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)

1.Специални случаи за прилагане на GDPR

Част от изискванията на GDPR са пряко свързани с определени специфични ситуации. Пример за такава, специфична ситуация е случая, когато организация обменя лични данни със страна извън ЕС.

Най-общия въпрос в случая е:
• Приложими ли са за организацията специалните условия / изисквания за обработка на лични данни?

1.1 Общи въпроси
• Ще се предават лични данни, към страна (и) извън ЕС ?

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.44 (общи принципи за трансфер) **Администратора грябва да определи дали ще се предават лични данни щъм страна (и) извън ЕС**	A.18.1.4 (l) (Тайна и защита 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.
Чл.44 (общи принципи за трансфер) **При случаи на предаване на личнни данни към страни извън ЕС, правните основания за този обмен трябва да бъдат ясно определеви и докуменнирани.**	A.18.1.4 (I) (Тайна и защита 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.
Чл.46 (трансфер) **Когато администратора предава данни в страна извън ЕС, трябва да има договор / споразумение (писмени) със съответния администратор и/или обработващ данни от тази страна.**	A.15.1.2 (Разглеждане на сигурността в рамките на споразумения с доставчици) **Контрол** Всички приложими изисквания към сигурността на информацията трябва дабъдат въведени и съгласувани с всеки доставчик, който може да има достъп, да обработва, да съхранява, да разпространява или да предоставя ИТ инфраструктурни компоненти за информацията на организацията.	Няма допълнителен контрол
Чл.46 и 47 (трансфер) **Администраторът ще одитира отсрещната страна за съответствие с изискванията на GDPR и за спазването на клаузите, и меркиге за сигурност, описани в съответния договор / споразумение.**	A.15.1.2 (Разглеждане на сигурността в рамките на споразумения с доставчици) **Контрол** Всички приложими изисквания към сигурността на информацията трябва дабъдат въведени и съгласувани с всеки доставчик, който може да има достъп, да обработва, да съхранява, да разпространява или да предоставя ИТ инфраструктурни компоненти за информацията на организацията.	Няма допълнителен контрол

Препоръки за изпълнение на изискванията по чл.44 и чл.46

В GDPR има редица възможности за намиране на правни основания за обмен на лечни данни със страни извън ЕС, както следва:

1.Европейската комисия (ЕК) е отчела, че в редица страни извън ЕС има национални закони, които осигуряват адекватно ниво на защита на личните данни. ЕК поддържа актуален списък на тези одобрени и сигурни „трети“ страни. Обикновано това са страни членки на ЕС.

2.Ива възвожности за трансфер а данни, към страни извън ЕС, на базата на двустранни споразумения между ЕК и съответната страна. Тези двустранни споразумения могат да не включват цялата страна, но те могат да включват организации в страната, които ясно са показали и доказали високо ниво на сигурност. Един, добре познат пример в това направление е споразумението Safe Harbour, между ЕК и САЩ. Това споразумение обаче е обявено за незаконосъобразно (през 2015 г.) от Европейския съд. От 2016 е в сила ново споразумение - **Privacy Shield.**

Освен това, администраторът може да предава данни към обработващ данни, базиран в страна извън ЕС, при наличие на **изричен договор** за трансфер на лични данни. Този договор трябва да бъде одобрен от съответния, национален надзорен орган. В тази област, ЕК е разработила стандартен договор, който моге да бъде използван, като правна основа за трансфир на лични данни. В някаи страни на ЕС е прието, че, ако се използва този стандартен догово за транфер на данни, без каквото и да е изменение на неговите клаузи, то не е необходимо одобрение от националния Надзорен орган. Това правно основание (изричен договор за обмен – особено стандартизиран от ЕК)е най-често използваното за трансфер на лични данни.

3.Възможно (но това почти не се случва) е да се осъществи правно обоснован трансфер на лични данни към страна извън ЕС в някои ограничени случаи. Съответния трансфер може да се основава на съгласие на субектана данни или, ако е необходим за изпълнението на договор, като това е в интерес на субекта на данни и обществото, основава се на националните закони или се извършва еднократно.

1.2 Общи въпроси

• Организацията в съответствие ли е с национaлното интерпретиране / внедряване на изискванията за защита на личните данни, описани в 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)**
Много от членовете в GDPR позволяват национално интерпретиране и правила за внедряване. **Администратора трябва да определи наличието на национално интерпретиране и внедряване на GDPR, и ако има такива, да**	A.18.1.4 (l) (Тайна и защита 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

осигури, че е в съответствие с тях.		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.

1.3 Общи въпроси

• Организацията в съответствие ли е с друго, приложимо законодателство, различно от GDPR, но занимаващо се с обработката налични 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)**
Много от членовете в GDPR позволяват национално интерпретиране и правила за внедряване. **Администратора трябва да определи дали законите в държавите от ЕС поставят специални правила – често, специфични за определени сектори – за обработка на личните данни, и с кои от тях трябва да бъде в съответствие.**	A.18.1.4 (l) (Тайна и защита 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 изпълнението

В много от страните от ЕС има секторно специфични ред и правила за обработка на личните данни. Напр., за секторите здравеопазване, средства за масово осведомяване, пазар на труда и др. При необходимост,съответния администратор трябва да осигури съответствие с техните изисквания, както е приложимо.

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