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.Права на субекта на данни

Цел

Организацията трябва изясни, дали предоставя възможности на субектите на лични данни да ползват пълноценно правата си.

1.1Общи въпроси

• Позволява ли организацията на субектите на данни да ползват пълноценно правата си ?

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.12 (2) (прозрачност) **Администраторът съдейства на субекта на данни по начин, осигуряващ го с възможности да упражнява своите права.**	A.12.1.1 (документирани процедури за работа) **Контрол** Процедурите за работа трябва да бъдат документирани и достъпни за всички потребители, които се нуждаят от тях.	Няма допълнителен контрол
Чл.12 (3) (прозрачност) **Администратора ще може да отговори на запитвания на субекта на данни, без прекомерно**	A.12.1.1 (документирани процедури за работа) **Контрол** Процедурите за работа трябва да бъдат документирани и достъпни за	Няма допълнителен контрол

забавяне и при всички случаи, в рамките на един месец от получаването на запитването.	всички потребители, които се нуждаят от тях.	
Чл. 13 (1) (2) (информацията, която трябва да се предостави, когато се събират данни от субекта на данни) Чл.14 (1) (2) (информацията, която трябва да се предостави, когато се придобиват данни НЕ от субекта на данни) Чл. 15 (1) (права и достъп на субекта на данни) **Администратора ще осигури субекта на данни с информация за обработките и съответните им операции, независимо от това дали данните са събрани от самия субект или са придобити от трета страна. В допълнение към задълженията на администратора за активно предоставяне на информация на субекта на данни преди започване на обработките, субекта може във всяко време да изисква достъп до данните и до информация, свързана с обработките.** **Администраторът трябва да разкрива най-малкото, следната информация:** **-Информация за идентичността и за контакт (същата информация, ако е приложимо, се предоставя е за служителя по защита на личните данни;** **-Целите на обработките и правните основания за тяхното извършване;** **-Легитимните интереси на**	A.12.1.1 (документирани процедури за работа) **Контрол** Процедурите за работа трябва да бъдат документирани и достъпни за всички потребители, които се нуждаят от тях. A.6.1.1 (роли и отговорности по информационната сигурност) **Контрол** Трябва да бъдат определени и разпределени всички отговорности по информационната сигурност 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.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. A.13.2.1 (іполитика и процедури за обмен на информация) **Контрол** Трябва да съществуват официални политики, процедури и механизми за контрол, за да се защити обменът на информация чрез използване на всички средства за комуникация.	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. **Забележка:** Когато за трансфера на информация се използват физически носители, трябва да има изградена система, чрез която да се регистрират входящите и изходящи физически носители, съдържащи лични данни, вкл., и типа на физическите носители; оторизираните податели и получатели; дата и време; брой на физическите носители. Когато е възможно, може да се приложат допълнителни мерки за сигурност (напр., криптиране на данните), с цел да се осигури, че данните могат дъ бъдат достъпни само в крайната (планираната) точка за получаване, а не по пътя на трансфера.

администратора, ако обработките се основават на принципа за „баланс на интересите“; **-Категориите персонални данни;** **-Категориите получатели на лични данни;** **-Информация за трансфера на лични данни към трети страни (ако е приложимо);** **-Времето за извършване (периода) за извършване на обработките (вкл. И съхраняване);** **-Правата, корекциите или изтриването на личните данни, ограниченията в обработките, правата за преносимост на данните;** **-Възможност за отказ от дадено съгласие;** **-Възможност за оплакване към надзорен орган;** **-Източниците за придобиване на лични данни (за трети стрени);** **-Информация за това, дали личните данни се обработват, като част от изпълнението на договор;** **-Информация, ако обработките се използват за „профилиране“;** **-Информация, ако личните данни се използват за нови цели;**		
Чл.16 (корекция) Чл.17 (право за изтриване) Чл. 18 (право за ограничение на обработките) **Администратора ще осигури изпълнението на правото на субекта на данни, за корекция или изтриване на данните**. **Администратора ще осигури ограничение на обработките, в съответствие с изискването на субекта на данни.**	A.12.1.1 (документирани процедури за работа) **Контрол** Процедурите за работа трябва да бъдат документирани и достъпни за всички потребители, които се нуждаят от тях.	Няма допълнителен контрол

