

# Проверь свою компанию на соответствие требованиям GDPR.

GDPR (General Data Protection Regulation) – регламент ЕС по Обработке персональных данных в Европе для международного IT-рынка, вступил в действие **25 мая 2018 года**. Вы попадаете под действие GDPR, если:

- У вашей компании есть Представительства или филиалы на территории ЕС
- Вы предлагаете услуги или товары жителям Евросоюза.
- Вы проводите мониторинг активности пользователей из ЕС.

Условия регламента действуют не только на граждан ЕС, но и на резидентов. Если гражданин РФ уезжает учиться или работать в одну из стран Евросоюза, он становится ее резидентом. Когда он пользуется вашим сайтом или приложением, на вашу компанию автоматически распространяются правила GDPR. За их несоблюдение грозит штраф в размере 20 000 000 евро или 4% от годового оборота в зависимости от того, какая сумма больше. Российским компаниям важно пройти проверку на соответствие GDPR, чтобы не допустить финансовых потерь.

Перед вами контрольный список, выполнение условий которого поможет защитить вашу компанию и персональные данные ваших клиентов. Если вам удалось дойти до конца списка и выполнить необходимые условия, то вы значительно сократили риски штрафов!

## Правовая база и прозрачность

- Определите, какие персональные данные обрабатывает ваша компания и кто имеет доступ к ним.
- Подготовьте юридическое обоснование вашей деятельности в сфере обработки персональных данных.
- Предоставьте информацию об обработке данных и юридическое обоснование, прописанное в вашей политике конфиденциальности.

## Безопасность данных

- Всегда принимайте во внимание вопрос защиты данных, с момента начала разработки продукта до каждой обработки персональных данных.
- Используйте шифрование, псевдоним или анонимность личных данных, где это возможно.
- Создайте внутреннюю политику безопасности для членов вашей команды и повышайте уровень знаний сотрудников о защите данных.
- Внедрите процесс уведомления властей и ваших субъектов данных в случае взлома системы.
- Если тип обработки данных может привести к рискам для прав и свобод людей, то контролер должен сделать оценку воздействия этого способа обработки на защиту персональных данных. Разработайте заранее алгоритм проведения оценки.

## Ответственность и управление

- Назначьте человека, ответственного за обеспечение соответствия GDPR в вашей организации.
- Подпишите соглашение об обработке персональных данных между вашей организацией и компаниями, которые делают это от вашего имени.
- Если ваша организация находится за пределами ЕС, назначьте представителя в одной из стран-членов ЕС.
- Назначьте сотрудника по защите данных внутри компании (при необходимости).

## Политика конфиденциальности

- Ваши клиенты могут получить информацию о себе по запросу.
- Ваши клиенты могут обновить или исправить неточную либо неполную информацию о себе.
- Ваши клиенты могут запросить удалить свои личные данные.
- Ваши клиенты могут попросить прекратить обработку персональных данных.
- Ваши клиенты могут получить копию своих личных данных в формате, который легко передать другой компании.
- Ваши клиенты могут возражать против обработки персональных данных.
- Если вы принимаете решения в отношении людей на основе автоматизированных процессов, у вас есть процедура для защиты их прав.