

Сайтът използва "бисквитки", за да има възможност да предоставя проактивно най-полезната за вас информация.



Абонирай се сега

Данъци   Осигуряване   Счетоводство   Трудово право   Търговско право   СИДДО

## GDPR - ЗАДЪЛЖЕНИЯ НА ОБРАБОТВАЩИТЕ ЛИЧНИТЕ ДАННИ

КОМЕНТАРИ - ЗАЩИТА НА  
ЛИЧНИТЕ ДАННИ

### GDPR - задължения на обработващите личните данни

Десислава Кръстева, адвокат

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

Актуално към 07. 03. 2018 г.

2018 © tita.bg

### 1. Основни роли при обработването на личните данни

Всички права запазени. Условия за ползване.

Фигурите на администратора и на обработващия лични данни не са нови.

Въсъщност в Регламент 2016/679 (GDPR/ Регламента) е запазена концепцията за ролите:

- на администратор и

- **на обработващ лични данни,**

позната от Директива 95/46/EО и действащия Закон за защита на личните данни (ЗЗЛД).

**Администратор** (data controller) съгласно Регламент (ЕС) 2016/679 е **физическо или юридическо лице, публичен орган, агенция или друга структура**, която **сама** или **съвместно** с други **определя**:

- **целите и**
- **средствата** за обработването на лични данни.

В допълнение, когато целите и средствата за това обработване се определят от правото на Съюза или правото на държава членка, администраторът или специалните критерии за неговото определяне могат да бъдат установени в правото на Съюза или в правото на държава членка (чл. 4, т. 7).

**Администраторът** може да **обработва личните данни**:

- самостоятелно или
- чрез възлагане на обработващ/и лични данни.

От своя страна, **обработващ** (data processor) (1) е **физическо или юридическо лице, публичен орган, агенция или друга структура**, която **обработва** лични данни **от името на администратора** (чл. 4, т. 8).

Макар, както отбелязахме, фигурите на администратора и обработващия лични данни да не са нови, в съвременния високотехнологичен свят и при появата на все по-комплексни дейности по обработване на данни **преценката кой е администратор и кой е обработващ личните данни** става **все по-трудна** и нееднозначна. Обично в рамките на едно единствено правоотношение (като изпълнението на един единствен договор за услуги) едно лице може да съвместява и извършва едновременно дейности и като администратор, и като обработващ лични данни.

Определянето на ролите на лицата, участващи в обработването на личните данни, обаче, е предпоставка за сълюдяване на изискванията на Регламента и за гарантиране правата на субектите на данни.

В зависимост от това **каква роля има едно лице при обработването на лични данни** за него съгласно Регламента възникват **различни задължения**.

Поради това, преди да бъдат коментирани конкретните задължения на обработващия лични данни, е

**необходимо да бъде уточнение в кои случаи едно лице**, което обработва лични данни **действа като и съставлява обработващ лични данни** по смисъла на Регламента.

**Администратор е лицето**, което **само или съвместно с други определя целите и средствата за обработването на личните данни**, а **обработващият лични данни е лице**, което **обработва лични данни от името на администратора**.

Съществува **и още една фигура**, която участва **в обработването на лични данни - лицата, действащи под ръководството**:

- на администратора или
- на обработващия.

Регламентът предвижда, че:

- **обработващият** и
- **всяко лице, действащо под ръководството на администратора или на обработващия**, което има достъп до личните данни,

обработва тези данни **само по указание на администратора**, освен ако обработването не се изисква от правото на Съюза или правото на държава членка.

Наличието на специален и самостоятелен текст за „обработването под ръководството на администратора или на обработващия лични данни“ сочи, че Регламентът ясно разграничава лицата, действащи под ръководството на администратора или на обработващия от самия администратор и обработващ.

**Лицата, действащи под ръководството на администратора или на обработващия не са нито администратори, нито обработващи личните данни.**

Иначе Регламентът би използвал официалните термини „администратор“ или „обработващ личните данни“.

**„Лица, действащи под ръководството на администратора или на обработващия“** са всъщност **служителите на администратора или на обработващия**, които под **тяхно ръководство** извършват **дейности по обработване на лични данни**.

Поради това е изключително **важно да се подчертава**, че разгледаните по-долу **задължения на**

**обработващите лични данни не се отнасят** до и не се прилагат към **служителите** (назначени на трудов договор) на администратора

**Извършените съобразно указанията на техния работодател** – администратора, **действия** следва да се считат за **действия на самия администратор**.

