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

ОПЕРАТИВНО РЪКОВОДСТВО

ЗА МАЛКИТЕ И СРЕДНИ ПРЕДПРИЯТИЯ ,

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

1.Обхват на въздействие на GDPR

Цел
Трябва да се определи, дали организацията и информацията, която тя обработва са обект на GDPR.

1.1.Общи въпроси
• Организацията обект ли е на GDPR ?

Контрол

Член от GDPR , определящ изисквания, свързани с МСП	**Контроли (сигнатура по ISO 27002:2013) свързани със съответните членове на GDPR**	**Допълнителни контроли (сигнатура по ISO 27018:2014) свързани със съответните членове на GDPR (при използване на публични „облачни“ услуги за обработка на лични данни)**
Чл.3 (териториален обхват) Чл.27 (представителство) **Организацията трябва да определи дали е в обхвата на GDPR**	A.18.1.4 (съответствие с тайната и защитата на информацията за самоличността) **Контрол** Трябва да бъде осигурена тайната и защитата на информацията за самоличността според изискванията на съответните нормативни актове и регламенти, където са приложими.	A.11 (съответствие с тайната на информацията за самоличността) A.11.1 Географско разположение на информация за самоличността **Контрол** Организациите поддържащи (оператор) публичен „облак“ и изпълняващи обработка на лични данни (обработващ лични данни) на администратори, трябва да определят и документират страните, в които личните данни могат да бъдат съхранявани. A.11.2 Планирани места за получаване на информация за самоличността **Контрол** Информацията за самоличността, предавана чрез мрежите за обмен на данни, трябва да бъде контролирана, с цел да се

		осигури, че е пристигнала на планираното място за получаване.

Препоръки за изпълнение на изискванията по чл.3 и чл.27 от GDPR

Всички администратори и обработващи лични данни, които са установени в ЕС, са в обхвата на GDPR, независимо от това, дали обработките на личните данни се извършват в или извън ЕС.

Организациите, които създават продукти и/или услуги за граждани от ЕС (определени чрез езика, валутата или като клиенти в ЕС), са в обхвата на GDPR.

Организациите, които регистрират режим на работа за субекти на данни, вътре в ЕС (напр. наблюдение, профилиране и/или определяне на предпочитания), са в обхвата на GDPR.

Ако организациите извършват дейности по последните две позиции е необходимо да определят свой представител за ЕС.

Ако организацията е определила, че е в обхвата на GDPR, то тя трябва ясно да **документира** основанията, от които произтича това нейно решение. Това документиране може да стане чрез прилагане на контрол А.18.1.4 (ISO 27002), в рамките на документ **„Политика за защита на личните данни“**. Наличието и изпълнението на тази Политика, на практика представлява контролен / защитен механизъм, осигуряващ изпълнението на съответните изисквания на GDPR.

Забележка: Политиката за защитата на личните данни, не се разработва единствено и само за целите на изпълнението на горепосочените членове на GDPR. В тази Политика се включват много други въпроси, свързани със защитата на личните данни. Тя не се разработва единствено и само за да се оповести и/или покаже на „видно“ място – тя трябва да се изпълнява и организацията трябва да има и да предоставя (както е приложимо) ясни доказателства за това изпълнение.

Ако организацията е определила, че е в обхвата на GDPR и използва публични „облачни“ услуги за обработка на лични данни, то тя трябва ясно да **документира местата (страните)**, в които се съхранява обработваните в публичния „облак“ лични данни (контрол А.11.1 от ISO 27018) и **приложените средства за контрол** (технически, административни и др.) на получаването на предаваните лични данни на предварително определените (планирани) места (контрол А.11.2 от ISO 27018).

Забележка: Организацията е в правото си да изисква от оператора на публичния „облак“, който тя използва за обработка на лични данни, да получава информация за местата за тяхното съхранение. От друга страна, оператора на публичен „облак“, би трябвало да предоставя достъп до такава информация на своите клиенти, още повече, че самия той, обработвайки лични данни на организацията, попадат в обхвата на GDPR, в качеството си на „обработващ лични данни“. Организациите могат, в този случай, де се възползват и от съществуващи международни договори за трансфер на данни, в които се обхващат и оператори на публични „облаци“.

1.2.Общи въпроси

• Информацията, която организацията обработва (или възнамерява да обработва) дали е в обхвата на GDPR (представлява ли лични данни) ?

Контрол

Член от GDPR , определящ изисквания, свързани с МСП	**Контроли (сигнатура по ISO 27002:2013) свързани със съответните членове на GDPR**	**Допълнителни контроли (сигнатура по ISO 27018:2014) свързани със съответните членове на GDPR (при използване на публични „облачни“ услуги за обработка на лични данни)**
Чл.4 (1) (лични данни) **Организацията трябва да определи, дали ще обработва личните данни, както се изисква в GDPR.**	A.8.2.1 (класифициране на информацията) **Контрол** Информацията трябва да бъде класифицирана според изискванията на нормативните актове, нейната стойност, критичност и чувствителност към неоторизирано разкриване или модифициране.	Няма допълнителен контрол

Препоръки за изпълнение на изискванията по чл.4 (1) от GDPR

GDPR обхваща личните данни, които се обработват чрез автоматизирани средства (системи), а също и **всяка друга обработка** на лични данни, която може да бъде използвана за регистриране в система.
Личните данни са всякакъв вид информация, свързана с идентифицирано физическо лице или с възможна негова идентификация, посредством тази информация.
Личните данни обхващат псевдонимизацията и **изключват** анонимизацията.

Физическо лице, с възможна идентификация е лице, което може да бъде идентифицирано (директно или индиректно) отчитайки:
-идентификатори, като име, № на личен документ, данни за местонахождение или
-“on-line” идентификатори от всякакъв тип – напр. IP, RFID, “бисквитки“(cookie) или
-други характеристики, специфични за отделните лице – напр. физически, генетични, умствени, културни, социални, финансови и др.

Забележка: В преамбюлите 30 и 64, и в чл.4 (1) на GDPR, “идентификаторите“ са определени, като нещо, което може да се използва за идентифициране на физически лице.

Ако организацията е определила, че ще обработва личните данни, в съответствие с изискванията на GDPR, тя трябва ясно да документира основанията за това свое решение и да разработи и приложи **Политика за класифициране на личните данни** (контрол A.8.2.1 от ISO 27002) , включваща и препратки към съответните **процедури, инструкции и др**.за работа с класифицирана лична информация. В документацията по този въпрос, трябва да има и описан механизъм за управление на класифицираните лични данни.

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