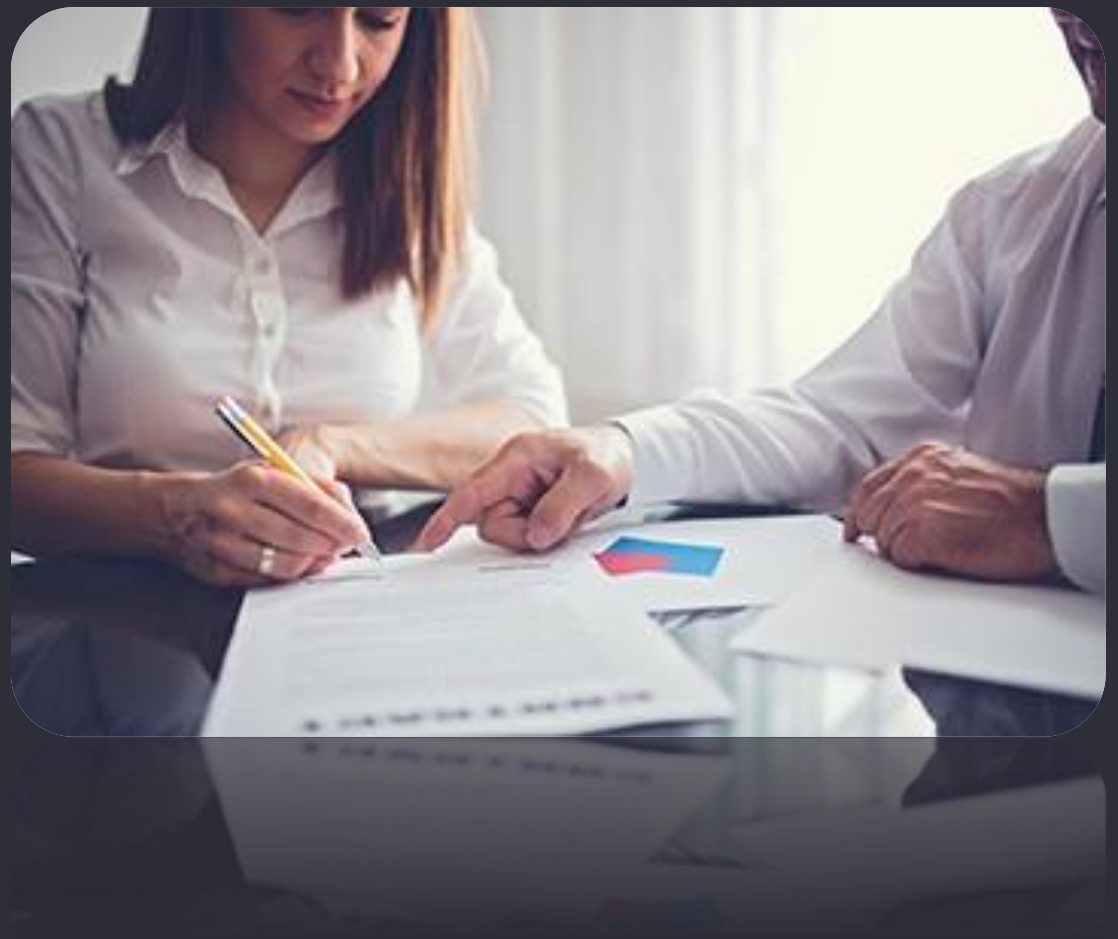
Модул 2

Новите промени в ролите и отговорностите на администраторите на данни и обработващите данни



Written by

Концепцията за „администратор“

1. Администраторът на данни е физически или юридическо лице, публичен орган, агенция или друг орган, който сам или съвместно с други определя целите и средствата за обработка на лични данни.

2. Ключовата роля на администратора е да определя целите, за които личните данни се събират, съхраняват, използват, променят и разкриват

3. Администратор на данни може да бъде юридическо или физическо лице. Въпреки широкия характер на дефиницията кой може да бъде администратор на данни, трябва да се даде приоритет администраторът да се счита за компанията или органа като такъв, а не за физическо лице, назначено от компанията или органа.

4. Съвместните администратори трябва да определят съответните си отговорности за спазване на GDPR по прозрачен начин.За по-нататъшна защита на лицата, от съвместните администратори се изисква да предоставят „същността на споразумението“ на разположение на субектите на данни. Субектите на данни могат да упражняват правата си съгласно GDPR по отношение на и срещу всеки от администраторите.

5. Администраторът може да делегира решения от техническите и организационните аспекти на обработката на обработващия, при условие че запазва най-важните решения за цели или средства за себе си.

Становище 1/2010 & Насоки 07/2020

- **Контрол, произтичащ от изрична правна компетентност**
- **Контрол, произтичащ от косвена компетентност**
- **Контрол, произтичащ от фактическо влияние**

Концепцията за „администратор“/„съвместен администратор“

Насоки 07/2020

Някои дейности по обработка са естествено свързани с ролите или дейностите на предприятието (например поради традиционните роли на професионален опит), което налага отговорности

Обработката се отнася до вашите отношения със субектите на данни като служители, клиенти, членове и т.н.