## **2. Задължения на обработващия лични данни**

Сред **ключовите новости**, които въвежда Регламентът спрямо Директива 95/46/EО са **задълженията на обработващите лични данни лица**.

По Директивата и съответно по действащия ЗЗЛД единственото задължено лице беше администратора.

**Регламентът**, обаче, **възлага директно задължения и към обработващите лични данни**.

**Обработващите лични данни**, също така, **вече ще могат и да бъдат санкционирани** директно от надзорния орган **за нарушения на изискванията на Регламента**.

- **Да не се отклонява от или да действа извън указанията на администратора**

Основната характеристика на ролята на администратора е, че той определя целите и средствата за обработването на личните данни.

Именно поради това чл. 28, ал. 10 от GDPR предвижда, че ако **обработващ лични данни** наруши Регламента, **определяйки целите и средствата на обработването**, обработващият личните данни **се счита за администратор** по отношение на това обработване.

То тук следва и **първото и ключово задължение** на обработващия лични данни, а именно **да не се отклонява от или да не действа извън указанията/** възлагането на администратора, **да не определя нови цели и средства за обработването** на данните и **да не изземва компетенциите** на администратора.

Подобен тип действия сами по себе си биха могли да съставляват **нарушение на изискванията на Регламента**.

Вземането на **ключовите решения относно обработването на личните данни е изцяло дейност и отговорност на администратора.**

С вземането на тези решения всъщност администраторът поема отговорността за законосъобразността им обработване и за него възникват задълженията да осигури и гарантира защитата на правата на субектите на данни. За разлика от администратора обработващият действа от името на администратора, т. е. по възлагане, съгласно наредданията на администратора и взетите от него решения.

**Функциите на обработващия** и извършваните от него дейности са **подчинени на решенията, взети от администратора** и адресирани като нареддания към обработващия.

**Типични примери**, при които има **възлагане на дейности по обработване на лични данни** от администратор към обработващ лични данни са:

- възлагането **дейности по изготвяне на ведомости за заплати** към **външна счетоводна къща**,
- използването на **различни облачни услуги и платформи**,
- използване **на хостинг услуги**,
- на колокейшън услуги,
- на **външни услуги за IT поддръжка**,
- използване на **външен кол център** за обслужване на клиенти и др. под.

В случаите, когато **обработващият вземе решение** относно целите или средствата за обработване на личните данни, той се **отклонява от наредданията на администратора** по един от следните начини:

1. Извършва дейности по обработване, които не са му били наредени/указани от администратора – това са **действия без необходимите нареддания** от администратора; или
2. Извършва дейности по обработване, които нарушават наредданията, дадени му от администратора – това са **действия на директно неизпълнение на наредданията** на администратора.

**Всяко отклонение на обработващия от наредданията на администратора пречи на администратора да осигури законосъобразността на обработването и да гарантира защитата на правата на засегнатите субекти.**

**Ключовите въпроси** относно обработването на личните данни, които се решават **само и единствено от**

**администратора** и съответно по отношение на които обработващият няма право да се намесва са относно:

1. **целите** на обработването;
2. **средствата**, с които се обработват данните;
3. **данные**, които се обработват;
4. **сроковете**, в които се обработват;
5. **место**, където се обработват; и
6. **лицата, които обработват данные**.

Всеки един от тези аспекти е ключов, за да може администраторът да изпълни задължението си по чл. 24, ал. 1 от Регламент (ЕС) 2016/679 „да гарантира и да е в състояние да докаже, че обработването се извършва в съответствие с“ Регламента.

Да вземем на **пример** един доставчик на услуга „Кабелна телевизия“ (**администратор**), който възлага на външна организация – call център (**обработващ**), **дейности по обслужване на неговите абонати**, свързани:

- с приемане и обработване на **обажданията на абонатите за възникнали аварии** и проблеми с услугата, както и
- с извършване на **периодични маркетингови дейности** по предлагане на неговите нови или промоционални услуги.

За целите на изпълнение на възложените му задачи call центърът **има достъп до данни за абонатите на доставчика**. Изискванията към услугите на кол центъра са уредени писмено в договора му с доставчика. **Изрично е предвидено**, че **call центърът** ще обработва **данные на абонатите единственно** за целите по предоставяне на **възложените му с договора услуги/ задачи**.

