**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.Принципи за обработка на личните данни

Необходимо е организацията да определи, дали ще обработва личните данни, в съответствие със съответните принципи в GDPR

### 1.1Общи въпроси

• Организацията ще изпълнява ли принципите за обработка на личните данни ?
• Обработките на личните данни пропорционални ли са на целите на тези обработки (изисква ли се тяхното изпълнение) ?
• Възможно ли е организацията да използва по-малко „агресивни / натрапчиви“ начини за работа с личните данни (вкл. за събиране на данни) и пак да постигне поставените цели на обработките ?

### 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.5 (принципи)<br><br>**Организацията трябва да определи кои лични данни ще обработва и по какъв начин ще се извършва обработката** | A.8.2.3 (работа с активи)<br><br>**Контрол**<br><br>Трябва да бъдат **разработени и приложени процедури** за работа с активи в съответствие с класификационната схема на информацията, приета от организацията. | Няма допълнителен контрол |

| | | |
|---|---|---|
| Чл.5 (1) (законосъобразност, безпристрастност и прозрачност)<br>Чл.6 (1), „a“ (съгласие)<br>Чл.7(съгласие)<br>Чл.8(съгласие за деца)<br>Чл.9( 2) „a“ (съгласие)<br><br>**Ако за съответната обработка има правно основание, под формата на съгласие, то това съгласие трябва да бъде документирано** | A.18.1.4 (съответствие с тайната и защитата на информацията за самоличността)<br><br>**Контрол**<br>Трябва да бъде осигурена тайната и защитата на информацията за самоличността според изискванията на съответните нормативни актове и регламенти, където са приложими.<br><br>A.12.1.1 (документирани процедури за работа)<br><br>**Контрол**<br>Процедурите за работа трябва да бъдат документирани и достъпни за всички потребители, които се нуждаят от тях. | A.11 (съответствие с тайната на информацията за самоличността)<br><br>A.11.1 Географско разположение на информация за самоличността<br><br>**Контрол**<br>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.<br><br>A.11.2 Планирани места за получаване на информация за самоличността<br><br>**Контрол**<br>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.5 (1) (законосъобразност, безпристрастност и прозрачност)<br>Чл.6 (1), „f“ (легитимни интереси)<br><br>**Ако съответната обработка е базирана на принципа за баланс на интереси между легитимните интереси на организацията (администратор) и интересите на субекта на данни за защита на личните данни, то този баланс трябва да бъде изрично документиран**. | A.18.1.4 (съответствие с тайната и защитата на информацията за самоличността)<br><br>**Контрол**<br>Трябва да бъде осигурена тайната и защитата на информацията за самоличността според изискванията на съответните нормативни актове и регламенти, където са приложими.<br><br>A.12.1.1 (документирани процедури за работа)<br><br>**Контрол**<br>Процедурите за работа трябва да бъдат документирани и достъпни за всички потребители, които се нуждаят от тях. | A.11 (съответствие с тайната на информацията за самоличността)<br><br>A.11.1 Географско разположение на информация за самоличността<br><br>**Контрол**<br>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.<br><br>A.11.2 Планирани места за получаване на информация за самоличността<br><br>**Контрол**<br>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.5 (1) (законосъобразност, безпристрастност и прозрачност)<br>Чл.6 (1), „b“ (договор) и „c“ (правни задължения)<br><br>**Ако съответната обработка на лични данни се основава на договор или на правни задължения, тези обстоятелства трябва да бъдат документирани.** | A.18.1.4 (съответствие с тайната и защитата на информацията за самоличността)<br><br>**Контрол**<br>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)<br><br>A.11.1 Географско разположение на информация за самоличността<br><br>**Контрол**<br>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.<br><br>A.11.2 Планирани места за получаване на |

| | | |
|---|---|---|
| | | информация за самоличността<br><br>**Контрол**<br>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.5 (1) (законосъобразност, безпристрастност и прозрачност)<br>Чл.6 (законосъобразност на обработката)<br>Чл.9 (чувствителна информация)<br>Чл. 85 (обработване и свобода на изразяването и и информация – за челите на журналистиката, летуратурата, актьорското майсторство и академизма)<br>Чл.86 (обществен достъп до до официални документи)<br>87 (национални идентификационни номера)<br>Чл. 88 (трудово-правни отношения)<br>Чл. 89 (обществен интерес, наука, история и статистика)<br>Чл. 90 (тайна)<br><br>**Организацията трябва да документира правните основания за извършване на обработка на съответните категории лични данни.** | A.18.1.4 (съответствие с тайната и защитата на информацията за самоличността)<br><br>**Контрол**<br>Трябва да бъде осигурена тайната и защитата на информацията за самоличността според изискванията на съответните нормативни актове и регламенти, където са приложими.<br><br>A.12.1.1 (документирани процедури за работа)<br><br>**Контрол**<br>Процедурите за работа трябва да бъдат документирани и достъпни за всички потребители, които се нуждаят от тях. | A.11 (съответствие с тайната на информацията за самоличността)<br><br>A.11.1 Географско разположение на информация за самоличността<br><br>**Контрол**<br>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.<br><br>A.11.2 Планирани места за получаване на информация за самоличността<br><br>**Контрол**<br>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.5 (1) (законосъобразност, безпристрастност и прозрачност)<br><br>**Организацията трябва осигури прозрачност и пропорционалност (на целите на обработките) на обработките на лични данни** | A.18.1.4 (съответствие с тайната и защитата на информацията за самоличността)<br><br>**Контрол**<br>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)<br><br>A.11.1 Географско разположение на информация за самоличността<br><br>**Контрол**<br>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.<br><br>A.11.2 Планирани места за получаване на информация за самоличността |

