Принципи на обработката на лични данни и законосъобразност на процеса

1. **Кога личните данни се обработват в съответствие с Регламента?**

- Законосъобразно, добросъвестно и по прозрачен начин (законосъобразност, добросъвестност и прозрачност);
- Изрично указани, легитимни цели. Всяко вторично обработване не може да е несъвместимо с първоначалните цели (ограничение по цели);
- Подходящи, свързани и ограничени до необходимите данни (сведени до минимум);
- Точни и при необходимост поддържани в актуално състояние (точност);
- Обработвани за не по дълъг период за постигане на целите (ограничение на съхранението);
- Обработвани при използване на подходящи технически и организационни мерки (цялостност и поверителност);
- Администраторът следва да може да докаже спазването на всеки принцип (отчетност).
- ЗАКОНОСЪОБРАЗНОСТ

2. **Обработването е законосъобразно, само ако и доколкото е приложимо поне едно от следните условия:**

- съгласие за обработване на личните му данни за една или повече конкретни цели;
- обработването е необходимо за изпълнението на договор, по който субектът на данните е страна, или за предприемане на стъпки по искане на субекта на данните преди сключването на договор;
- обработването е необходимо за спазването на законово задължение, което се прилага спрямо администратора;
- обработването е необходимо, за да бъдат защитени жизненоважните интереси на субекта на данните или на друго физическо лице;
- обработването е необходимо за изпълнението на задача от обществен интерес или при упражняването на официални правомощия, които са предоставени на администратора;
- обработването е необходимо за целите на легитимните интереси на администратора или на трета страна, освен когато пред такива интереси преимущество имат интересите или основните права и свободи на субекта на данните, които изискват защита на личните данни, по-специално когато субектът на данните е дете.

- ЗАКОНОСЪОБРАЗНОСТ ПОСТИГНАТО СЪС **СЪГЛАСИЕ**

3. **В случай че администраторът реши да обработва данните на това основание, той следва да е в състояние да докаже, че съгласието е:**
   - свободно изразено – не е дадено под натиск или заплаха от неблагоприятни последици (напр. по-висока цена на услуга);
   - конкретно – отделно съгласие за всяка конкретно определена цел, а когато е относимо - и за конкретна категория лични данни;
   - информирано – дадено на основата на пълна, точна и лесно разбираема информация;
   - недвусмислено – не се извлича или предполага въз основа на други изявления или действия на лицето;
   - дадено с активно действие: чрез изрично изявление или ясно потвърждаващо действие, вкл. онлайн. Мълчанието на лицето или предварително отметнати квадратчета за съгласие не могат да се приемат за валидно съгласие.

4. **Съгласие на дете във връзка с услуги на информационното общество**

- При събиране на съгласие във връзка с прякото предлагане на услуги на информационното общество на деца, обработването на данни на дете е законосъобразно, ако детето е поне на 16 години. Ако детето е под 16 години това обработване е законосъобразно само ако и доколкото такова съгласие е дадено или разрешено от носещия родителска отговорност за детето.
- В такива случаи администраторът полага разумни усилия за удостоверяване, че съгласието е дадено или разрешено от носещия родителска отговорност за детето, като взема предвид наличната технология.
- На децата се полага специална защита на личните данни, тъй като те не познават достатъчно добре съответните рискове, последици и гаранции, както и своите права, свързани с обработването на лични данни:
  - използването на лични данни на деца за целите на маркетинга;
  - създаване на личностни или потребителски профили и събирането на лични данни по отношение на деца при ползване на услуги, предоставяни пряко на деца.
- Съгласието на носещия родителска отговорност **не следва да е необходимо** в контекста на пряко предлаганите на деца услуги за превенция и консултиране.
- Обработване на специални категории данни