Независимо от това, **call центърът** се възползва от достъпа си до данните за контакт на абонатите и започва да ги **прозвънява**, за да им предложи **продукти, предлагани от друг негов клиент** - домакински уреди.

Така **call центърът се отклонява** от възложеното му от администратора (доставчика), нарушува указанията му и действа като администратор по отношение на дейностите, свързани с тези прозвънявания, тъй като е взел решенията относно:

- **целите** (определил е **нова цел** – директен маркетинг на чужди стоки; **категориите данни** – имена и

телефонен номер на абонатите) и

- **средствата** – извършване на справки в базите данни, до които му е даден достъп и телефонни обаждания.

- **Писмено уреждане на отношенията с администратора**

**Отношенията** между:

- обработващия и
- администратора

относно обработването на личните данни трябва да бъдат уредени с **писмен договор** или с **друг писмен правен акт** съгласно правото на Съюза или правото на държава членка, който е задължителен за обработващия лични данни спрямо администратора.

Особено важно е да се подчертава, че **не е достатъчно** да има **писмен договор между администратора и обработващия лични данни**.

**Този договор** трябва **задължително по конкретен начин да адресира и урежда възложените дейности по обработване на лични данни**.

Нещо повече Регламентът въвежда **изисквания относно минималното съдържание на такъв договор**.

Този договор трябва да урежда и указва **задължително**:

1. **предмета** на възложеното обработване на лични данни;
2. **срока** на действие на обработването;
3. **естеството** на възложеното обработване;
4. **целта**, за които се възлага обработването;
5. **категориите лични данни и категориите субекти на данни**, обект на обработването; и
6. **задълженията и правата на администратора и на обработващия** по отношение на възложеното обработване.

**Липсата на такъв договор** в отношенията между администратора и обработващия лични данни сама по себе си би означавала вече, че **обработващият лични данни нарушива изискванията на Регламента**.

В този договор или друг правен акт трябва **задължително** да са предвидени **определенi задължения за**

**обработващия лични данни**, които по своята същност се припокриват с основните му задължения съгласно Регламента.

Макар обработващите лични данни да действат по възлагане от администратора, **по отношение на стандартизиирани услуги**, изискващи обработването на лични данни, по-подходящ (а в редица случаи и единствен възможен) подход е **предложението** за обхвата на **конкретните задължения** и ангажименти **относно мерки за защита на данните и начин за обработването им**:

- да бъдат **предлагани от обработващия лични данни** и
- единствено **да бъдат потвърждавани като възлагане от администратора**.

В противен случай обработващите лични данни могат да се озоват в ситуация на пълна невъзможност да изпълняват задълженията си към всички администратори (всички свои клиенти).

**Например**, една **счетоводна къща**, която получава конкретни и различни указания за счетоводните програми и системи, които използва от всеки свой клиент (администратор). По този начин може да се създаде ситуация, при която служителите на счетоводната къща е необходимо да използват едновременно над 50 и дори повече различни програми и системи.

- **Обработка личните данни само по документирано нарејдане на администратора**

В продължение на **принципа за отчетност**, въведен с чл. 5 от Регламента, не само договорните отношения между администратора и обработващия лични данни е необходимо да бъдат писмено уредени, но и **всички нарејдания и указания на администратора към обработващия лични данни** относно възложеното му обработване трябва да са **документирани, т.е. писмени, проследими**.

Регламентът **забранява на обработващия** лични данни **да изпълнява указания** на администратора, които **не са документирани**.

Всяко такова обработване би било извършено от обработващия лични данни на негов риск и отговорност, тъй като, както бе посочено по-горе, действията без или извън указанията на администратора могат да доведат до това обработващият да бъде третиран като администратор по отношение на конкретното действие по обработване.

**Единственото изключение** от това задължение е в случай, че правото на Съюза или приложимото право

на държава членка изисква обработващият лични данни да извърши обработване на личните данни, което е извън предвиденото в договора му с администратора.

Обичайно това са **задължения за предоставяне на данни на друго лице** и по-конкретна **на определени компетентни държавни органи**.

