ОБЩ РЕГЛАМЕНТ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ
(EU General Data Protection Regulation - GDPR)

ОПЕРАТИВНО РЪКОВОДСТВО

ЗА МАЛКИ И СРЕДНИ ПРЕДПРИЯТИЯ ,

ЗА ВНЕДРЯВАНЕ НА ИЗИСКВАНИЯТА, В СЪОТВЕТСТВИЕ С GDPR И ЗАКОНА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ (проект)

ВЪВЕДЕНИЕ

Целта на това Оперативно ръководство (ОР) е практически да подпомогне малките и средни предприятие (МСП), при работата им с GDPR.

GDPR е много обширен и детайлен документ. За да бъде „приведен“ GDPR в практически използваем документ, това ОР обръща основно внимание на тези изисквания, които са свързани с особеностите на МСП. Освен това, ОР обвързва тези подбрани изисквания с подходящи за прилагане контролни / защитни механизми, като за целта са използвани препоръките на ISO 27002 – 2013 / Information technology — Security techniques — Code of practice for information security controlsл

Забележка: За пълноценното ползване на ОР и за постигане на практическото му прилагане е препоръчително, най-малкото, в МСП да има базови познания по GDPR и информационната сигурност (напр. ISO 27000 – 2018 / Information technology — Security techniques — Information security management systems — Overview and vocabulary)

Начален въпросник

Следващите въпроси са тясно свързани с основните части на GDPR и е препоръчително МСП да отговорят на тях, и да документират своите отговори. Изпълнението на тази дейност силно ще подпомогне последващото разбиране и практическо прилагане на изискванията за защитата на личните данни.

Въпроси:

1. Дали организацията е обект (в обхвата) на GDPR?
2. Дали информацията, която организацията обработва (желае да обработва) е обект (в обхвата) на GDPR?
3. Какви категории лични данни се обработват в организацията (или има желание / намерения да се обработват)?
4. Какви обработки извършва и/или ще извършва организацията с личните данни?
5. Каква е функцията на организацията – администратор и/или обработващ на лични данни – отчитайки обработките, които извършва с тях?
6. Организацията има ли правни основания за обработка на исканите (и получавани) от нея лични данни?

7. Изпълнява ли организацията принципите за обработка на личните данни, съгласно изискванията на GDPR?
8. Изпълняваните от организацията обработки на личните данни, пропорционални (съответстват ли и в каква степен) ли са на целите на тези обработки?
9. Възможно ли е организацията да събира и обработва личните данни по по-малко „натрапчив“ и/или „агресивен“ начин, като запазва възможностите си за постигане на целите на обработките?
10. Изпълнява ли организацията изискванията, свързани с правата на субектите на данни (физическите лица за които се събират и обработват лични данни) при обработката на личните им данни (съгласно изискванията на GDPR)?
11. Изпълнява ли организацията задълженията, свързани с отчетността, документирането, трансфера и сигурността при обработката на лични данни (съгласно изискванията на GDPR)?
12. Прилагат ли се специални условия за обработката на лични данни в организацията?(напр. ползване на организация за обработка на лични данни, базирана извън ЕС)

Основни определения, използвани за целите на ОР (на база определенията в GDPR)

- **„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 физическо лице;
- **„обработване“** означава всяка операция или съвкупност от операции, извършвана с лични данни или набор от лични данни чрез 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 данните стават достъпни, 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 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 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 личните данни, независимо дали е трета страна или не. Същевременно публичните органи, които могат да получават лични данни в рамките на конкретно разследване в съответствие с правото на Съюза или правото на държава членка, не се считат за „получатели“; обработването на тези данни от посочените публични органи отговаря на приложимите правила за защита на данните съобразно 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 имат право да обработват личните данни;
- **„нарушение на сигурността на лични данни“** означава нарушение на сигурността, което води до случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до лични данни, които се предават, съхраняват или обработват по друг начин;

Забележка: За повече информация за използваната терминология може да се ползва GDPR и по-специално чл. 4 „Определения“

GDPR – изисквания и контролни / защитни механизми за тяхното изпълнение

В следващите части на ОР, изискванията на GDPR, подбрани специално за МСП, са свързани с подходящи контролни / защитни механизми и съответните препоръки за тяхното внедряване. По този начин, за всяко изискване на GDPR се определя един или повече, конкретни контролни / защитни механизми, следвайки препоръките на ISO 27002. За МСП, администратори на лични данни, които ползват публични „облачни“ услуги за тяхната обработка, са добавени и допълнителни контролни / защитни механизми, в съответствие с препоръките на ISO 27018 – 2014 / Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

Изискванията на GDPR (свързани с МСП), съответните контролни / защитни механизми и препоръките за тяхното внедряване са описани в ОР за следните области:

1. Обхват на въздействие на GDPR
2. Обработка на лични данни;
3. Принципи за обработка на личните данни
4. Права на субекта на лични данни
5. Задължения на МСП (администратор и/или обработващ лични данни) по сигурността
6. Специални случаи за прилагане на GDPR
7. Документи, свързани с внедряването на изискванията на GDPR, за защита на личните данни

Забележка: След приемането на новия Закон за защита на личните данни, това ОР ще бъде своевременно актуализирано, както е приложимо.