АУДИТ · МСФО · КОНСАЛТИНГ · АУТСОРСИНГ

GDPR
новый регламент Евросоюза по защите данных:

АКТУАЛЬНО ДЛЯ БЕЛОРУССКОГО БИЗНЕСА

Now, for tomorrow

bakertilly

Что такое GDPR и на кого он распространяет свое действие?

GDPR (General Data Protection Regulation) –
Общий регламент по защите данных, принятый Европейским союзом для обеспечения согласованного и высокого уровня защиты физических лиц и устранения препятствий для движения потоков персональных данных в рамках Евросоюза

GDPR ужесточает требования к уровню безопасности информационных потоков, содержащих персональные данные физических лиц, находящихся на территории ЕС, а также устанавливает меры ответственности за их несоблюдение

GDPR вступает в силу 25 мая 2018 года

GDPR распространяет свое действие на:

1. компании, учрежденные в ЕС, а также филиалы, представительства, отделения, дочерние структуры компаний, учрежденных за пределами ЕС

2. компании, учрежденные за пределами ЕС, если они осуществляют обработку персональных данных физических лиц, находящихся на территории ЕС, в связи с:

2.1. предложением товаров или услуг этим физическим лицам, независимо от того, связано это с их с оплатой или нет

Например: онлайн магазины, онлайн игры, разработчики приложений, транспортные компании, компании-перевозчики, туроператоры

∗ субъекты данных находятся в одном или нескольких государствах-членах ЕС;
∗ компанией используется язык или валюта, обычно используемые в одном или нескольких государствах-членах ЕС (существует возможность заказывать товары и услуги на этом языке или упоминается о том, что потребителями товаров или пользователями услуг могут быть физические лица, находящиеся на территории ЕС).

2.2. мониторингом действий этих физических лиц

Например: скоринг, мониторинг транзакций, аналитика данных для целей рекламы

∗ в результате обработки персональных данных компания может составить профиль физического лица;
∗ данные профиля физического лица могут быть использованы компанией для анализа или прогнозирования действий лица на рабочем месте, в экономической ситуации, его состояния здоровья, личных предпочтений, интересов, надежности, поступков, местонахождения или передвижений.

GDPR применяется к обработке персональных данных автоматическими средствами и без их использования.

Какие персональные данные находятся под защитой GDPR?

«Персональные данные» (personal data) в GDPR означают любую информацию, относящуюся к идентифицированному или идентифицируемому физическому лицу, находящемуся на территории ЕС

имя, идентификационный номер, данные о местоположении, онлайн-идентификатор, показатели, характерные для физической, физиологической, генетической, умственной, экономической, культурной или социальной идентичности данного физического лица, отпечатки пальцев, генетические данные, биометрические данные, расовая и этническая принадлежность, сексуальная ориентация, информация о здоровье, данные о личной жизни, данные о семье, об используемых устройствах, религиозных взглядах, философских воззрениях, политических взглядах, хобби и времяпровождении, интересах и увлечениях, история путешествий, финансовая информация, информация о членстве в профсоюзах и иных организациях, IP-адрес, cookie-файлы, теги радиочастотной идентификации, инструменты аутентификации (учетная запись, пароль)

*граждане ЕС,
резиденты ЕС,
физические лица, пребывающие в ЕС на основании визы или ином законном основании,
беженцы*

Защита, предусмотренная GDPR, применяется к **любым физическим лицам, находящимся на территории ЕС**, независимо от их национальной принадлежности или места жительства, а также от того, осуществляется ли сама обработка на территории ЕС

Кто такие контролёр и обработчик персональных данных в смысле GDPR?

«контролёр» (controller) –

физическое или юридическое лицо, государственный орган, агентство или иной орган, который самостоятельно или совместно с другими **определяет цели и средства обработки персональных данных**

«обработчик» (processor) –

физическое или юридическое лицо, государственный орган, агентство или иной орган, который **обрабатывает персональные данные от имени и по поручению контролёра**

Обработкой персональных данных считается любое действие, совершаемое с персональными данными, включая:

- сбор
- запись
- организацию
- структурирование
- хранение
- адаптацию
- изменение
- восстановление

- использование
- раскрытие при передаче
- распространение или обеспечение доступности
- группировку / комбинацию
- ограничение
- уничтожение

	КОНТРОЛЁР	ОБРАБОТЧИК
специальные обязанности	• получить согласие субъекта персональных данных на их обработку (письменное заявление (в том числе в электронной форме); устное заявление, проставление галочки при посещении сайта; выбор технических настроек услуг информационного общества; иное документальное подтверждение или способы действий, которые ясно указывают в данном контексте принятие субъектом данных предлагаемой обработки персональных данных); • предоставить субъекту персональных данных информацию о целях обработки данных; рисках, правилах, средствах защиты и правах в отношении обработки персональных данных и о том, как реализовать свои права в связи с такой обработкой; сроках обработки данных; контролёре; намерении контролёра передать персональные данные в третью страну (если это применимо) и пр. • принять локальные нормативные акты и внутренние правила, а также осуществить меры, которые, будут соответствовать принципам защиты персональных данных; • предусмотреть средства для получения электронных запросов субъектов персональных данных и ответов на них (в срок до 1 месяца); • помогать субъекту персональных данных в реализации его прав; • уведомлять субъекта персональных данных и надзорный орган об утечке персональных данных; • **взаимодействовать только с теми обработчиками, которые соблюдают требования GDPR**. Если количество сотрудников компании-контролёра превышает 250, контролёр обязан **вести учетные записи обработки данных** (в письменном/электронном виде) с указанием: • наименования и реквизитов контролёра, его представителя и инспектора по защите персональных данных; • целей обработки; • категорий субъектов данных и категорий персональных данных; • категорий получателей, которым персональных данные были или будут раскрыты, включая получателей в третьих странах; • сроков удаления различных категорий данных, когда это возможно; • технических и организационных мер безопасности.	• действовать на основании договора с контролёром, определяющим: содержание, предмет и продолжительность обработки; характер и цели обработки; тип персональных данных и категории субъектов данных; • возвратить или удалить персональные данные по окончании их обработки (по выбору контролёра); • привлекать других обработчиков к выполнению своих обязанностей (субподрядчиков) только с предварительного письменного разрешения контролёра. Если количество сотрудников компании-обработчика превышает 250, обработчик обязан **вести учетные записи обработки данных** (в письменном/электронном виде) с указанием: • наименования и реквизитов обработчика и контролёра, а также инспектора по защите персональных данных; • категорий персональных данных; • технических и организационных мер безопасности.