| | | |
|---|---|---|
| | | **Контрол**<br>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.5 (1) (законосъобразност, безпристрастност и прозрачност)<br><br>**Организацията трябва осигури прозрачност на обработките на лични данни** | A.18.1.4 (съответствие с тайната и защитата на информацията за самоличността)<br><br>**Контрол**<br>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)<br><br>A.11.1 Географско разположение на информация за самоличността<br><br>**Контрол**<br>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.<br><br>A.11.2 Планирани места за получаване на информация за самоличността<br><br>**Контрол**<br>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.5 (1) “в“ (ограничение на целите)<br><br>**Организацията трябва да осигури, че обработките са ограничени до определените, изключителните (специалните) и легитимните цели.** | A.18.1.4 (съответствие с тайната и защитата на информацията за самоличността)<br><br>**Контрол**<br>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)<br><br>A.11.1 Географско разположение на информация за самоличността<br><br>**Контрол**<br>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.<br><br>A.11.2 Планирани места за получаване на информация за самоличността<br><br>**Контрол**<br>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.5 (1) “в“ (ограничение на целите)<br><br>**Организацията трябва да осигури, че обработките няма да се извършват за несъвместими цели.** | A.18.1.4 (съответствие с тайната и защитата на информацията за самоличността)<br><br>**Контрол**<br>Трябва да бъде осигурена тайната и защитата на информацията за самоличността според изискванията на съответните нормативни актове и | A.11 (съответствие с тайната на информацията за самоличността)<br><br>A.11.1 Географско разположение на информация за самоличността<br><br>**Контрол**<br>Организациите поддържащи (оператор) публичен „облак“ и изпълняващи обработка |

| | | |
|---|---|---|
| | 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.<br><br>A.11.2 Планирани места за получаване на информация за самоличността<br><br>**Контрол**<br>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.5 (1) "c" (минимизация на данните)<br><br>**Организацията трябва да осигури, че ще се извършват само обработки, които отговарят и са ограничени единствено и само за постигане на техните цели. Включително, че целите не могат да се постигнат с по-малко „натрапчиви " методи и операции.**<br><br>**Забележка:** Под „натрапчиви" може да се разбира досадни / обезпокоителни методи и операции, насочени към субекта на лични данни. | A.18.1.4 (съответствие с тайната и защитата на информацията за самоличността)<br><br>**Контрол**<br>Трябва да бъде осигурена тайната и защитата на информацията за самоличността според изискванията на съответните нормативни актове и регламенти, където са приложими.<br><br>A.12.1.1 (документирани процедури за работа)<br><br>**Контрол**<br>Процедурите за работа трябва да бъдат документирани и достъпни за всички потребители, които се нуждаят от тях. | A.11 (съответствие с тайната на информацията за самоличността)<br><br>A.11.1 Географско разположение на информация за самоличността<br><br>**Контрол**<br>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.<br><br>A.11.2 Планирани места за получаване на информация за самоличността<br><br>**Контрол**<br>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.1(1) „d" (точност – виж и Чл.16 - 21)<br><br>**Организацията трябва да осигури точност и актуалност на личните данни с които работи.** | A.12.1.1 (документирани процедури за работа)<br><br>**Контрол**<br>Процедурите за работа трябва да бъдат документирани и достъпни за всички потребители, които се нуждаят от тях. | Няма допълнителен контрол |
| Чл.1(1) „d" (точност – виж и Чл.16 – 21)<br><br>**Организацията трябва да осигури, че некоректните лични данни са изтрити или коригирани.** | A.12.1.1 (документирани процедури за работа)<br><br>**Контрол**<br>Процедурите за работа трябва да бъдат документирани и достъпни за всички потребители, които се нуждаят от тях. | Няма допълнителен контрол |
| Член 5(1) „e" (ограничения при съхраняването на лични данни)<br><br>**Организацията трябва да** | A.12.1.1 (документирани процедури за работа)<br><br>**Контрол**<br>Процедурите за работа трябва да | Няма допълнителен контрол |

