

Общият регламент за защита на данните (GDPR) предвижда тежки санкции при нарушаване на правилата за обработване на лични данни. Тези правила обаче се различават според това каква функция има едно лице при обработването на лични данни – дали определя целите и средствата за тази дейност или само ги изпълнява. Затова трябва да бъде направено разграничение между понятията администратор и обработващ на лични данни, съответно какви са техните задължения при извършване на обработването.

За целите на GDPR, обработване на лични данни включва всички процеси по събиране, съхраняване и въобще използване на информация, която се отнася до или може да бъде свързана с конкретно физическо лице. Така например обработване на лични данни представлява предоставянето на облачни услуги, когато клиентът съхранява лични данни в рамките на предоставеното му пространство на облака. В този случай доставчикът на услуги обичайно не използва тези лични данни, за да предоставя услугата, но би могъл да има достъп до тях, а и има задължение да следи за сигурността на сървърите, където се намират данните. Следващата особеност е, че личните данни не винаги е лесно да бъдат идентифицирани като такива – имена, данни за документи за самоличност и т.н. винаги попадат в тази категория, но има други категории данни, които отново могат да бъдат свързани с дадено лице при условие че бъдат комбинирани с други данни. Така например данните за местонахождението на един автомобил, събрани с информацията за собственика или водача му, могат да разкрият настоящото местонахождение на лицето, неговия адрес или бизнес отношения. Затова при преценка дали се обработват лични данни винаги трябва да се изяснява въпросът дали допълнителни данни, които може дори да не са достъпни в момента, биха позволили дадена информация да се свърже с конкретно физическо лице.

Преди започване на каквато и да е операция с лични данни, съгласно даденото по-горе определение, всяко лице трябва да прецени каква е неговата роля при обработването на данните, за да изясни своите задължения и отговорности в тази връзка. Най-важната роля и респективно най-голямата отговорност е за администратора на лични данни – това е лицето, което определя целите и средствата за обработване на личните данни. Обработващият на лични данни, за сметка на това, е лицето, на което са възложени отделни операции по съхраняване, пренос, сортиране и

т.н. на лични данни. Основният характерен белег на обработващия на лични данни е, че той не определя целите на обработването, т.е. не решава какво следва да се случи с личните данни. Тези цели се задават от администратора, като лицето – обработващ може да има известна свобода при избора на средства за постигането им, но тези средства следва да се съгласуват с администратора, който е възложил обработването. В разглеждания пример с предоставянето на облачни услуги, клиентът е администратор – той е събрал за определена от него цел дадени лични данни, като е възложил на доставчика на услуги да ги съхранява и да предоставя достъп до тях при определени условия. В този случай доставчикът на услуги е обработващ на лични данни, докато действа в рамките на възложеното му, като би станал администратор, ако например използва събраните от клиента лични данни за собствени цели – за да разпространява рекламни съобщения и др.

Ролите на администратор и обработващ на лични данни са различни за всяка отделна операция по обработване на лични данни – едно и също лице обичайно действа ту като администратор, ту като обработващ в рамките на един и същи ден, а понякога дори и по отношение на едни и същи данни. В разглеждания пример доставчикът на услуги е обработващ на лични данни по отношение на информацията, която клиентът му е възложил да съхранява, но е администратор по отношение на данните на самия клиент (име, представители и т.н.), които обработва за целите на изпълнение на договора за облачни услуги.

Във връзка с разграничението между администратор и обработващ на лични данни следва да бъдат направени две важни бележки. На първо място, администратор или обработващ могат да бъдат както физически, така и юридически лица. Това обаче не означава, че служителите на администратора са обработващи – понятията администратор и обработващ предполагат известна самостоятелност, известна свобода при вземането на решение по отношение на обработването на данни. Така например администратор ще е дружеството, което ползва данните, а не неговият управител, но физическо лице ще бъде администратор, ако това лице осъществява самостоятелна дейност, за целите на която обработва данните. Същото е в сила при обработващите – физическо лице, предоставящо конкретна услуга в рамките на дейност на свободна практика може да е обработващ, но не и служителите на дружество, което предоставя същите услуги за своя сметка. Втората бележка е по

отношение на възможността две или повече лица да са съвместни администратори. Това е сложна ситуация, при която тези лица съвместно вземат решенията относно целите и средствата на обработването. Приема се, че две или повече лица са съвместни администратори само ако не биха могли да извършват дадено обработване самостоятелно, а само заедно.

Администраторът на лични данни е лицето, което има най-голям обем задължения съгласно GDPR. Той трябва да гарантира спазването на принципите на законност, прозрачност, отчетност и т.н.; да предостави съответна информация на лицата, за които се отнасят данните; да гарантира правата да се коригират неверни данни, да се ограничи обработването или изцяло да се преустанови и т.н. Администраторът носи отговорност пред лицата, чиито данни обработва, включително и за дейността на обработващите, които е избрал за изпълнение на отделни операции. Затова администраторът има задължение винаги да урежда отношенията с обработващите с договор или по друг задължителен начин, като GDPR предвижда редица въпроси, които задължително трябва да бъдат уговорени.

Обработващият носи по-ограничена отговорност, тъй като не определя целите и средствата за обработване на данните – за тези решения отговаря изцяло администраторът. Обработващият обаче трябва задължително да осигури прозрачност на извършваните от него операции, включително какви технически и организационни мерки за защитата на данните прилага, дали ангажира други обработващи, както и да предостави възможност на администратора да го проверява. Освен това обработващият има задължението да изпълнява указанията на администратора по отношение на данните – кога следва да бъдат коригирани или изтрети, дали следва да се спре работата с тях във връзка с определени операции и т.н. Допълнителен ангажимент на обработващия е да следи своите служители и да гарантира, че те спазват правилата за защита на личните данни. Обработващият носи и отговорност пред администратора за изпълнението на задълженията си съгласно сключения договор, а в определени случаи може да отговаря и директно пред лицата, чиито данни обработва.

Изложеното по-горе обхваща само основните задължения при работа с информация като администратор и обработващ на лични данни, като тези задължения варират в голяма степен според конкретната операция по обработване и не могат да бъдат

разгледани в пълен обем. Може да бъдат дадени обаче няколко принципни препоръки за избягване на най-честите проблеми в практиката. На първо място, сключването на договор за разпределяне на отговорностите по обработването на лични данни е задължително, като това може да стане и чрез общи условия, предложени от администратора или обработващия. Също така винаги трябва да бъдат идентифицирани правилно обработващите, които участват в дадена операция, като тук трябва да бъдат включени всички лица, които имат достъп дори до част от данните. В използвания пример ако доставчикът на облачни услуги използва външни услуги за поддръжка на сървърите си, той трябва да уведоми клиента си за това, като посочи кое лице има физически достъп до носителите на данните и би могло волно или неволно да доведе до изтриването им. От обратна страна, обработващият трябва да посочва ясно и точно какви мерки за сигурност прилага и те трябва да бъдат одобрени от администратора. В противен случай всяка от страните ще носи отговорност при нарушаване сигурността на данните.

Независимо от изложеното, и всеки администратор и обработващ на лични данни носят отговорност за допуснати нарушения на регламента пред компетентния национален орган съгласно GDPR. В България това е Комисията за защита на личните данни,, като отговорността им може да бъде ангажирана и директно по съдебен ред.