В тези случаи обработващият лични данни е длъжен да информира администратора за съществуването на това негово задължение, освен ако и това не му е забранено от правото на Съюза или от приложимото право на държава членка (най-често такъв тип задължения се откриват в контекста на задължения за оказване на съдействие при разследване на престъпления, защита на националната сигурност, данъчен контрол и др. под.).

- **Ангажимент за поверителност**

**Обработващият** е задължен да **гарантира**, че **лицата, оправомощени да обработват личните данни** (лицата, действащи под неговия контрол), са поели **ангажимент за поверителност** или са задължени по закон да спазват поверителност.

- **Технически и организационни мерки за осигуряване сигурността на личните данни**

**Обработващият** лични данни е необходимо да прилагане **подходящи технически и организационни мерки** по такъв начин, че обработването да протича в съответствие с изискванията на Регламента и да осигурява сигурността на личните данни и защитата на правата на субектите на данни.

- **Забрана за превъзлагане на дейности по обработване**

**Едно от най-важните задължения** на обработващите личните данни лица е **забраната да превъзлагат** каквито и да е дейности по обработване и да включват други обработващи лични данни лица в обработването, което им е възложено от администратора.

За да бъде преодоляна тази забрана е необходимо обработващият лични данни да е получил **предварително конкретно или общо писмено разрешение от администратора**.

Обработващият **не може да включва друг обработващ данни** такова без предварителното конкретно или общо писмено разрешение на администратора.

В допълнение, в случай на общо писмено разрешение, обработващият данни винаги **информира администратора за всякакви планирани промени за включване или замяна на други лица, обработващи данни, като** по този начин **дава възможност на администратора да оспори тези промени.**

Когато обработващ лични данни включва друг обработващ лични данни за извършването на дейности по обработване от името на администратора **на това друго лице е необходимо да се наложат** (с договор или друг правен акт) **същите задължения** за защита на данните като задълженията, предвидени в отношенията между администратора и обработващия лични данни.

- **Подпомага администратора**

Обработващият лични данни е задължен да подпомага администратора, за да се гарантира изпълнението на изискванията:

- за осигуряване на сигурност на личните данни,
- за уведомяване при нарушения в сигурността на данните и
- за извършването на оценка на въздействието и
- за провеждането на предварителни консултации с надзорния орган (КЗЛД).

**Конкретният обхват** и същност на това подпомагане ще зависи и ще е **пряко свързано**:

- **с естеството** на конкретното обработване и
- **с информацията**, до която му е осигурен достъп.

**Особен акцент** следва тук да се постави върху това, че **задълженията за уведомяванена надзорния органи и на засегнатите субекти** при нарушение на сигурността на данните **възникват за администратора**, дори и когато самото нарушение е настъпило по отношения на данните, обработвани от обработващия.

**Администраторът е длъжен да уведоми КЗЛД** и след преценка на риска за правата и свободите на субектите на данни евентуално да информира и тях.

Що се отнася до обработващия лични данни, то неговото задължение в ситуация на нарушение на сигурността е **да информира незабавно администратора и да му предостави цялата необходима**

**информация, с която разполага,** така че да може администраторът да изпълни в срок и надлежно своите задължения за уведомяване.

Наред с посоченото по-горе дължимо съдействие при нарушения на сигурността подпомага администратора, доколкото е възможно, чрез подходящи технически и организационни мерки, обработващият е задължен и **да подпомага администратора при изпълнението на задължението му да отговаря на искания за упражняване на правата на субектите на данни.**

В какво точно ще се състои това съдействие ще зависи от конкретното естество на възложеното му обработване на лични данни.

Подобно на **задълженията за уведомяване при нарушение на сигурността на данните, задълженията, свързани с осигуряването на възможности за упражняване правата на субектите на данни** и съответно тяхното съблюдаване, са адресирани **към администратора**.

Субектите могат да упражняват своите права спрямо администратора.

Посоченото по-горе задължение за съдействие на администратора включва и **изискване** към обработващия лични данни **да осигурява достъп на администратора до цялата информация**, необходима за доказване на изпълнението на задълженията му като обработващи, и да позволява и **да допринася за извършването на одити**, включително проверки, **от страна на администратора** или на друг одитор, оправомощен от администратора.

- **Заличава или връща личните данни**

По избор на администратора обработващия лични данни е задължен да заличи или върне на администратора всички лични данни след приключване на услугите по обработване, както и да заличи съществуващите копия, освен ако правото на Съюза или правото на държава членка не изисква тяхното съхранение.