- **Забранява се обработването на лични данни и не се прилага, ако е налице едно от следните условия:**
- изрично съгласие за обработването на тези лични данни;
- обработването е необходимо за упражняването на специалните права на администратора или на субекта на данните по силата на трудовото право и правото в областта на социалната сигурност и социалната закрила;
- за да бъдат защитени жизненоважните интереси на субекта на данните когато физически или юридически не е способен да даде своето съгласие;
- обработването се извършва при подходящи гаранции в хода на законните дейности на фондация, сдружение или друга структура с нестопанска цел, с политическа, философска, религиозна или синдикална цел, при условие че обработването е свързано единствено с членовете или бившите членове на тази структура или с лица, които поддържат редовни контакти с нея във връзка с нейните цели, и че личните данни не се разкриват без съгласието на субектите на данните;
- обработването е свързано с лични данни, които явно са направени обществено достояние от субекта на данните;
- когато съдилищата действат в качеството си на правораздаващи органи;
- важен обществен интерес което е пропорционално на преследваната цел, зачита същността на правото на защита на данните и предвижда подходящи и конкретни мерки за защита на основните права и интересите на субекта на данните;
- за целите на превантивната или трудовата медицина, за оценка на трудоспособността на служителя, медицинската диагноза, осигуряването на здравни или социални грижи или лечение, или за целите на управлението на услугите и системите за здравеопазване или социални грижи;
- обработването е необходимо от съображения от обществен интерес в областта на общественото здраве, като зачита същността на правото на защита на данните и предвижда подходящи и конкретни мерки за защита на основните права и интересите на субекта на данните;
- обработването е необходимо за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели, зачита същността на правото на защита на данните и предвижда подходящи и конкретни мерки за защита на основните права и интересите на субекта на данните.

5. **Законосъобразност, базирана на договор или нормативен акт**
   - Обработването на данни следва да е законосъобразно, когато то е необходимо в контекста на договор или при намерение за сключване на договор;
   - Когато обработването се извършва в съответствие с правно задължение, наложено на администратора на лични данни или при упражняване на официални правомощия, за обработването следва да има основание в **правото на Съюза или в правото на държава членка**;
   - Правото на Съюза или на държава членка следва да определя също и целта на обработването;
   - в това право биха могли да се посочат още:
     - спецификациите за определянето на администратора на лични данни;
     - видът данни, които подлежат на обработване;
     - съответните субекти на лични данни;
     - образуванията, пред които могат да бъдат разкривани лични данни;
     - ограниченията по отношение на целите;
     - периодът на съхранение и други мерки за гарантиране на законосъобразното и добросъвестно обработване;
     - дали обработката се извършва само от публичен орган.

6. **Законосъобразност базирана на защита на лицето**
   - Обработването на лични данни следва да се счита за законосъобразно и когато е необходимо, за да се защити интерес от първостепенно значение за живота на субекта на данните или на друго физическо лице.
   - Обработването на лични данни единствено въз основа на жизненоважен интерес на друго физическо лице следва да се състои по принцип, **само когато обработването не може явно да се базира на друго правно основание**.
   - Някои видове обработване могат да обслужват както важни области от обществен интерес, така и жизненоважните интереси на субекта на данните, например когато обработването е необходимо за хуманитарни цели, включително за наблюдение на епидемии и тяхното разпространение или при спешни хуманитарни ситуации, по-специално в случай на природни или причинени от човека бедствия.
   -

7. **Законосъобразност, базирана на преобладаващ интерес**
   - Законните интереси на даден администратор, включително на администратор, пред когото може да бъдат разкрити лични данни, или на трета страна могат да предоставят правно основание за обработването, **при условие че интересите или основните права и свободи на съответния субект на данни нямат преимущество**, като се вземат предвид основателните очаквания на субектите на данни въз основа на техните взаимоотношения с администратора.
   - Такъв законен интерес може да е налице, когато:
     - между субекта на данни и администратора на лични данни съществува съответното определено взаимоотношение - субектът на данни е клиент или подчинен на администратора на лични данни.
     - обработването на лични данни за целите на директния маркетинг може да се разглежда като осъществявано поради законен интерес
     - обработването на лични данни, строго необходимо за целите на предотвратяването на измами, също представлява законен интерес на съответния администратор на данни.
     - предоставяне на данни в рамките на група предприятия, при спазване на мерките за защита
     - При всички случаи, за установяването на законен интерес би била необходима внимателна преценка, включително дали субектът на данни може по времето и в контекста на събирането на данни основателно да очаква, че може да се осъществи обработване на личните данни за тази цел.
   - Интересите и основните права на субекта на данни биха могли по-конкретно да имат преимущество пред интереса на администратора, когато личните данни се обработват при обстоятелства, при които субектите на данни основателно не очакват по-нататъшна обработка.
   - Това правно основание **не следва да се прилага спрямо обработването на данни от публичните органи** при изпълнението на техните задачи.

