ЧТО НУЖНО ДЕЛАТЬ, ЧТОБЫ ИЗБЕЖАТЬ САНКЦИЙ ПО GDPR?

июль 2018

ЧТОБЫ ПОНЯТЬ, РАСПРОСТРАНЯЕТСЯ ЛИ GDPR на деятельность вашей компании, нужно ответить на следующие вопросы:

- Есть ли у компании представительства (филиалы) на территории Европейского Союза?
- Обрабатываете ли вы персональные данные граждан стран-участниц Европейского Союза по поручению европейского оператора?
- Руководствуетесь ли при осуществлении деятельности по обработке персональных данных законодательством Европейского Союза или страны-участницы Европейского Союза?
- Осуществляете ли отдельные виды обработки персональных данных европейских граждан, в частности хранение, накопление, с использованием технических мощностей, находящихся на территории Европейского Союза?

Если вы ответили «ДА» хотя бы на один вопрос, то с большой вероятностью можно сказать, что на деятельность вашей компании GDPR все же распространяется.

КАКИЕ ДЕЙСТВИЯ НУЖНО ПРЕДПРИНЯТЬ?

I. ПРОВЕДИТЕ АУДИТ ИНФОРМАЦИОННЫХ ПОТОКОВ ВАШЕЙ КОМПАНИИ

- **Какие ПД граждан Европейского Союза вы собираете?**
- **Насколько собираемый объем ПД необходим для достижения целей их обработки?**

Если есть возможность,
МИНИМИЗИРУЙТЕ либо **АНОНИМИЗИРУЙТЕ**
обрабатываемый перечень ПД.

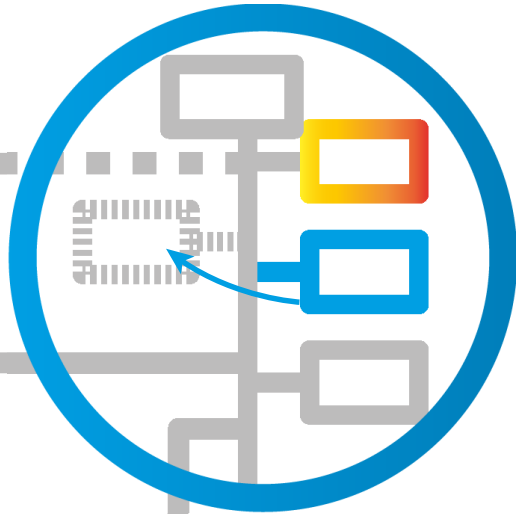
II. ПРОАНАЛИЗИРУЙТЕ ЛОКАЛЬНУЮ НОРМАТИВНУЮ БАЗУ НА ПРЕДМЕТ СООТВЕТСТВИЯ ВАШЕЙ ДЕЯТЕЛЬНОСТИ ТРЕБОВАНИЯМ GDPR

НЕОБХОДИМО ПОДДЕРЖИВАТЬ В АКТУАЛЬНОМ СОСТОЯНИИ:

документы, определяющие политику компании в отношении обработки персональных данных;

локальные акты по вопросам обработки персональных данных;

положения о порядке и условиях обработки персональных данных в типовых формах и договорных документах.



III. ИНФОРМИРУЙТЕ О СВОЕЙ ДЕЯТЕЛЬНОСТИ ПО ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ДОСТУПНО И ПОНЯТНО

- **Право** граждан стран Европейского Союза на **получение информации** об обработке их ПД является ключевым в системе прав субъектов, заложенных в GDPR.
- Рекомендуется **размещать ссылку** на политику в отношении обработки персональных данных на всех страницах сайта, где осуществляется сбор ПД.
- При использовании метрических программ, направленных на сбор cookie-файлов, **обеспечьте правовую основу** для их сбора и последующего использования.

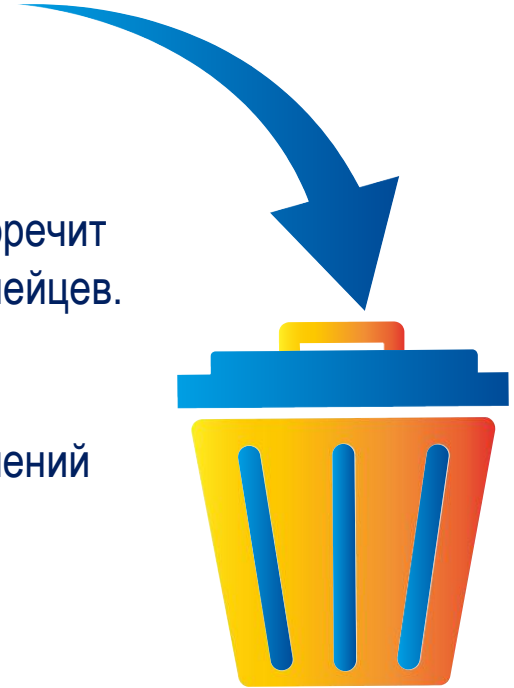
IV. ОГРАНИЧИВАЙТЕ ХРАНЕНИЕ ПД ЗАКОННЫМИ СРОКАМИ, ДОСТИЖЕНИЕМ ЦЕЛИ ОБРАБОТКИ ИЛИ ОТЗЫВОМ СОГЛАСИЯ СУБЪЕКТА НА ОБРАБОТКУ ПД

