АЛЕРТ

Роскомнадзор опубликовал рекомендации операторам персональных данных в связи с участившимися случаями утечек данных

Вниманию операторов персональных данных

Юридическая компания «Пепеляев Групп» сообщает, что Роскомнадзором опубликованы рекомендации операторам при организации и осуществлении деятельности по обработке персональных данных.

Контролирующий орган объясняет необходимость в таких разъяснениях участившимися случаями неправомерного распространения персональных данных, а также результатами анализа содержания скомпрометированных баз данных.

Рекомендации состоят из восьми пунктов. Рассмотрим каждый из них и предложим меры, которые, на наш взгляд, могут понадобиться компании в связи с выполнением конкретной рекомендации.

Рекомендация 1:

Минимизируйте перечень персональных данных, которые собираете и обрабатываете. Используйте лишь те данные, которые действительно необходимы для оказания услуг, продажи товаров и иной деятельности организации.

Необходимые меры:

- Анализ процессов обработки персональных данных на предмет выявления «избыточных» персональных данных;
- Формирование перечня (реестра) обрабатываемых персональных данных в соответствии с требованиями п. 2 ч. 1 ст. 18.1 ФЗ «О персональных данных»);
- Подготовка/анализ форм анкет субъектов персональных данных (например, анкета соискателя/клиента/контрагента) для исключения случаев обработки «избыточных» персональных данных.

Рекомендация 2:

Обеспечьте раздельное хранение различных категорий персональных данных (клиенты, работники, соискатели и т. д.), в том числе несовместимых между собой по целям обработки.

Необходимые меры:

- Анализ баз данных, содержащих персональные данные, выявление несоответствий в случаях, если обработка осуществляется в целях, несовместимых между собой;
- Разработка перечня мест хранения материальных носителей персональных данных и/или перечня лиц, осуществляющих их обработку либо имеющих к ним доступ;
- Регулярное обучение персонала требованиям к обработке персональных данных.

Рекомендация 3:

Храните идентификаторы, указывающие на человека (ФИО, e-mail, телефон, адрес) и данные о взаимодействии с ним (оказанные услуги, проданные товары, переписка, договора и т. д.) в разных, не связанных друг с другом непосредственно, базах данных. Используйте для связи этих баз синтетические идентификаторы, не позволяющие без дополнительной информации и алгоритмов отнести информацию в этих базах к конкретному субъекту персональных данных, и храните их отдельно от предыдущих двух баз.

Необходимые меры:

- Определение возможности отнесения обрабатываемых данных к персональным данным;
- Технический аудит баз данных в соответствии с требованиями ст. 19 ФЗ «О персональных данных»;
- Регулярное обучение персонала требованиям к обработке персональных данных.

Рекомендация 4:

Откажитесь от практики накопления персональных данных «на всякий случай», от формирования профилей клиента, если это не жизненно нужно для организации. Своевременно уничтожайте персональные данные при достижении цели их обработки (например, после оказания услуги).

Необходимые меры:

- Разработка локальных нормативных актов, регулирующих процедуру уничтожения персональных данных;
- Анализ процессов обработки персональных данных на предмет выявления «избыточных» персональных данных;
- Формирование перечня (реестра) обрабатываемых персональных данных в соответствии с требованиями п.2 ч. 1 ст. 18.1 ФЗ «О персональных данных»);
- Регулярное обучение персонала требованиям к обработке персональных данных.

Рекомендация 5:

Используйте технические и программные средства, принадлежащие оператору, для обеспечения необходимого уровня безопасности данных. Поручение обработки данных третьим лицам не снимает с оператора ответственности, но снижает контроль со стороны оператора за принимаемыми мерами безопасности.

Необходимые меры:

- Полный технический аудит систем, в которых происходит обработка персональных данных, выявление нарушений требований, подготовка рекомендаций;
- Разработка локальных нормативных актов по обеспечению безопасности персональных данных при их обработке;
- Разработка форм соглашений с контрагентами (поручение обработки, передача персональных данных).

Рекомендация 6:

Своевременно информируйте Роскомнадзор о признаках и (или) наступивших инцидентах, повлекших (возможно повлекших) распространение персональных данных субъектов.

