
20. Пак там , с. 13-14.
21. Guidelines on Consent under Regulation 2016/679 (project), p. 19.