Регламент (ЕС) 2016/679 (GDPR) – общ анализ от гледна точка на счетоводителя/ТРЗ-служителя

Термини

„Лични данни“ означава всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано („субект на данни“). Физическо лице, което може да бъде идентифицирано, е 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 лице.

„Обработване“ означава всяка операция или съвкупност от операции, извършвана с лични данни или набор от лични данни посредством автоматични или други средства като събиране, записване, организиране, структуриране, съхранение, адаптиране или промяна, извличане, консултиране, употреба, разкриване чрез предаване, разпространяване или друг начин, по който се получава достъп до данните, подреждане или комбиниране, ограничаване, изтриване или унищожаване.

„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 ЕС или правото на държава-членка,

администраторът или специалните критерии за неговото определяне могат да бъдат установени в правото на ЕС или в правото на държавата-членка.

„Оператор“ или още „обработващ лични данни“ означава физическо или юридическо лице, публичен орган, агенция или друга структура, която обработва лични данни от името на администратора.

„Получател“ означава физическо или юридическо лице, публичен орган, агенция или друга структура, пред която се разкриват лични данни, независимо дали става въпрос за трета страна или не. Същевременно публичните органи, които могат да получават лични данни в рамките на конкретно разследване в съответствие с правото на ЕС или правото на държава-членка, не се считат „получатели“; обработването на тези данни от посочените публични органи отговаря на приложимите правила за защита на данните според целите на обработването

„Трета страна“ означава физическо или юридическо лице, публичен орган, агенция или друг орган, различен от субекта на данните, администратора, обработващия лични данни и лицата, които под прякото ръководство на администратора или на обработващия лични данни разполагат с право да обработват личните данни.

„Съгласие на субекта на данните“ означава всяко свободно изразено, конкретно, информирано и недвусмислено указание за волята на субекта на данните, чрез изявление или ясно потвърждаващо действие, което изразява неговото съгласието свързаните с него лични данни да се обработват.

„Нарушение на сигурността на лични данни“ означава нарушение на сигурността, водещо до случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или

достъп до лични данни, които се предават, съхраняват или обработват по друг начин.

„Представител“ означава физическо или юридическо лице, което е установено в ЕС и което, назначено от администратора или обработващия лични данни в писмена форма съгласно член 27, представлява администратора или обработващия лични данни във връзка с техните съответни задължения по Регламента за защита на личните данни.

„Задължителни фирмени правила“ маркира политики за защита на личните данни, които се спазват от администратор или обработващ лични данни, установен на територията на държава-членка, при предаване или съвкупност от предавания на лични данни до администратор или обработващ лични данни в една или повече трети държави в рамките на група предприятия или група дружества, които участват в съвместна стопанска дейност.

„Надзорен орган“ означава независим публичен орган, създаден от държава членка съгласно член 51 от Регламента.

Служител по защита на данните – още наричан **„Длъжностно лице по защита на данните“** (ДЗЛД).

Регламента и неговото въздействие върху счетоводителя/ ТРЗ-служителя

Към 25 май 2018 г. регламентът отмени и замести Директива № 95/46/ ЕО относно защитата на лицата по отношение на обработката на лични данни и свободното движение на такива данни (член 94 от GDPR).

Регламентът е пряко приложим във всички държави-членки съгласно Договора за функционирането на Европейския съюз. В

резултат на това от 25 май 2018 г. регламентът също така замени вътрешната регулаторна рамка в конкретна област.

Общият регламент за защита на данните (GDPR) изисква всяка компания, предлагаща продукти и услуги за физически лица в България и Европейския съюз, да обработва лични данни, като например да извършва събиране, съхранение и обмен на данни, в пълно съответствие с неговите разпоредби.

Счетоводните фирми и самите счетоводители и ТРЗ-служители също обработват лични данни. Ето защо задължението да прилагате режима при обработването на тези данни (например в ситуациите, когато попълвате данъчни декларации или предоставяте услуги като начисляване на заплати), няма как да Ви отмине. В същото време като предприятие обработвате личните данни на Вашите собствени служители, включително чувствителни лични данни като например биометрични данни (които получавате от болнични листове), данни от лични карти, данни за образование и професионална квалификация и т.н.

Обработката на лични данни трябва да се извършва в съответствие с принципите, изложени в чл. 5 от Регламента:
а) личните данни трябва да бъдат обработвани законосъобразно, добросъвестно и по прозрачен начин по отношение на субекта на данните;
б) те трябва да се събират за конкретни, изрично указани и легитимни цели и да не се обработват по-нататък по начин, несъвместим с тези цели; по-нататъшното обработване за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели се счита, съгласно член 89, параграф 1, за несъвместимо с първоначалните цели;
в) личните данни трябва да са подходящи, свързани с и ограничени до необходимото във връзка с целите, за които се обработват;
г) личните данни трябва да са точни и при необходимост да бъдат поддържани в актуален вид; трябва да се 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;
д) личните данни се съхраняват във форма, която позволява идентифицирането на субекта на данните за период, не по-дълъг от необходимия за целите, за които се обработват личните данни; личните данни могат да се съхраняват за по-дълги срокове, доколкото ще бъдат обработвани единствено за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели съгласно член 89, параграф 1, при условие че бъдат приложени подходящите технически и организационни мерки, за да се гарантират правата и свободите на субекта на данните;
е) личните данни ще бъдат обработвани по начин, който гарантира подходящо ниво на тяхната сигурност, включително защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане, като се прилагат подходящи технически или организационни мерки;

Макар да звучат теоретично, в действителност тези принципи са много важни на практика, тъй като те винаги трябва да се разглеждат под призмата на цялостната обработка на лични данни. Именно тези принципи ще се взимат предвид при евентуално определяне на нарушения и санкциите, когато се правят проверки.

Основни действия, които счетоводителите/ ТРЗ-служителите трябва да предприемат, за да се подготвят за прилагането на регламента

а) да изяснят връзката между администраторите на лични данни и лицата, обработващи лични данни (т.е. операторите).

GDPR определя две ясни роли за използването на лични данни:

администратори и оператори на данни (лице, обработващо данните). В резултат на това трябва да помислите кой каква от ролите изпълнява Вашата счетоводна фирма.

Това разграничение е по същество важно при отчитане на следното:
а) Задълженията на администратора са по-многобройни от тези на оператора. Например, с изключение на ограничени ситуации, администраторът е длъжен да информира субектите на данни за обработката на личните им данни и нейните специфики.
б) Отговорността на администратора е по-широка от тази на оператора, особено по отношение на наказателната отговорност.
в) Правата на субектите на данни се упражняват главно във взаимоотношенията им с администратора, докато операторът подпомага администратора в осигуряване съблюдаването на тези права.

Администратор на данни се явява организацията, която определя целта и установява средствата за събиране и съхранение на лични данни. В зависимост от Вашата сфера на работа, Вие можете да обработвате данните от името на друга фирма, която се явява техен администратор. При това положение действате като упълномощено лице оператор (например в контекста на настоящото ръководство – доставчик на счетоводни и ТРЗ услуги). В този случай Вие обработвате данните в интерес на администратора им, поради което Вашата счетоводна фирма се счита оператор на лични данни. Въпреки това, ако същевременно с горепосочените си задължения, изпълнявате и задължения в свой собствен интерес (като например докладвате определени нарушения) или обработвате данните на собствените си служители, Вие изпълнявате ролята на администратор на данни.

Иначе казано, това, че за своите клиенти – администратори се явявате оператор на данни, не значи, че не можете едновременно с това да сте администратор на данни.