8. **Обработка за конкретни цели. Обработка на данни за цели различни от първоначално обявената**
   - Обработването на лични данни за цели, различни от тези, за които първоначално са събрани личните данни, следва да бъде разрешено

единствено когато обработването е съвместимо с целите, за които първоначално са събрани личните данни;

- Ако обработването е необходимо за изпълнението на задача от обществен интерес или свързана с упражняването на официални правомощия, в правото на Съюза или в правото на държава членка могат да бъдат определени и уточнени задачите и целите, за които по-нататъшното обработване следва да се счита за съвместимо и законосъобразно;
- По-нататъшното обработване за целите на архивирането в обществен интерес, за целите на научни или исторически изследвания, или за статистически цели следва да се разглежда като съвместими законосъобразни операции по обработване;
- Когато **субектът на данните е дал съгласието** си или за да се гарантират по-специално важни цели от широк обществен интерес, на администратора следва да се позволи да обработва по-нататък личните данни, независимо от съвместимостта на целите;
- Във всеки случай, прилагането на принципите и по-специално информирането на субекта на данните относно тези други цели и относно неговите права, включително правото да възрази, следва да бъдат гарантирани;

9. Точност и актуалност на обработката Минималност на обработваните данни

- точни и при необходимост да бъдат поддържани в актуален вид;
- трябва да се предприемат всички разумни мерки, за да се гарантира своевременното изтриване или коригиране на неточни лични данни, като се имат предвид целите, за които те се обработват („точност“);
- подходящи, свързани със и ограничени до необходимото във връзка с целите, за които се обработват („свеждане на данните до минимум“);
    - Определяне на минималното количество необходими данни е елемент на прилагането на принципа „неприкосновеност при проектиране”;
    - Определянето на минималното количество необходими данни е елемент и на организационните мерки за защита

10. Осигуряване на адекватно ниво на сигурност

- Администраторите се подчиняват на едно и също законодателство – разположени на територията на ЕС;
- По силата на договор са договорили ниво на защита съответстващо на Общия регламент;

- Организациите спазват стандартни договорни клаузи, утвърдени от Европейската Комисия;
- Подчиняват се на правила в рамките на група предприятия, утвърдени от един надзорен орган на страна членка на ЕС;
- Сертифицирани са по утвърдени от Комитета за защита на данни критерии;
- Признават един и същ етичен кодекс, утвърден от Комитета по защита на данните;
- Подчиняват се на правила утвърдени от Европейската комисия – Privacy Shield;
- трети страни, които според Европейската комисия предоставят адекватно ниво на защита – Швейцария, Аржентина, Нова Зеландия

11. Отчетност

- Спазването на всички принципи за допустимост на обработката на лични данни може да бъде оценена по следните показатели:
- Управленска структура;
- Преглед на личните данни;
- Политики за неприкосновеност на данните;

12. Прилагане на защитата при обработката;

- Програма за обучение;
- Управление на риска за информационната сигурност;
- Управление на риска от трети страни;
- Уведомления при пробив в системата;
- Поддържане процедури за запитвания и жалби;
- Мониторинг за нови оперативни практики;
- Програма за управление на нарушенията;
- Мониторинг на процедурите за обработване;
- Следене на външните критерии

13. Прилагане на защитата на личните данни при обработката
Поддържа оперативни политики и процедури в съответствие с политиката за поверителност

- Поддържане на политики/процедури за събирането и използването на чувствителни лични данни (включително биометрични данни);
- Поддържане на политики/процедури за поддържане на качеството на данните;
- Поддържане на политики/процедури за анонимизация на лични данни

- Поддържане на политики/процедури за преглеждане на дейностите по обработка на лични данни, извършени изцяло или частично чрез автоматизирани средства;
- Поддържане на политики/процедури за повторна (вторична, secondary) употреба на личните данни;
- Поддържане на политики/процедури за събиране на информираното (предпочитаното) съгласие;
- Поддържане на политики/процедури, предназначени за унищожаване на личните данни;
- Интегриране на защитата на личните данни в използването на бисквитки (cookies) и механизми за проследяване;
- Интегриране на защитата на личните данни в записите за практики на задържане на данните;
- Интегриране на защитата на личните данни в практиките за директен маркетинг;
- Интегриране на поверителността на данните в практиките за маркетинг по електронната поща
- Интегриране на защитата на личните данни в практиките за телемаркетинг
- Интегриране на защитата на личните данни в практиките за поведенческата реклама
- Интегриране на защитата на личните данни в практиките за наемането
- Интегриране на защитата на личните данни в практиките за проверка (проучване) на служителите
- Интегриране на защитата на личните данни в социалните медийни практики
- Интегриране на защитата на личните данни в политиките/процедурите за защита на вашите собствени мобилни (носими) устройства (Bring Your Own Device, BYOD)
- Интегриране на поверителността на личните данни в практиките за здравето и безопасността
- Интегриране на защитата на личните данни в взаимодействия с профсъюзните организации (работническите съвети) (works councils)
- Интегриране на защитата на личните данни в практики за мониторинг на служителите