АСОЦИАЦИЯ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Защо е важно кой кой е според GDPR?

На пръв прочит, функциите на администратор и обработващ изглеждат почти еднакви, но всъщност между тях има фундаментални разлики и ако не се държи сметка за техните самостоятелни роли и функции в процеса на обработване би могло да се стигне до значими негативни последици на практика. Така например при пробив в сигурността, в резултат на които има изтичане или кражба на лични данни, както администраторът, така обработващият и Надзорния орган, ще бъдат пряко заинтересовани да се установи кой каква отговорност носи.

Съгласно Регламента:

Администратор

чл.4, ал. 7 от Регламента сочи, че „администратор“ означава 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; 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;

Обработващ

Легална дефиниция за обработващ е дадена в чл.4, ал.8 от Регламента според, която „обработващ лични данни“ означава физическо или юридическо лице, публичен орган, агенция или друга структура, която обработва лични данни **от името на администратора**;

Независимо от това, на пръв поглед ясно разграничение, много често, когато дадена организация трябва сама да се определи като администратор или обработващ данни тя среща сериозни затруднения. В практиката често се случва, Компания погрешно да счита себе си за обработващ и поради това да поддържа напр. Регистър по чл.30, ал.2, вместо този по чл.30, ал.1 от Регламента, който следва да се поддържа от администратора на лични данни. По нататък в процеса на събиране и обработване на личните данни е много вероятно същата Компания поради това грешно самоопределяне да не спази и други задължения, които има поради качеството си на администратор съгласно Регламента.

Как да определим кой е администратор и кой е обработващ лични данни?

Отличителният белег на администратора на лични данни е, че той определя целите и средствата на обработването, респективно упражнява цялостен контрол на процеса по обработване на данните.

Тук е важно да се направи едно уточнение – възможно е да съществува повече от един администратор – напр. при хипотезата за съвместни администратори, регламентирана в чл.26 от Регламента. Според текста на цитираната разпоредба, двама или повече администратори, които „съвместно определят целите и средствата на обработването“ са съвместни администратори.

Администратор на лични данни ли сте?

За да може да се определите като администратор лични данни, най-напред е нужно да си отговорите на следните въпроси:

- Събирате ли лични данни и ако да - извършвате ли тази дейност на легално основание?
- Определяте ли какви лични данни ще събирате, респективно техните категории?
- Определяте ли целта за която събирате личните данни, респективно целта за която ще ги използвате?
- Определяте ли категориите субекти, чиито лични данни събирате?
- Определяте ли дали в последствие ще споделяте събраната информация и с кого?
- Определяте ли колко дълго ще съхранявате събраните от Вас лични данни както и имате ли възможност да направите изменение?

Ако сте дали положителен отговор на всички изброени въпроси, то Вие без съмнение сте администратор на лични данни, т.к. само като такъв бихте могли да взимате горните решения.

Разпределяне на ролите още от самото начало

Важно е организациите, които участват в дейности обработване на лични данни да установяват своите отговорности, респективно задълженията си още на най-ранен етап – преди процеса по обработка на данните да е започнал. В този смисъл е и текстът на чл.28 от новия Регламент (ЕС) 2016/679. Така, следвайки предписанията на цитираната разпоредба, страните трябва в изброената по-долу последователност да предприемат следните стъпки :

1. **избор на обработващ**, който предоставя *„достатъчни гаранции за прилагането на подходящи технически и организационни мерки“*, така че обработването да протича в съответствие с изискванията на Регламента и да осигурява защита на правата на субектите на данни.

Преди да избере обработващ лични данни, администраторът трябва да се убеди, че той предоставя всички възможни и необходими гаранции за прилагане на разпоредбите на приложимото законодателство и е в състояние да ги докаже. За тази цел е необходимо да се премине през процедура за избор на обработващ. Изборът се прави чрез извършване на т.нар. оценка на обработващия, която трябва да даде информация относно следните факти: подходящи ли са прилаганите от обработващия технически и организационни мерки и средства за защита на личните данни, включително адекватни ли са мерките за сигурност и защита на личните данни. Също така е възможно, в процеса на оценка може да се изиска и извърши преглед на неговите Вътрешни правила и политики по отношение на защита на данните или да се установи има внедрени признати международни сертификати за управление на качеството в неговата Организация и т.н.