Не е необходимо администраторът да има достъп до обработваните данни. Две страни, едната от които няма такъв достъп, могат да бъдат съвместни администратори
CJEU, C-25/17, Свидетели на Йехова

Две страни, които нямат една и съща цел за обработката, могат да бъдат съвместни контрольори, ако преследваните цели са тясно свързани/допълващи се
CJEU, C-40/17, Fashion IDCJEU, C-210/16, Wirtschaftsakademie

Простото съществуване на взаимна изгода

Просто използване на обща система/инфраструктура за обработка на данни

Просто последователно обработване на едни и същи лични данни във верига от операции

Условията на договора могат да помогнат, но НЕ винаги са решаващи

Концепцията за „обработващ“

01

GDPR определя обработващия като „физическо или юридическо лице, публичен орган, агенция или друг орган, който обработва лични данни от името на администратора“.

02

Съществуването на обработващ на данни зависи от решението на администратора да делегира ялата или част от дейността по обработване на външна организация или физическо лице. Ролята на обработващия произтича от конкретните дейности на организацията в конкретен контекст.

03

Обработващ, който надхвърля мандата си и решава целите или основните средства на обработване, се счита за администратор по отношение на тази обработка.

Насоки 07/2020: може да вземе решение за „несъществени средства“

04

GDPR изисква обработващия лични данни да ги обработва само по указания на администратора чрез договор или задължителен правен акт, регулиращ отношенията между администратора и обработващия лични данни, който да бъде сключен в писмена форма.

Най-добри практики при договаряне на реда и условията на отношенията между администратор и администратор

- Договор или друг правен акт съгласно законодателството на ЕС или на държава-членка, който е в писмена форма, включително в електронна форма, който е обвързващ;
- Определяне на съответните отговорности по отношение на:

- упражняването на правата и задълженията на субектите на данни за предоставяне на информация;
- общи принципи за защита на данните;
- правно основание;
- мерки за сигурност;
- оценки на въздействието върху защитата на данните;
- използване на лица, обработващи личните данни;
- обмен с трети държави;
- контакти със субекти на данни и надзорни органи, вкл. задължение за уведомяване за разкриване на данните.

Най-добри практики при договаряне на реда и условията на отношенията между администратор и обработващ (1)

- **Договор или друг правен акт, който е в писмена форма, включително в електронна форма, и е задължителен.**

- **Не представяйте само разпоредбите на GDPR! Трябва да предоставите подробна информация за:**

- предмета, продължителността и естеството на обработката;
- вида на личните данни, които ще бъдат обработвани, и категориите субекти на данни;
- правата и задълженията на администратора (вкл. да извършва проверки и одити);

Не трябва да се налагат ограничения на одиторските права на администратора в рамките на споразумението по чл. 28 от GDPR!

- правата и задълженията на обработващия (вкл. задължението да обработва данни по нареждане на администратора, за да се гарантира, че само лица, гарантиращи поверителност, ще бъдат упълномощени да обработват личните данни, да предприемат подходящи технически и организационни мерки);
- необходимо ниво на сигурност;

Най-добри практики при договаряне на реда и условията на отношенията между администратор и обработващ

- **Не забравяйте да уточните:**

- начина, по който обработващият лични данни ще подпомага администратора при изпълнението на неговите задължения по GDPR;
- конкретна времева рамка за уведомяване на администратора за разкриване на данни;
- за обработващи - избор между общи и конкретни предварителни писмени упълномощения;
- дали предаването на данни извън ЕС/ЕИП е разрешено или забранено;
- възможност за промяна на избора дали данните, обработвани от обработващия, да бъдат изтрити или възстановени.

- **Кодекс на поведение.**

Как да изберем нашия обработващ лични данни (1)

- **Използвайте само обработващи, които дават достатъчни гаранции за прилагане на подходящи технически и организационни мерки.**

- **Елементи, които трябва да се имат предвид при оценката на риска:**

- експертните познания на обработващия (напр. технически опит по отношение на мерките за сигурност и нарушения на данните);
- надеждността на обработващия;
- възможностите на обработващия;
- оценктата и репутацията на обработващия на пазара; и
- спазването на обработващия на одобрен кодекс за поведение или механизъм за сертифициране.

20 май 2021 г.: Кодексите за поведение, одобрени от EDPB за доставчиците на облачни инфраструктурни услуги в Европа - вече имат абонати.

Да не се използва в контекста на международен пренос на лични данни.

Как да изберем нашия обработващ лични данни (2)

- **Изискайте съответната документация:**
- политика за поверителност,
- условия за ползване,
- запис на дейностите по обработка,
- политика на управление,
- политика за сигурност на информацията,
- доклади за външни одити,
- признати международни сертификати, като серия ISO 27000).

N.B.! Дисбалансът във възможностите на малък администратор на данни по отношение на големите доставчици на услуги не е оправдание за приемане на условията на GDPR!