Учетные записи ведутся, независимо от количества сотрудников, если:

* обработка может привести к возникновению рисков для прав и свобод субъектов данных,
* обработка не носит случайный характер,
* обработка охватывает специальные категории данных,
* персональные данные касаются судимости или правонарушений.

общие обязанности контролёра и обработчика

- осуществлять **технические и организационные меры**, обеспечивающие надлежащий уровень безопасности персональных данных, включая:
  - псевдонимизацию и криптографическую защиту персональных данных;
  - средства для обеспечения постоянной конфиденциальности, целостности, доступности и устойчивости систем обработки;
  - средства своевременного восстановления доступности и доступа к персональным данным в случае природного или технического инцидента;
  - регулярные проверки и оценку эффективности технических и организационных мер, обеспечивающей безопасность обработки;
- назначить **инспектора по защите персональных данных**, если ключевая деятельность контролёра или обработчика заключается в:
  - обработке данных, которая в силу своего характера, своего объема и/или целей требует регулярного и систематического мониторинга субъектов данных в больших масштабах;
  - масштабной обработке особых категорий данных, а также персональных данных, касающихся осужденных в уголовном порядке и правонарушителей;
- сотрудничать с надзорным органом (по его запросу).

альтернативные обязанности (выполняет либо контролёр, либо обработчик)

Контролёр или обработчик должны **назначить представителя в ЕС**, за исключением случаев, когда:

- обработка носит случайный характер,
- обработка не включает в себя масштабную обработку конкретных категорий персональных данных,
- обработка персональных данных, связанных с уголовными приговорами и правонарушениями, едва ли обернётся рисками для прав и свобод физических лиц, с учётом характера, обстоятельств, сферы применения и целей обработки,
- контролёр является органом или учреждением государственной власти.

Каковы последствия несоблюдения требований, установленных GDPR?

Как контролёр, так и обработчик должны компенсировать **ЛЮБОЙ УЩЕРБ**, который физическое лицо может понести в результате обработки, нарушающей требования GDPR*.

Дело в отношении контролёра или обработчика истец может возбудить в судах государств-членов ЕС, в которых:
A. находится контролёр или обработчик, либо
B. проживает субъект данных

За любое отступление от требований GDPR нарушителю может быть объявлен **выговор** или наложен **административный штраф** в размере (в зависимости от того, какая из этих сумм окажется выше):

- до 4% от мирового годового оборота компании;
- до 20 000 000 €**

Нарушение бизнес-связей с европейскими партнерами (отказ от сотрудничества)

*Когда обработка может привести к дискриминации, краже персональных данных или мошенничеству, финансовым потерям, ущербу для репутации, нарушению профессиональной тайны и пр.

**При определении размера штрафа надзорным органом будут учитываться:
характер, тяжесть и продолжительность нарушения; преднамеренный характер нарушения; меры, принятые для смягчения нанесенного ущерба; степень ответственности или любые другие ранее совершенные нарушения; способ, посредством которого надзорному органу стало известно о нарушении; соблюдение мер, принятых в отношении контролёра или обработчика; соблюдение ими кодексов поведения; любые иные отягчающие или смягчающие вину обстоятельства.

Что делать, если ваша компания подпадает под действие GDPR?

1. Проанализировать процессы обработки персональных данных на предмет соответствия требованиям GDPR

2. Определить организационные меры, необходимые для соответствия процессов обработки требованиям GDPR

3. Внедрить механизмы защиты персональных данных, установленные GDPR, в процессы обработки

4. Использовать технические меры защиты персональных данных в зависимости от системы

5. Осуществлять постоянный мониторинг соответствия процессов обработки требованиям GDPR

Для того, чтобы процессы обработки персональных данных в вашей компании соответствовали требованиям GDPR, необходимо учитывать следующие аспекты:

1) технический (шифрование для неиспользуемых данных; шифрование данных во время их передачи; шифрование бэкапов; антивирус и пр.);

2) организационный (получение дифференцированного согласия субъекта персональных данных на их обработку; предоставление субъекту персональных данных возможности реализовать права, закрепленные GDPR; назначение инспектора по защите персональных данных; назначение представителя в ЕС; ведение учетных записей обработки персональных данных; проверка соответствия деятельности обработчиков требованиям GDPR (если ваша компания является контролёром) и пр.);

3) правовой (создание Privacy Policy, Information Governance Policy или иного локального акта; контроль за соответствием организационных мер требованиям GDPR).

Компания «Бейкер Тилли Бел» готова оказать вам консультационную поддержку в сфере организационных аспектов применения GDPR.

О компании Baker Tilly Bel

Бейкер Тилли Бел – аудиторская и консалтинговая компания с широким спектром услуг в сфере аудита, налогообложения и консультирования.

Контакты
ул. Суражская 10, офис 4, 2 этаж
Минск, 220007, Беларусь

T: +375 (17) 394 95 03
Ф: +375 (17) 394 77 40

www.bakertilly.by