Необходимые меры:

- Подача в Роскомнадзор уведомления о факте неправомерной или случайной передачи персональных данных, повлекшей нарушение прав субъектов персональных данных;
- Разработка процедуры на случай неправомерной или случайной передачи персональных данных, повлекшей нарушение прав субъектов персональных данных;

- Регулярное обучение персонала требованиям к обработке персональных данных.

Рекомендация 7:

Принимайте меры физического контроля доступа к данным во избежание компрометации данных внутренним нарушителем.

Необходимые меры:

- Разработка локальных нормативных актов (инструкций работников) по вопросам обработки персональных данных;
- Проработка технических аспектов контроля доступа к персональным данным.

Рекомендация 8:

Назначьте ответственного в вашей организации за защиту персональных данных, наделите его необходимыми полномочиями.

Необходимые меры:

- Разработка приказа о назначении, инструкции ответственного за организацию обработки персональных данных;
- Регулярное обучение лица, ответственного за организацию обработки персональных данных.

О чем подумать, что сделать?

Установление факта распространения (предоставления) в сети «Интернет» баз данных, содержащих персональные данные, может привести к проведению внепланового контрольного (надзорного) мероприятия в отношении компании[1]. Данное правило применяется даже в условиях действующего моратория на проверки.

В рамках внепланового контрольного (надзорного) мероприятия (проверки) могут быть выявлены различные несоответствия деятельности компании требованиям ФЗ «О персональных данных». В частности, может быть установлен факт невыполнения требований ч. 5 ст. 18 ФЗ «О персональных данных» (сбор персональных данных с использованием баз данных, находящихся в РФ). Штраф за такое нарушение составляет до 6 млн руб.[2]

---

[1] Абзац 8 подп. а п. 3 Постановления Правительства РФ от 10.03.2022 № 336 «Об особенностях организации и осуществления государственного контроля (надзора), муниципального контроля».
[2] Часть 8 ст. 13.11 Кодекса РФ об административных правонарушениях от 30.12.2001 № 195-ФЗ.

Обращаем ваше внимание на то, что на отзыв в Правительство РФ направлен законопроект, предусматривающий штраф за допущенную утечку от 3 млн руб. до 3% совокупного размера суммы выручки компании.

Вероятно, рекомендации Роскомнадзора позволят если не исключить риск утечки полностью, то снизить потенциальный ущерб от нее.

Операторам персональных данных целесообразно проверить выполнение рекомендаций Роскомнадзора и, в случае необходимости, пересмотреть внутренние процессы с целью приведения их в соответствие с ними. Привлечение стороннего консультанта поможет более объективно оценить процессы обработки персональных данных.

Помощь консультанта

Специалисты «Пепеляев Групп» готовы оказать компаниям всестороннюю юридическую поддержку.

Спектр услуг «Пепеляев Групп» включает:

- Проведение аудита процессов обработки персональных данных, включая технические аспекты;
- Подготовка правовых заключений по вопросам, связанным с осуществлением обработки персональных данных;
- Разработка локальных нормативных актов и иных документов (например, анкет, согласий на обработку персональных данных, соглашений о поручении обработки), связанных с осуществление обработки персональных данных;
- Подготовка уведомлений о намерении осуществлять обработку персональных данных и/или трансграничную передачу персональных данных;
- Поддержка при взаимодействии с субъектами персональных данных и/или Роскомнадзором;
- Организация обучения персонала требованиям к обработке персональных данных;
- Поддержка лица, ответственного за организацию обработки персональных данных (в т.ч. по техническим аспектам);
- иные услуги.

Специальные пакеты услуг:

- «Документы для сайта» - приведение сайта компании в соответствие с требованиями ФЗ «О персональных данных».

- «Письменные согласия» - набор согласий, для которых необходима обязательная письменная форма.

Контактная информация

Николай Солодовников
Партнер

T: +7 (495) 767 00 07
n.solodovnikov@pgplaw.ru

Полина Бардина
Руководитель цифровой группы

T: +7 (495) 767 00 07
p.bardina@pgplaw.ru