2. **сключване на договор, между администратор и обработващ**, който следва да е в писмен вид и да е наличен и в електронен вариант и да включва задължителното съдържание съгласно чл.28, пар.3 от Регламента.

След като администраторът избере този обработващ, който според него предоставя „достатъчни гаранции за прилагането на подходящи технически и организационни мерки по такъв начин, че обработването да протича в съответствие с изискванията на Регламента и да осигурява защита на правата на субектите на данни“, следва между тях да се сключи писмен договор. В договора страните следва да определят всички въпроси, свързани с обработването – предмет, срок, действие, цел на обработването, категориите субекти, вид на обработваните данни, подходящите технически и организационни мерки, които ще се използват от обработващия, като гарант за защита на личните данни и др. изчерпателно посочени реквизити в чл.28, ал.3 от Регламента. Тук е важно да се спомене, че ако обработващия се отклони, и не спази договора като сам започне да определя целите и средствата на обработването, той самият ще се счита за администратор по отношение на това обработване.

Обработващ на лични данни за друг администратор

След като изяснихме кои решения се взимат от администратора, по-долу, ще се фокусираме на въпросите, който са от компетенциите на обработващия лични данни.

При изпълнение на функциите си, обработващия съобразява следните обстоятелства:

- да обработва личните данни само по документирано нареждане на администратора, включително що се отнася до предаването на лични данни на трета държава или международна организация, освен когато е длъжен да направи това по силата на правото на Съюза или правото на държава членка, което се прилага спрямо него като в този случай го уведоми за това предварително;
- да действа под ръководството и по указание на администратора при обработване на данните;
- да не включва други обработващи без предварителното конкретно или общо писмено разрешение на администратора;
- да прецени какви „подходящи“ технически и организационни мерки, ще използва, за да обезпечи сигурността на обработваните от него данни;
- да избере как ще съхранява обработваните лични данни;
- да гарантира, че лицата, оправомощени да обработват личните данни, са поели ангажимент за поверителност;
- да подпомогне администратора да отговори на искания за упражняване на предвидените в глава III права на субектите на данни;
- да осигури достъп на администратора до цялата информация, необходима за доказване на изпълнението на задълженията си;
- да уведоми незабавно администратора, ако според него дадено нареждане нарушава Регламента или други разпоредби на Съюза или на държавите членки относно защитата на данни;
- да заличи или върне на администратора всички лични данни след приключване на услугите по обработване.

Тези изброявания не бива да се считат за изчерпателни по отношение разликите между администратор и обработващ, а следва да илюстрират различията по между им. Така, обработващия лични данни има свободата да избира техническите и организационни мерки, които ще прилага, така че те да са „подходящи“ и да осигуряват „достатъчни гаранции“, като

същевременно не може да вземе нито едно от основните решения напр. какви ще бъдат личните данни, които ще се обработват, с каква цел ще се обработват и т.н., тъй като такива решения могат да се взимат само от администратора.

Обработващите лични данни също са администратори

Обработващите лични данни за други администратори също имат категория лични данни за която се явяват администратор – напр. счетоводна къща е администратор на лични данни по отношение на данните, които събира и обработва за своите служители и контрагенти и едновременно с това обработващ лични данни, по отношение на данните за служители на свой клиент, които обработва с цел изплащане на работни заплати.

От друга страна обстоятелството, че една организация сключва договор или използва друга организация за предоставяне на дадена услуга не означава непременно, че другата организация е в позицията на обработващ за първата лични данни. Дали дадена организация е администратор или обработващ лични данни зависи на първо място дали за целта на ползваната услуга/сключен договор се обработват лични данни, ролята и отговорност във връзка с обработката на всяка една организация.

Настоящата статия не представлява правен съвет. Тя съдържа мнение/коментар на нашите експерти и е само с цел подпомагане на компаниите при спазване изискванията на Регламент (ЕС)2016/679.