При сборе ПД европейских граждан требование о локализации данных на территории РФ на компанию не распространяется.

V. ПРЕДУСМОТРИТЕ ПРАВО НА ЗАБВЕНИЕ И НА ПЕРЕНОС ДАННЫХ В ЛОКАЛЬНЫХ АКТАХ

Право на забвение

Субъекты вправе требовать удаления информации о них из результатов поиска, если она не представляет общественного интереса. Удаление информации возможно, если это не противоречит интересам общества или иным фундаментальным правам европейцев.



Переносимость данных

Компании обязаны предоставлять бесплатно и без иных ограничений электронную копию ПД другой компании по требованию самого субъекта ПД.

VI. ЗАПРАШИВАЙТЕ ОТДЕЛЬНОЕ СОГЛАСИЕ ПО КАЖДОЙ ЦЕЛИ ОБРАБОТКИ

- GDPR устанавливает требования в отношении формы получения согласия на обработку данных в виде утверждения или в форме четких активных действий субъекта. Таким образом, **ИСКЛЮЧАЕТСЯ ВОЗМОЖНОСТЬ ПОЛУЧЕНИЯ СОГЛАСИЯ ПО УМОЛЧАНИЮ, ПО БЕЗДЕЙСТВИЮ СУБЪЕКТА.**

- **СОГЛАСИЕ НА ОБРАБОТКУ ПД МОЖЕТ БЫТЬ ПРИЗНАНО НЕДЕЙСТВИТЕЛЬНЫМ**, если у субъекта не было выбора или не было возможности отозвать свое согласие.

- Запрашивайте **ОТДЕЛЬНОЕ СОГЛАСИЕ ПО КАЖДОЙ ЦЕЛИ ОБРАБОТКИ**. Тем самым у субъекта появляется возможность отозвать согласие по деятельности, цель которой реально достигнута.

- **КОНКРЕТИЗИРУЙТЕ В СОГЛАСИИ ПЕРЕЧЕНЬ ОБРАБАТЫВАЕМЫХ ПД**, порядок и условия отзыва, а также конкретизируйте положения о третьих лицах, кому планируется передавать ПД субъектов или кого предполагается привлекать в рамках договора поручения.

- **СОГЛАСИЕ НА ОБРАБОТКУ ДАННЫХ РЕБЕНКА ДОЛЖНО БЫТЬ АВТОРИЗОВАНО РОДИТЕЛЯМИ** или законными представителями. Возрастной порог для родительской авторизации устанавливается государствами-членами ЕС отдельно.

VII. НАЗНАЧЬТЕ ОТВЕТСТВЕННОГО ЗА ЗАЩИТУ ПЕРСОНАЛЬНЫХ ДАННЫХ

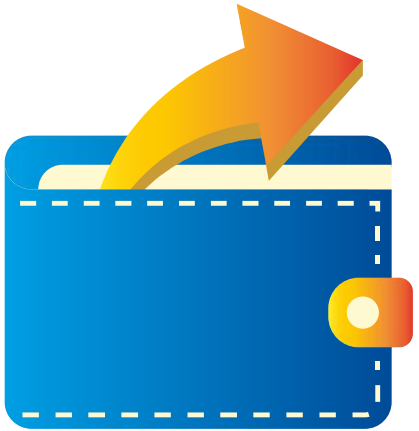
Компания должна опубликовать информацию о таком сотруднике, а также направить ее национальному регулятору по защите персональных данных соответствующей страны Европейского Союза.

КАКИЕ ШТРАФЫ ГРОЗЯТ ЗА НАРУШЕНИЕ GDPR?

Максимальный штраф за нарушение норм GDPR составляет

20 млн евро или **4%** оборота денежных средств.

Такое наказание предусматривается, как правило, за нарушения, связанные с несоблюдением прав и законных интересов субъектов.



Компания может быть оштрафована

на **2%** оборота денежных средств

за то, что не уведомила надзорный орган и субъекта ПД об утечке в течение **72** часов или не провела оценку возможного ущерба.

СПАСИБО ЗА ВНИМАНИЕ!