- **Водене на регистри по чл. 30, ал. 2 от GDPR**

Разгледаните до тук **задължения на обработващия личните данни** са функция на **подчинената му роля спрямо администратора**.

Това са задължения в контекста на конкретни възлагания на обработване на лични данни, в контекста на

отношенията на обработващия лични данни с конкретни администратор.

Извън това, обаче, **GDPR въвежда** и някои **самостоятелни задължения на обработващия**.

Преди всичко това е задължението на обработващите лични данни да поддържат **регистри на всички категории дейности по обработване**, извършвани от името на администратор.

Съдържанието на тези регистри е **различно от регистрите по чл. 30, ал. 1 от GDPR**, които трябва да бъдат **водени от администраторите**.

То е по-съкратено и е съобразено със специфичната роля на обработващия, а именно – ролята му на лице, което действа от името на администраторите.

**Регистърът по чл. 30, воден от обработващия** трябва да съдържа **най-малко**:

- името и координатите за връзка на обработващия или обработващите лични данни и на длъжностното лице по защита на данните;
- името и координатите на всеки администратор, от чието име действа обработващият лични данни и — когато това е приложимо —на представителя на администратора или обработващия лични данни и на длъжностното лице по защита на данните;
- категориите обработване, извършвано от името на всеки администратор;
- предаването на лични данни на трета държава или международна организация (ако има такова) и документация за приложените подходящи гаранции за осигуряването на адекватно ниво на защита на данните; и
- **описание на организационните и техническите мерки за сигурност на данните**, когато е възможно.

#### • **Длъжностно лице по защита на данните**

Подобно на администраторите **и за обработващите личните данни** лица Регламентът въвежда **задължение за определяне на длъжностно лице по защита на данните**, ако характерът на извършваните дейности по обработване налага назначаването на такова (съобразно критериите по чл. 37, ал. 1).

По-конкретно **за обработващият лични данни** може да възникне задължение за **назначаване на длъжностно лице по защита на данните**, ако:

- е **публичен орган** или структура; или
- основните дейности по обработване, които извършва, се състоят в операции по обработване, които поради своето естество, обхват и/или цели изискват **редовно и систематично мащабно наблюдение на субектите на данни**; или
- основните дейности по обработване, които извършва, се състоят в **мащабно обработване на специалните категории данни** съгласно и на лични данни, свързани с присъди и нарушения.

На практика, **в определени случаи за обработващия лични данни** може да е налице **задължение за назначаване на длъжностно лице по защита на данните**, макар за администратора, възложил му съответното обработване, да не е налице такова задължение.

**Пример** за това е ситуация, при която дребен търговец използва за обработването на личните данни на своите служители информационна система, разположена върху „облачна“ платформа.

В този случай мащаба на извършваното от дребния търговец като работодател обработване на данните за малобройния му персонал не поражда необходимостта от назначаване на длъжностно лице по защита на личните данни.

Същевременно, обаче, ако доставчикът на тази услуга (обработващ), базирана върху облачни технологии, предоставя такава услуга на множество други дребни търговци в целия ЕС, то той би извършвал обработване, което по своето естество, системност и мащаби може да попадне в критериите по чл. 37 и да бъде задължен да си назначи длъжностно лице по защита на личните данни.

#### • Санкции

Размерите на санкциите, които могат да бъдат налагани на обработващите лични данни лица при нарушения на GDPR, са **същите като** тези предназначени **за администратори**.

### 3. Заключение

Направеният до тук очерк на **задълженията на обработващите лични данни** лица сочат, че макар и нововъведени с GDPR, те са **съществени**.

За да съблюдават изискванията на Регламента и за да си гарантират в максимална степен защитата на техните права и интереси обработващите личните данни ще е необходимо преди всичко:

- 1. Стриктно да изискват от администраторите писмено, надлежно и детайлно уреждане на възлаганите им дейности по обработване на лични данни. По отношение на заварените отношения – да преуредят по надлежен начин договорите си със своите възложители/клиенти;**
- 2. Да обработват личните данни съобразно документираните наредждания на администратора;**
- 3. Да оказват адекватно и съответстващо на възложените им дейности съдействие на администратора** при спазване на неговите задължения; и
- 4. Да водят регистри** за извършваните от тях дейности по обработване на лични данни.