Рекомендации РКН: политика обработки персональных данных

Роскомнадзор обнаружил, что в этом году стали чаще встречаться инциденты с **неправомерной** передачей персональных данных граждан. В связи с данным тревожным фактом госслужба выпустила набор рекомендаций, соблюдение которых поможет не нарушать порядок обработки персданных и, как следствие, избегать штрафов за это.

Вот **список необходимых мер**, разработанный ведомством:

1. Минимизация списка персданных, с которыми работает компания. Постарайтесь ограничиться только теми сведениями, без которых у фирмы действительно не было бы возможности оказывать услуги, продавать товары и вести иную деятельность.
2. Храните разные категории персданных раздельно, например, данные клиентов, сотрудников и соискателей, включая сведения, несовместимые друг с другом по целям обработки.
3. Хранение идентификаторов, указывающих на конкретную личность (ФИО, электронной почты, адреса и телефона) отдельно от информации о работе с ней (проданные ей товары оказанные ей услуги, договоры, корреспонденция), притом в разных базах данных, которые не связаны непосредственно друг с другом.
4. Применение для связи между такими базами синтетических идентификаторов, которые бы не позволили без дополнительных сведений и особых алгоритмов отнести данные в этих базах к определённому субъекту персданных. Храните всё это также отдельно от вышеуказанных 2 баз.
5. Отказ от накопления персданных и формирования профилей клиентов без особой необходимости по причине «вдруг пригодится».
6. Своевременное уничтожение персданных после выполнения задачи, для которой требовалось их обрабатывать (допустим, после оказания клиенту услуги).
7. Использование техники и ПО, принадлежащих оператору, так, чтобы обеспечвать нужную степень безопасности данных. Если оператор поручит обработку данных третьим лицам, это не снимет с него ответственность, зато осложнит контроль за применением мер безопасности.
8. Своевременное сообщение в РКН о подозрениях на и/или об уже явно свершившихся случаях, которые привели (или предположительно привели) к утечке персональных данных людей.
9. Необходимо также физически контролировать доступ к персданным, чтобы внутренний нарушитель не смог скомпрометировать их.
10. Назначение сотрудника, который в компании будет отвечать за защиту персданных, и предоставление ему соответствующих полномочий.

Напомним, что несоблюдение законов, регламентирующих защиту персональных данных, считается административным правонарушением, за которое полагается ответственность по **ст. 13.11 КоАП**. По этой статье могут оштрафовать на сумму до 6 000 000 руб.

Читайте также Продление сертификатов сотрудников организаци