Чл.19 (задължения за оповестяване) **Администраторът ще информира всички трети страни, за всяка корекция или изтриване на лични данни, свързани с конкретен субект на данни.**	A.12.1.1 (документирани процедури за работа) **Контрол** Процедурите за работа трябва да бъдат документирани и достъпни за всички потребители, които се нуждаят от тях.	Няма допълнителен контрол
Чл.20 (преносимост на данните) **Администраторът ще предоставя данни за субекта на данни в структуриран, общо приет, машинно четабилен формат на самия субект или на всеки друг администратор, на база искане от субекта на данни**	A.12.1.1 (документирани процедури за работа) **Контрол** Процедурите за работа трябва да бъдат документирани и достъпни за всички потребители, които се нуждаят от тях.	Няма допълнителен контрол
Чл.21 (право на възражение) **Администраторът ще управлява правата на субекта на данни, свързани с негови възражения към обработките на лични данни.**	A.12.1.1 (документирани процедури за работа) **Контрол** Процедурите за работа трябва да бъдат документирани и достъпни за всички потребители, които се нуждаят от тях. 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.
Чл.22 (профилиране) **Като правило, администраторът не може да извършва профилиране на субектите на данни, и трябва да осигури, че това практически не се случва.** **Ако профилирането е: необходимо за**	A.12.1.1 (документирани процедури за работа) **Контрол** Процедурите за работа трябва да бъдат документирани и достъпни за всички потребители, които се нуждаят от тях. A.18.1.4 (съответствие с тайната и защитата на информацията за самоличността)	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.

изпълнението на договор; правно оторизирано; или, изрично разрешено, чрез съответното съгласие на субекта на данни, профилирането може да бъде извършвано (т.е., то е легално).	**Контрол** Трябва да бъде осигурена тайната и защитата на информацията за самоличността според изискванията на съответните нормативни актове и регламенти, където са приложими.	A.11.2 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.12, 13, 14,15,16, 19, 20, 21 и 22

Администраторът ще подпомага субекта на данни по начин, който да му позволява да ползва пълноценно своите права. Освен другото, информацията трябва да бъде предоставяна на субекта на данни в лесно разбираем вид и език, а когато е възможно, и чрез подходящи, стандартизирани „икони".

Администратора ще осигурява поддръжка на субекта на данни безплатно, освен ако се получават многократно повтарящи се запитвания. Субекта на данни може да има промяна на своите лични данни по различни причини - напр., отказ от предварително дадено съгласие – вкл., тяхното изтриване. Ако администратора разкрива данните, то той трябва да оповести всяко искане за изтриване, корекция и премахване на връзките към информацията на страната (организацията) пред която се разкрива информацията.
Ако информацията е некоректна или незаконна, субекта на данни може да се възползва от правото си за предявяване на претенции (несъгласие), свързани с ограничаване на обработките на данни.
Субекта на данни трябва да има правото да получи своите лични данни в структуриран, общоприет машинно четабилен формат. Целта на това право е да позволи на субекта на данни да предостави своите лични данни на друг администратор. Субекта на данни има и правото да изисква администратора да предостави неговите лични данни на нов администратор.

Субекта на данни има право да НЕ бъда „профилиран". Профилирането може да се извършва само, когато е основано на изпълнение на договор; когато е разрешено по правен път или когато субекта на данни е дал изрично съгласие. Съгласието може да бъде дадено и за цели на маркетинга.

По собствена инициатива, администратора трябва да информира субекта на данни за обработките и съответните операции. Ако администратора получава личните данни директно от субекта на данни, обработващия данни трябва да информира за следното:

• идентификация на администратора и информация за контакт с него(вкл., за Служителя по защита на личните данни – ако е приложимо);
• целта и правните основания за извършване на обработките;
• категориите получатели, имащи достъп за обработване на информацията;
• има ли трансфер на данни към трета страна;
• период на обработката;
• права за изтриване или корекция на лични данни;
• права за несъгласие и ограничаване на обработката на данни;
• възможност за преносимост на данните;
• възможност за отказ от съгласие;

• възможност за оплакване на надзорен орган;
• дали, личните данни се обработват на основание част от договор;
• дали обработката е част от автоматизирана обработка за вземане на решения, базирани на информацията (профилинг);
• дали информацията се обработвеа за нови цели;

Ако информацията се събира от трета страна, администратора трябва да информира субекта на данни кои категории лични данни ще бъда обработване и от какви източници постъпва информацията за него.

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