ОБЩИ ПОЛОЖЕНИЯ ПО GDPR

ВАЖНО!

Информацията в този документ не може и не трябва да бъде използвана в качеството на юридически съвет!

Надзорният орган по Регламент 2016/679 е Комисията за защита на личните данни (КЗЛД). Регламентът създава възможност за консултации с надзорния орган, който да издаде препоръки по предприемане на мерки.

За да прилагаме правилно Регламент 679/2016 е необходимо да сме наясно с основните моменти, около които същият развива уредбата, касаеща личните данни и тяхната защита.

Отбелязваме, че регламентите, като правни актове на ЕС, от който Република България е част, са пряко приложими и местни закони не могат да им противоречат. Съответно, на правата и задълженията, заложени в тях, лицата могат да се позовават пряко.

На първо място: основните, засягащи абсолютно всеки администратор и обработващ лични данни, понятия:

1. Лични данни – без да се впускаме в сухата буква на регламента, ще е най-лесно да приемем, че всяка единица информация, която по някакъв начин може да се свърже с един човек и същият съответно да бъде идентифициран или лесен за идентификация, представлява лични данни;

2. Обработване на лични данни – отново – най-лесно е да се приеме, че всяка дейност, отнасяща се по някакъв начин до определен набор от лични данни, представлява обработка;

3. Администратор на лични данни (АЛД) – лице или структура, които самостоятелно или съвместно определят целите и средствата за обработването на лични данни;

4. Обработващ лични данни (ОЛД) – лице или структура, които обработват лични данни от името на администратора;

На второ място трябва да се запознаем с принципите, въведени с Регламента:

1. Принцип на законосъобразност, добросъвестност, прозрачност – данните трябва да бъдат обработвани законосъобразно, добросъвестно и по прозрачен начин по отношение на субекта на данните;

2. Принцип на ограничение на целите на обработката – обработката

трябва да се извършва за конкретни, изрично указани и легитимни цели. Т.е. обработката не трябва да се извършва по начин, несъвместим с определените цели.

3. Обработка, сведена до минимум – данните и обработката им трябва да са подходящи на целта, предвидена за обработката

4. Принцип на точността – при обработката на данните, същите трябва да са поддържани в актуален вид. Съответно следва да се гарантира своевременното изтриване или коригиране на неточностите и да се взимат предвид за това целите на обработката;

5. Принцип за ограничение на съхранението – данните да се съхранявани във форма, която да позволява идентифицирането на субекта на данните за период, не по-дълъг от необходимото за целите, за които се обработват личните данни

6. Цялостност и поверителност - обработвани по начин, който гарантира подходящо ниво на сигурност на личните данни: защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане, като се прилагат подходящи технически или организационни мерки, както и защита срещу достъп до неограничен кръг от физически лица;

7. Принцип на отчетност – администраторът носи отговорност, че спазва всички принципи и може да докаже, че ги спазва.

Третото, което следва да се извърши е план по самото прилагане на Регламента. Стъпките, които се предлагат тук се отнасят до основните изисквания на регламента, без да имат претенция за изчерпателност и конкретика:

1. Запознаване с нормативната база – текуща и бъдеща, отнасяща се до защитата на личните данни при тяхната обработка. Това, естествено, включва подробно и ясно познаване на конкретни права и задължения за администратори, обработващи и физически лица;

a. Познаването на нормативната база дава много важна информация по въпроса за определяне правните основания за събиране и обработване на личните данни. Правилното или неправилното определяне на основанието е критична точка, която предварително може да реши или създаде набор от проблеми.

2. Анализ на дейностите по обработка – това е логична втора стъпка след пълно и правилно познаване на нормативния акт. Според организацията, в която ще се прилага регламента, следва да се отчитат специфичните особености по обработка, които да се отразят при конкретното имплементиране на нормативните изисквания;

3. Преценка относно необходимостта от ДЛЗЛД – като последица от запознаване с нормата и прилагането ѝ според специфичната дейност трябва да се вземе предвид наличието или липсата на необходимост от назначаване на ДЛЗЛД.

4. Оценка и управление на рисковете – администраторите и обработващите трябва да са наясно с възможността за пробив на сигурността при обработката, която извършват. Правилната преценка на възможността от такива инциденти и тежестта на последиците от едно такова събитие са задължение, което е от особена важност във връзка с последващите точки;

5. Консултации с КЗЛД – Регламентът създава възможност за консултации с надзорния орган, който да издаде препоръки по предприемане на мерки, защитаващи обработването;

6.Мерки – на база всичко взето до този момент предвид, следва да се набележат конкретни технически, организационни и др. мерки за защита. Под влиянието им трябва да попаднат всички дейности и системи, обработващи лични данни;

7.Документираност – във връзка с един от посочените принципи следва да се поддържа определен набор от регистри, бланки и документи, които в дадени моменти да се предявяват пред физическите лица с права спрямо техните лични данни или пред надзорния орган (КЗЛД) в рамките на законната му дейност;

8.Информираност на служителите – АЛД и ОЛД следва да положат усилия в посока образование на служителите им. Служители, които не познават правата на субектите на личните данни, могат да възбудят търсене на отговорност спрямо техния работодател, а в крайни случаи и към самите тях.

ОмегаСофт ООД