Чек-лист

Изменения в законодательстве о персональных данных: что нужно знать для соответствия требованиям регуляторов?

С 1 сентября 2022 года вступает в силу закон, который ужесточает правила обработки персональных данных (ФЗ от 14.07.2022 №266-ФЗ).

Главные изменения:

- ✓ Компании будут чаще взаимодействовать с Роскомнадзором и ГосСОПКА
- ✓ Расширяется практика запросов от субъектов персональных данных
- ✓ Организация, которая обрабатывает персональные данные, обязана обеспечить их безопасность
- ✓ Закон требует указывать триаду сведений о собираемых ПДн – их перечень, цели обработки и действия, которые будут совершаться с данными
- ✓ Вводятся ограничения по трансграничной передаче данных
- ✓ Предоставлять биометрические данные станет необязательным

Чек-лист изменений

1. Взаимодействие с регулятором

Оператор ПДн обязан уведомлять Роскомнадзор обо всех случаях обработки персональных данных, даже если это еще только намерение.

Закон предусматривает всего два случая, когда обрабатывать ПДн можно без уведомления Роскомнадзора:

- Обработка ПДн без каких-либо средств автоматизации.

- Работа государственных информационных систем по охране безопасности и общественного порядка.

Что нужно сделать:

- [ ] Обновить документы, регламентирующие взаимодействие оператора ПДн с Роскомнадзором.
- [ ] Разработать шаблоны уведомлений в соответствии с новыми требованиями.

2. Обязанность сообщать об атаках и утечках ПДн

24 часа – в течение суток необходимо сообщать Роскомнадзору (через форму на сайте регулятора) обо всех инцидентах, в результате которых произошла утечка ПДн.

72 часа – в течение трех суток уведомить Роскомнадзор о результатах внутреннего расследования по инциденту (виновники утечки, причины, потенциальный вред и т. д.). Компании обязаны взаимодействовать с **ГосСОПКА (Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак)** – сообщать об утечках ПДн. При этом не нужно интегрироваться технически — сообщить об инциденте можно и по телефону, и по почте.

Что нужно сделать:

- [ ] Актуализировать регламенты по реагированию и расследованию инцидентов в организации.
- [ ] Наладить сбор доказательной базы из DLP-системы.
- [ ] Ввести в компании процедуру по уведомлению регуляторов об утечках.

3. Трансграничная обработка и передача ПДн

До 1 марта 2023 г. компании, осуществляющие трансграничную передачу, обязаны направить в Роскомнадзор два уведомления: **одно** – о намерении осуществлять обработку ПДн, **второе** – о намерении трансграничной передачи. Оператор ПДн теперь обязан запрашивать у иностранных обработчиков информацию о защите персональных данных. Если обработку ПДн осуществляют иностранные компании, то они тоже несут ответственность перед субъектом.

Что нужно сделать:

- [ ] Разработать оповещение о факте трансграничной обработки ПДн (должен включать оценку условий по сохранению конфиденциальности данных за рубежом).
- [ ] Привести в соответствие новым правилам уведомление о трансграничной передаче ПДн.

4. Запросы субъектов персональных данных (Data Subject Access Request, DSAR)

10 рабочих дней (ранее было 30) – срок, в течение которого компания должна выполнить запрос субъекта персональных данных и предоставить ему эти сведения. Субъект ПДн в рамках своего запроса может также потребовать прекратить обработку его ПДн.

Срок ответа на запрос может быть продлен на пять рабочих дней, если оператор ПДн обоснует такую необходимость.

Что нужно сделать:

- [ ] Разработать регламент работы с субъектами ПДн.
- [ ] Актуализировать документы, регламентирующие сроки ответа на запросы субъектов персональных данных.

5. Изменения в работе с биометрическими данными

С 1 сентября 2022 г. предоставлять оператору ПДн свои биометрические данные станет необязательным. Как правило, к биометрическим персональным данным относят:

- фотографию,
- видеоизображение человека,
- дактилоскопические данные,
- информацию о радужной оболочке глаза,
- результаты анализов ДНК,
- запись голоса.

При этом компания – оператор ПДн не вправе отказать субъекту в оказании услуг и заключении договора.

Что нужно сделать:

- [ ] Привести форму согласия в требуемый вид (прописать необязательность сдачи биометрических данных).

Для соответствия требованиям 152-ФЗ и минимизации рисков утечки персональных данных необходимо также использовать технические средства защиты информации, например DLP-систему Solar Dozor.

Solar Dozor 20 лет помогает компаниям из разных сфер и отраслей деятельности предотвращать утечки конфиденциальной информации и выявлять признаки корпоративного мошенничества. Отличается производительностью, проработанным интерфейсом, полнофункциональным агентом под Linux и macOS, возможностью геораспределенной работы и технологичностью (нейронные сети, UBA, поддержка VDI). Решение подходит для импортозамещения, включено в реестр российского ПО, а также сертифицировано ФСТЭК России.

Узнать подробнее