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.Обработка на личните данни

Цел

Организацията трябва да разкрие правната база за обработването от нея на лични данни (или тези, които има намерение да обработва). В допълнение, организацията трябва ясно да определи своите функции в процеса за обработката на личните данни. Организацията, трябва да определи и упълномощения надзорен орган, с който да контактува в съответните случаи, описани в GDPR.

1.1.Общи въпроси

• Какви категории лични данни обработва (или ще обработва) организацията?

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.6 (общи лични данни) и чл.9 (чувствителни лични данни) **Организацията трябва да определи, какви категории от лични данни ще обработва**	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.6 и чл.9 от GDPR

GDPR определя две основни категории от лични данни – **общи** лични данни и **чувствителни** лични данни. **Чувствителните** лични данни са свързани и/или разкриват раса, етнос, политически възгледи, религиозна или философска вяра, генетика, биометрия, здравно състояние, сексуален живот и сексуална ориентация. **Криминалната** информация, съдържаща лични данни е специална категория на общите лични данни, изискваща допълнителни защити.

След като организацията е определила категориите лични данни, които ще обработва, тя трябва ясно да документира основанията за това свое решение и да разработиq 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. В случай на обработка и на **криминална** информация, трябва да се спазват националните (или приетите международни) ред и правила за сигурност и това трябва да бъде документирано в **Политика за класифициране на личните данни,** като изрично се посочат съответните закони, директиви, регламенти, наредби, процедури и др., както е приложимо.

1.2.Общи въпроси

• Какви видове обработки на лични данни ще използва организацията ?

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) 2 (обработване) **Организацията трябва да определи, какви обработки ща използва за съответните категории лични данни**	A.8.1.3 (допустимо използване на активите) **Контрол** Трябва да бъдат посочени, документирани и прилагани правила за допустимо използване на информация и активи, свързани с информацията и средствата за обработване на информация.	Няма допълнителен контрол

Препоръки за изпълнение на изискванията по чл.4 (1) 2 от GDPR

Обработката на лични данни, в съответствие с определението в GDPR , трябва да се разбира широко, както следва: „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;

След като, организацията е определила, какви обработки ще извършва с различните категории лични данни, тя трябва ясно да документира основанията за това свое решение и да разработи, и приложи съответните **ред и правила** чрез **Политика за допустимите обработки на личните данни** (контрол A.8.1.3 от ISO 27002) , включваща и препратки към съответните **процедури, инструкции и др**., както е

приложимо. В тази документация, трябва да има и описан механизъм за **контрол и управление на достъпа на външни лица** до активи на организацията, обработващи лични данни.

1.3.Общи въпроси

• Каква функция изпълнява организацията – на администратор и/или на обработващ лични данни – при работата си с личните 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) 7 (администратор) **Организацията трябва да определи за кои обработки на лични данни е „администратор“**	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.	Няма допълнителен контрол
Чл.4 (1) 8 (обработващ лични данни) **Организацията трябва да определи за кои обработки на лични данни е „обработващ лични данни“**	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.4 (1) 7 и чл.4 (1) 8 от GDPR

Организацията може да изпълнява и двете функции (администратор и обработващ данни) или само една от тях за определени обработки, и други функции за други обработки на лични данни. Организацията е отговорна за личните данни, ако тя определя целите на обработките и средствата / методите, чрез които те се извършват, т.е., в този случай тя е „администратор“. Организацията, „обработващ лични данни“, извършва обработките на база инструкциите на „администратора“.

След като организацията е определила своите функции, по отношение работата с личните данни – администратор и/или обрабоващ лични данни - 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 предоставя (както е приложимо) ясни доказателства за това изпълнение.

Ако организацията е определила, че 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“.

