Европейска комисия

Седем стъпки за подготовка

на дружествата за Общия регламент относно защитата на данните

Правосъдие и потребители

За кого се отнася това ръководство?

Това ръководство има за цел да помогне на онези дружества, които не обработват лични данни като основна бизнес дейност, като например МСП, които основно обработват само личните данни на своите служители или списъци на клиенти. Това включва например търговци или магазини, като хлебарници или месарници, или доставчици на услуги, като архитекти. В това ръководство се посочват стъпките, които трябва да предприемете, за да се подготвите за ОРЗД.

Лични данни са всяка информация, свързана с действително съществуващо живо физическо лице (а не с юридическо лице). Това включва например: собствено име, фамилия, домашен адрес, имейл адрес или данни за местоположение от картата, показана на вашия мобилен телефон. Обикновено такъв е случаят с данните, които е възможно да съхранявате за вашите служители, клиенти или доставчици.

Колкото по-малък е рискът, който дейностите ви представляват за личните данни, толкова по-малка е вашата отговорност

Прилагане на основните принципи:

- **събиране на лични данни с ясно определена цел, без да се използват за нещо друго** (ако поискате от клиентите си да ви дадат имейлите си, за да могат да получават новите ви оферти или промоции, не можете да използвате тези имейли за нищо друго, нито да ги продавате на друго дружество);
- **не трябва да се събират повече данни от необходимото** (ако правите доставка по домовете, на вас са ви необходими например адреса и името, посочено на звънеца, и не е нужно да знаете дали това лице е семейно или не) — просто трябва да вземете под внимание личните данни, които са под ваш контрол.

СТЪПКА 1 — ПРОВЕРЕТЕ ЛИЧНИТЕ ДАННИ, КОИТО СЪБИРАТЕ И ОБРАБОТВАТЕ, ЦЕЛИТЕ, ЗА КОИТО ГО ПРАВИТЕ, И НА КАКВО ПРАВНО ОСНОВАНИЕ

Имате **служители**; обработвате личните им данни въз основа на трудовия договор и въз основа на правни задължения (напр. изготвяне на отчет за данъчните власти/социалната система).

Можете да управлявате списък **с отделни клиенти**, за да им изпращате например известие за специални оферти/реклами, ако сте получили съгласие от тези клиенти.

Не винаги се нуждаете от съгласие. Има случаи, когато физическите лица ще очакват да обработвате данните им. Например като търговец на пици можете да обработвате адреса за доставка, за да рекламирате един от новите си продукти. Това се нарича законен интерес. Трябва да информирате физическите лица за намерението си и да преустановите обработването на такива данни, ако те поискат това от вас.

Ако управлявате списък с **доставчици** или **бизнес клиенти**, тогава вие правите това въз основа на договорите, които сте сключили с тях. Не е задължително договорите да са в писмена форма.

СТЪПКА 2 — ИНФОРМИРАЙТЕ ВАШИТЕ КЛИЕНТИ, СЛУЖИТЕЛИ И ДРУГИ ФИЗИЧЕСКИ ЛИЦА, КОГАТО СЪБИРАТЕ ЛИЧНИТЕ ИМ ДАННИ

Физическите лица трябва да знаят, че обработвате личните им данни, както и за каква цел.

Но не е необходимо да информирате физическите лица, когато те вече имат информация за това как ще използвате данните им — например когато клиент ви помоли да направите доставка до дома му.

Освен това трябва да информирате физическите лица при поискване от тяхна страна относно личните им данни, които съхранявате, и да им предоставите достъп до тези данни. Поддържайте данните си в изряден вид, така че когато например ваш служител ви попита какъв вид негови лични данни съхранявате, да можете да му ги предоставите лесно и без допълнителни усложнения.

СТЪПКА 3 — СЪХРАНЯВАЙТЕ ЛИЧНИТЕ ДАННИ ТОЛКОВА ДЪЛГО, КОЛКОТО Е НЕОБХОДИМО

Данни за вашите служители: за периода на трудовото правоотношение и свързаните с него правни задължения.

Данни за вашите клиенти: за периода на взаимоотношенията ви с клиентите и свързаните правни задължения (например за данъчни цели).

Изтрийте данните, когато вече не са необходими за целите, за които сте ги събрали.

СТЪПКА 4 — ЗАЩИТЕТЕ ЛИЧНИТЕ ДАННИ, КОИТО ОБРАБОТВАТЕ

Ако съхранявате тези данни в **ИТ система**, ограничете достъпа до файловете, които съдържат данните, напр. с парола. Редовно актуализирайте настройките за защита на вашата система.

(Забележка: ОРЗД не предписва изисквания относно използването на някоя конкретна ИТ система)

Ако съхранявате физически документи с лични данни, тогава се уверете, че те не са достъпни за неупълномощени лица; заключете ги в сейф или шкаф.

СТЪПКА 5 — ВОДЕТЕ ДОКУМЕНТАЦИЯ ЗА ВАШИТЕ ДЕЙНОСТИ, СВЪРЗАНИ С ОБРАБОТВАНЕТО НА ДАННИ

Изгответе кратък документ с обяснение на вида лични данни, които съхранявате, и по какви причини. Може да се наложи да предоставите наличната документация на вашия национален орган за защита на данните при поискване от негова страна.