| | | |
|---|---|---|
| **осигури, че личните данни се съхраняват по начин, позволяващ възможност за тяхното използване за идентифициране на субект на данни, за период от време, не по-дълъг от необходимия, за изпълнение целите на обработката.** | бъдат документирани и достъпни за всички потребители, които се нуждаят от тях. | |
| Член 5(1) „e“ (ограничения при съхраняването на лични данни)<br><br>**Организацията трябва за внедри съответните технически и организационни мерки (контроли) за сигурност, така, че личните данни да бъдат обработвани законосъобразно, с гарантирана степен на конфиденциалност, цялостност, наличности и устойчивост, без загуба, увреждане и/или разрушаване. (мерките за сигурност на личните данни са описани в следваща част на ОР, свързана със задълженията на организациите по сигурността на личните данни)** | A.12.1.1 (документирани процедури за работа)<br><br>**Контрол**<br>Процедурите за работа трябва да бъдат документирани и достъпни за всички потребители, които се нуждаят от тях. | Няма допълнителен контрол |
| Член 5(1) „f“ (конфиденциалност и цялостност на личните данни – виж също чл. 32)<br><br>**Организацията трябва за внедри съответните технически и организационни мерки (контроли) за сигурност, така, че личните данни да бъдат обработвани законосъобразно, с гарантирана степен на конфиденциалност, цялостност, наличности и устойчивост, без загуба, увреждане и/или разрушаване. (мерките за сигурност на личните данни са описани в** | A.5.1.1 (политики за информационна сигурност)<br><br>**Контрол**<br>Трябва да бъде определен набор от политики за сигурност на информацията, одобрен от ръководството, разпространен и разгласен на всички служители и съответните външни страни.<br><br>A.6.1.5 (информационната сигурност при управлението на проекти)<br><br>**Контрол**<br>Независимо от вида на проекта трябва да бъде отчетена сигурността на информацията при управление на проекти.<br><br>A.14.1.1 (анализ на изискванията за | Няма допълнителен контрол |

| | | |
|---|---|---|
| **следваща част на ОР, свързана със задълженията на организациите по сигурността на личните данни)** | сигурност и спецификации)<br><br>**Контрол**<br>Изискванията, имащи отношение към сигурността на информацията, трябва да бъдат включени в изискванията за нови информационни системи или подобряване на съществуващи информационни системи.<br><br>A.14.2.5 (принципи за сигурност при системното инженерство)<br><br>**Контрол**<br>Инженерни принципи за сигурни системи трябва да бъдат създадени, документирани, поддържани и приложени при всеки опит за реализиране на информационна система. | |

**Препоръки за изпълнение на изискванията по чл.5 (за всички позиции, описани в горната таблица)**

Организацията, администратор на лични данни е в правото си да реши какви обработки ще използва, отчитайки техните цели.Отговорността за обработките е на администратора на лични данни. Целта на обработките трябва да бъде ясно и точно определена, и документирана, без ненужни допълнителни разяснения.

Организацията, администратор на лични данни трябва да има и представя доказателства за правните основания за извършване на обработките. Как ще бъде документирано това, е решение на администратора. Ако администратора има намерение да използва личните данни за друга цел, то е необходимо да се оцени съвместимостта на двете цели. Това се извършва чрез оценка на взаимовръзките между двете цели; връзките между администратора и субекта на данни; чувствителността на данните; възможните последствия за субекта на данни; мерките за сигурност; и дали субекта на данни трябва да бъде информиран. Когато се извършва обработка, тя трябва да се ограничава до степен, която осигурява честно и безпристрастни отношение към субекта на данни. Това означава,че субекта на данни трябва да бъде информиран и да има възможност да се възползва от правата си, в пълен обем.

Администратора трябва да осигури прозрачност на обработките. Това може да се осъществи, като на субекта на данни се предостави информация за идентичността на администратора и за контакти с него; за целите на обработките; за правните основания; за възможното предаване на лични данни към трети страни; за периода на обработване; за профилирането (ако се извършва); за правата на субекта на данни. Тази информация трябва да се представи по ясен, четабилен начин или чрез стандартизирани „икони“.

Обработката на личните данни трябва да бъде точна и обновявана, като некоректната информация трябва да бъде изтривана или коригирана. Няма необходимост за редактиране на личните данни, ако за тях не са планирани допълнителни обработки; изтриването на личните данни трябва да се извършва само, когато това е необходимо. В много случаи грешните лични данни не трябва да бъдат изтривани, вместо това те могат да се коригират и това да бъде оповестено по подходящ начин.

Личните данни могат да бъдат изтривани, когато целите за тяхната обработка са постигнати. Освен

изтриване, личните данни могат да бъдат **анонимизирани,** като при този случай, организацията трябва да осигури, че не е възможно на практика отново да се идентифицира субекта на данни.

Организациите могат да внедрят адекватни мерки за защита на личните данни (на тяхната конфиденциналност, цялостност и наличност), така, както е описано в ISO 27001 / 27002 / 27018. В допълнение, самите ИТ системи, обработващи лични данни, трябва да има висока устойчивост на външни и вътрешни кибер атаки. Може, с голяма степен на увереност да се приеме, че тази устойчивост може да бъде постигната изпълнявайки изискванията на ISO 27001 и препоръките на ISO 27002 и ISO 27018.
Всички мерки за сигурност, които се внедряват за защита на личните данни, **трябва да са резултат от провеждането на оценка и анализ на риска.** Приложените мерки за сигурност трябва да бъдат периодично тествани, като осигуряват и възможност за възстановяване в случай на пробиви в сигурността.

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