1.4.Общи въпроси

• Организацията има ли правни основания за обработка на съответните категории 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)”.=6**
Чл.6 (общи лични данни – правна основа / законосъобразност за обработка) Чл.9 (чувствителни лични данни) Чл.85 (обработки и свобода на изразяване и информация – за	А.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	А.11 (съответствие с тайната на информацията за самоличността) А.11.1 Географско разположение на информация за самоличността **Контрол** Организациите поддържащи (оператор) публичен „облак“ и изпълняващи обработка

журналистически, академични, художествени, актьорски и литературни цели) Чл.86 (публичен достъп до официални документи) Чл.87 (обработка на национални идентификационни номера) Чл.88 (обработки, свързани с трудови / служебни правоотношения) Чл.89 (публичен интерес, научни, исторически и статистически цели) Чл.90 (опазване на тайната) **Организацията трябва да определи дали има правна основа за обработките които ще извършва на различните категории лични данни. В този контекст, организацията трябва да установи, дали съществуват специални национални правила, които трябва да бъдат взети под внимание (приложени съответните изисквания)**.	регламенти, където са приложими.	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.
Чл.4(1) 16 (основно място на установяване) Чл.60 (сътрудничество между надзорните органи) Чл.50 (компетенции на надзорните органи) **Организацията трябва да определи с кой надзорен орган в Европа ще контактува.**	A.6.1.3 (контакт с оторизираните органи) **Контрол** Трябва да се поддържат подходящи контакти със съответните оторизирани органи.	Няма допълнителен контрол

Препоръки за изпълнение на изискванията по чл.6, 9, 85, 86, 87, 88, 89, 90 и 4 (1)16, 60 и 55 от GDPR.

Организацията може да обработва общи персонални данни, ако са изпълнени принципите за тяхното обработване (разглеждат се в следваща част на ОР) и е изпълнено поне едно от следните условия:

- Получено е правно съгласие за обработка;
- Обработката е необходима за изпълнението на договор, в който субекта на данни е страна;
- Организацията „обработващ данни“, трябва да изпълнява правни задължения;

• Ако е необходимо да се защитават жизненоважни интереси на субекта на данни или на други лица;
• Ако е необходимо за изпълнението на задачи в обществен интерес или за функционирането на администратор, на база официално упълномощаване;
• При баланс на интереси, когато е необходимо за целите на легитимните интереси на администратора или на трета страна, с изключение на такива интереси, които погазват интересите или фундаменталните права, и свободи на субекта на лични данни.

Организацията може да обработва чувствителни лични данни, ако е налице, което и да е било от следващите условия:

• Получено е изключително съгласие за обработка;
• Правното основание за обработките се съдържа в трудовото законодателствоили / в колективните трудови договори;
• Ако се наложи защита на жизненоважни интереси на субекта на данни или на други лица;
• Ако обработките се извършват от фондации, асоциации и други организации с идеална цел, при изпълнение на техните легитимни дейности;
• Ако информацията е вече публикувана от самия субект на лични данни;
• Ако информацията е част от създаването, използването или защитата на правни претенции;
• Ако информацията е необходима за нуждите на съществени обществени интереси, имащи правно основание;
• Ако информацията е необходима за здравни цели;
• Ако информацията е необходима за исторически, научни или статистически цели; I

В допълнение към тези основни изисквания за обработка на лични данни, в някои области има (или може да се подготви и приложи) отделна правна рамка / база. Примери за такива области са:

• Журналистика;
• Образование, театър, кино, литература;
• Национални идентификационни номера;
• Трудово – правни въпроси и работна сила;
• Публичен интерес;
• Наука, история, статистика;
• Професионална тайна;
• Църковни и религиозни асоциации;
• Здравеопазване;

GDPR въвежда концепцията „one-stop-shop“, която означава, че всяка организация ще бъде обвързана с един надзорен орган в Европа. В общия случай,това ще бъде надзорния орган в страната, в която организацията е изградила основните си бизнес единици или в станата, където организацията взема решения за обработка на лични данни. В крайна сметка, организацията трябва да прецени към кой надзорен орган (само един) ще бъде свързана.

След като организацията е определила правната основа за обработките на различните категории лични данни, а също и е решила с кой надзорен орган ще бъде обвързана - то тя трябва ясно да **документира** съответните закони, наредби и др., и избрания надзорен орган,както е приложимо. Това документиране може да стане чрез прилагане на контрол A.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. В допълнение организацията е препоръчително да разработи и внедри **„Инструкция за контакт и взаимодействие с надзорен орган“.**

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 предоставя (както е приложимо) ясни доказателства за това изпълнение.

Ако организацията е определила, че 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 A.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 A.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, информация **за прилагането на изискванията на GDPR** за тяхната обработка и 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“.

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