Тези документи трябва да включват посочената по-долу информация.

ИНФОРМАЦИЯ	ПРИМЕРИ
Цел на обработването на данни	Информиране на клиентите за специални оферти/доставки до дома; плащане на доставчици; заплата и социални осигуровки на служителите
Видове лични данни	Данни за контакт на клиенти; данни за контакт на доставчици; данни на служители
Категории на съответните субекти на данни	Служители; клиенти; доставчици
Категории получатели	Органи по труда; данъчни власти
Периоди на съхранение	Личните данни на служителите — до края на трудовия договор (и свързаните с него правни задължения); личните данни на клиентите — до края на взаимоотношенията с клиента/договорните отношения
Технически и организационни мерки за сигурност за защита на личните данни	Редовно актуализиране на решенията за ИТ системите; заключен шкаф/сейф
Личните данни ще се предават ли на получатели извън ЕС	Използване на обработващ лични данни, който се намира извън ЕС (напр. за съхранение в „облак“)

СТЪПКА 6 — УВЕРЕТЕ СЕ, ЧЕ ВАШИЯТ ПОДИЗПЪЛНИТЕЛ СПАЗВА ПРАВИЛАТА

Ако ще възлагате обработването на лични данни на друго дружество, използвайте само доставчик на услуги, който гарантира обработване в съответствие с изискванията на ОРЗД (например мерки за сигурност). Преди да подпишете договор с дадено дружество, проверете дали то вече е направило съответните промени и корекции съгласно ОРЗД. Прикрепете тази проверка към договора.

СТЪПКА 7 — ПРОВЕРЕТЕ ДАЛИ ПОСОЧЕНИТЕ ПО-ДОЛУ РАЗПОРЕДБИ СЕ ОТНАСЯТ ДО ВАС

> За по-добра защита на личните данни организациите могат да назначат служител по защита на данните (СЗД). **Не е необходимо обаче да назначавате служител по защита на данните**, ако обработването на лични данни не е основна част от вашия бизнес, не е рисково обработване и вашата дейност не е в голям мащаб.

Ако например дружеството ви събира данни на клиентите само с цел доставка по домовете, не е необходимо да назначавате СЗД.

Дори ако трябва да използвате СЗД, това може да бъде съществуващ служител, натоварен с тази функция в допълнение към другите му задачи. Или може да бъде външен консултант; така както много организации използват външни счетоводители.

> **Обикновено не трябва да правите оценка на въздействието върху защитата на данните**

Такава оценка на въздействието е запазена за тези, които представляват по-голям риск за личните данни, например извършват мащабен мониторинг на обществено достъпна зона (напр. видео наблюдение).

Ако сте малко дружество, което управлява заплатите на служителите и списък на клиентите, не е необходимо да правите оценка на въздействието върху защитата на данните за тези операции за обработване.

Глоби

Надзорните органи за защита на данните са оправомощени да санкционират нарушенията на правилата за защита на данните. Те могат да приемат коригиращи мерки (като заповед или временно прекратяване на обработването) и/или да налагат глоби.

Решението им за налагане на глоба трябва да бъде пропорционално и основано на оценка на всички обстоятелства по конкретния случай.

Ако решат да наложат глоба, размерът на глобата ще зависи също така от обстоятелствата по случая, включително от тежестта на нарушението или от това дали нарушението е извършено умишлено или поради небрежност. Те също така ще вземат под внимание вашето отношение и намеренията ви.

Ако желаете да получите повече информация:

1. **Направете справка с онлайн ръководството на Европейската комисия относно реформата в областта на защитата на данните — достъпно на всички езици на ЕС:**

   europa.eu/dataprotection/bg

2. **Консултирайте се с вашия национален орган за защита на данните:**

   edpb.europa.eu/about-edpb/board/members_bg

ВАЖНО СЪОБЩЕНИЕ

Информацията, представена в това ръководство, има за цел да допринесе за по-доброто разбиране на правилата на ЕС за защита на данните.

Тя служи само за ориентиране — само текстът на Общия регламент относно защитата на данните (ОРЗД) има правна сила. Следователно само ОРЗД може да поражда права и задължения за физическите лица. Тези насоки не пораждат никакви права или очаквания, подлежащи на изпълнение.

Обвързващото тълкуване на законодателството на ЕС е от изключителната компетентност на Съда на Европейския съюз. Гледните точки, изразени в настоящите насоки, не засягат позицията, която може да заеме Комисията пред Съда.

Нито Европейската комисия, нито лице, действащо от името на Европейската комисия, носи отговорност за използването на информацията в това ръководство.

Тъй като този документ отразява състоянието на техниката в момента на изготвянето му, той следва да се разглежда като „жив инструмент“, отворен за усъвършенстване, и съдържанието му може да бъде предмет на изменения без предизвестие.

Отпечатано от OIB

Служба за публикации

Люксембург: Служба за публикации на Европейския съюз, 2018 г.

Print	PDF
ISBN 978-92-79-85377-7	ISBN 978-92-79-85393-7
doi:10.2838/35819	doi:10.2838/150675
DS-02-18-544-BG-C	DS-02-18-544-BG-N