

**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)**

**ПРЕПОРЪЧИТЕЛНИ И ЗАДЪЛЖИТЕЛНИ ДОКУМЕНТИ,
СВЪРЗАНИ С ВНЕДРЯВАНЕТО
НА ИЗИСКВАНИЯТА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ**

Забележка: Показаните по-долу в таблицата документи, не са краен списък от документите, свързани с внедряването на изискванията на GDPR. За всяка отделна организация могат да се появят още много допълнителни документи (напр., процедури, инструкции и др. по сигурността на личните данни). На практика, не съществува един, единствен набор от документи, за различните организации. В този смисъл, показаните по-долу в таблицата документи, могат и трябва да се разглеждат, като едно ядро, около което могат да се добавят различни документи, свързани с прилагането на изискванията за защита на личните данни – както е приложимо за съответната организация.

№	№ документ	Име на документа	Член на EU GDPR	Задължителен документ по GDPR	Препоръчителен документ
	1	Подготовка за работата по проект „Защита на личните данни в съответствие с изискванията на EU GDPR и законите на страната”			
1	1.1	Анализ и оценка на готовността на организацията за изпълнение изискванията за защита на личните данни	НЯМА	НЕ	ДА
2	1.2	План за изпълнение на проект „Защита на личните данни в съответствие с изискванията на EU GDPR и законите на страната”	НЯВА	НЕ	ДА
	2	Политики, свързани със защитата на личните данни			
3	2.1	Политика за защита на личните данни	Чл. 24(2)	ДА	

		Забележка: Към тази Политика може да има, както е приложимо, процедури, инструкции, планове, шаблони на документи и др., свързани със сигурността на личните данни			
4	2.2	Политика за защита на личните данни на служителите на организацията Забележка: Към тази Политика може да има, както е приложимо, процедури, инструкции, планове, шаблони на документи и др., свързани със сигурността на личните данни	Чл. 24(2)	НЕ	ДА
5	2.3	Съобщение, свързано с тайната на личните данни	Чл.12, 13 и14	ДА	
6	2.4	Регистър на съобщенията, свързани с тайната на личните данни	Чл.12, 13 и14	НЕ	ДА
7	2.5	Политика за запазване на личните данни Забележка: Към тази Политика може да има, както е приложимо, процедури, инструкции, планове, шаблони на документи и др., свързани със сигурността на личните данни	Чл. 5(1)(е), 13(1), 17 и 30	ДА	
8	2.6	Приложение – Опис , свързан със запазването на личните данни	Чл. 30	ДА	
9	2.7	Дръжностна характеристика на „Служител по защита на личните данни“	Чл. 37, 38 и 39	ДА	
	3	Дейности, свързани с обработките на лични данни			
10	3.1	Ръководство за подготовка на Опис на личните данни и съответните обработки, които се извършват с тях	Чл. 30	НЕ	ДА
11	3.2	Приложение – Опис на обработките на личните данни	Чл. 30	ДА	
	4	Управление на правата на субектите на данни			
12	4.1	Форма за съгласие на субекта на данни	Чл. 6(1)(а), 7(1) и 9(2)	ДА	
13	4.2	Форма за оттегляне на дадено съгласие от субекта над анни	Чл. 7(3)	НЕ	ДА
14	4.3	Фолма за родителско съгласие	Чл. 8	ДА	
15	4.4	Форма за оттегляне на дадено родителско съгласие	Чл. 8	ДА	
16	4.5	Процедура за искане на достъп от субект на данни	Чл. 7(3), 15, 16, 17, 18, 20, 21 и 22	НЕ	ДА

17	4.6	Форма за искане на достъп от субект на данни	Чл. 15	НЕ	ДА
18	4.7	Форма при разкриване на лични данни на субекта на данни	Чл.15	НЕ	ДА
	5	Оценка на въздействието върху защитата на личните данни			
19	5.1	Методология за оценка на въздействието върху защитата на личните данни	Чл.35	НЕ	ДА
20	5.2	Регистър на оценките на въздействие върху защитата на личните данни	Чл. 35	ДА	
	6	Трансфер на лични данни			
21	6.1	Процедура за трансграничен трансфер на лични данни	Чл. 1(3), 44, 45, 46, 47 и 49	НЕ	ДА
22	6.2	Приложение 1 – Стандартизирани клаузи в Договор за трансфер на лични данни	Чл. 46(5)	ДА	
23	6.3	Приложение 2 - Стандартизирани клаузи в Договор за трансфер на лични данни към обработващ данни	Чл. 46(5)	ДА	
	7	Съответствие на трети страни с GDPR			
24	7.1	Въпросник за оценка на съответствието с GDPR на обработващ данни.	Чл. 28 и 32	НЕ	ДА
25	7.2	Споразумение / договор с доставчик на услуги за обработка на лични данни	Чл. 28, 32 и 82	ДА	
	8	Сигурност на личните данни			
26	8.1	Политика за ИТ сигурност	Чл.32	НЕ	ДА
27	8.2	Политика за контрол на достъпа	Чл.32	НЕ	ДА
28	8.3	Политики за сигурност на ИТ звеното	Чл.32	НЕ	ДА
29	8.4	Политика за работа с лични компютърни средства	Чл.32	НЕ	ДА
30	8.5	Политика за работа с мобилни устройства	Чл.32	НЕ	ДА
31	8.6	Политика за „чисто“ бюро	Чл.32	НЕ	ДА
32	8.7	Политика за класифициране на информацията	Чл.32	НЕ	ДА
33	8.8	Политика за анонимизация и псевдонимизация	Чл.32	НЕ	ДА
34	8.9	Политика за използване на криптография	Чл.32	НЕ	ДА
35	8.10	План за възстановяване при бедствия	Чл.32	НЕ	ДА

36	8.11	Процедура за провеждане на вътрешни одити по сигурността	Чл.32	НЕ	ДА
37	8.12	Приложение – Въпроси за предварителна проверка на сигурността, при провеждане на вътрешни одити.	Чл.32	НЕ	ДА
	9	Пробиви в защитата на личните данни			
38	9.1	Процедура за отговор и уведомяване при пробив на защитата на личните данни.	Чл. 4(12), 33 и 34	ДА	
39	9.2	Регистър на пробивите в защитата на личните данни	Чл. 33(5)	ДА	
40	9.3	Форма за уведомяване на надзорния орган при пробив в защитата на личните данни.	Чл. 33	ДА	
41	9.4	Форма за уведомяване на субекта на данни, при пробив в защитата на личните данни.	Чл. 34	ДА	