

Изменения в законодательстве о персональных данных с 1 сентября 2022 года

В 2022 году в Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных" внесено большое количество изменений. Эти изменения фактически коснутся любой компании. Большая часть поправок вступит в силу с 1 сентября 2022 года, другая часть – с 1 марта 2023 года.

Источники:

- Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных" (далее - Закон о ПДн);
- Федеральный закон от 14.07.2022 N 266-ФЗ (далее - Закон 266-ФЗ).

1. Станет больше случаев, когда нужно уведомлять Роскомнадзор об обработке ПДн

С 01.09.2022 нужно уведомлять об обработке ПДн	Можно не уведомлять об обработке ПДн
– работников; – клиентов, даже если их данные нужны только для заключения и исполнения договоров и никуда не передаются; – членов (участников) общественного объединения или религиозной организации; – разрешенных для распространения; – даже если вы получили только фамилию, имя, отчество; – для однократного пропуска на территорию.	– которые включены в государственные информационные системы персональных данных, созданные в целях защиты безопасности государства и общественного порядка; – если вы обрабатываете ПДн без использования средств автоматизации; – которые обрабатываются в случаях, предусмотренных законодательством о транспортной безопасности.

Теперь практически любая компания должна уведомлять Роскомнадзор об обработке персональных данных.

На основании чего внесено изменение: подп. "а", "б" п. 14 ст. 1 Закона 226-ФЗ

Где будет закреплено: ч. 2 ст. 22 Закона о ПДн

2. В уведомлении нужно будет указывать информацию об обработке ПДн для каждой цели отдельно

В уведомлении Роскомнадзору для каждой цели обработки ПДн нужно будет указывать:

- категории ПДн;
- категории субъектов, ПДн которых обрабатываются;
- правовое основание обработки ПДн;
- перечень действий с ПДн;
- способы обработки ПДн.

До 31.08.2022 включительно в уведомлении можно не расписывать информацию об обработке ПДн отдельно для каждой цели.

Основание: подп. “в” п. 14 ст. 1 Закона 226-ФЗ

Где будет закреплено: ч. 3.1 ст. 22 Закона о ПДн

3. Установили новые требования к политике обработки ПДн

В политике в отношении обработки ПДн нужно определить для каждой цели обработки персональных данных:

- категории и перечень обрабатываемых ПДн;
- категории субъектов, ПДн которых обрабатываются;
- способы, сроки обработки и хранения ПДн;
- порядок уничтожения ПДн.

Ссылку на политику в отношении обработки ПДн нужно разместить на каждой странице сайта, на которой вы собираете ПДн.

Основание: п. 10 ст. 1 Закона 226-ФЗ

Где будет закреплено: п. 2 ч. 1 ст. 18.1 Закона о ПДн

4. В договоры с гражданами запретили включать некоторые условия об обработке ПДн

В договоры с гражданами нельзя будет включать условия, которые:

- ограничивают права и свободы субъекта ПДн;
- устанавливают случаи обработки ПДн несовершеннолетних, если иное не предусмотрено законодательством РФ;
- допускают в качестве условия заключения договора бездействие субъекта ПДн.

Основание: подп. “а” п. 3 ст. 1 Закона 226-ФЗ

Где будет закреплено: п. 5 ч. 1 ст. 6 Закона о ПДн

5. Запретили отказывать в обслуживании клиентов, если они не предоставляют биометрию

Биометрические ПДн – это сведения о физиологических и биологических особенностях человека, на основании которых можно установить его личность. Например, это отпечатки пальцев, рисунок радужной оболочки глаза и т. п. Обработать биометрические ПДн можно только с письменного согласия субъекта ПДн на их обработку. В этой части ничего не изменилось.

Но теперь гражданину нельзя будет отказать в обслуживании, если он не дает согласие на обработку биометрических ПДн или не предоставляет их.

Основание: п. 6 ст. 1 Закона 226-ФЗ

Где будет закреплено: ч. 3 ст. 11 Закона о ПДн

6. Изменились требования к поручению на обработку ПДн

Обработчики – это лица, которым оператор ПДн дал поручение на обработку ПДн.

По новым правилам в поручении на обработку ПДн необходимо указывать:

- перечень ПДн, которые будет обрабатывать обработчик;
- перечень действий (операций) с ПДн, которые будет осуществлять обработчик;
- цели обработки ПДн в рамках поручения;
- обязанность обработчика соблюдать конфиденциальность персональных данных;
- обязанность обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение ПДн граждан РФ с использованием баз данных, находящихся на территории Российской Федерации;
- обязанность обеспечивать меры, предусмотренные ст. 18.1 Закона о ПДн;
- обязанность обработчика направлять оператору отчет о соблюдении конфиденциальности и безопасности ПДн;
- обязанность обработчика обеспечивать безопасность ПДн при их обработке;
- требования к защите ПДн, которые предусмотрены ст. 19 Закона о ПДн;
- требование об уведомлении оператора об утечках ПДн.

Ответственность оператора и обработчика перед субъектом ПДн также распределяется немного по-другому.

Если обработчик – российские гражданин или юридическое лицо

Ответственность несет только оператор

Если обработчик – иностранное лицо

Ответственность несет и оператор, и обработчик

Основание: подп. “б” п. 3 ст. 1 Закона 226-ФЗ

Где будет закреплено: ч. 3 ст. 6 Закона о ПДн

7. Уменьшились сроки ответа на запросы об обработке ПДн

Если вы получите запросы об обработке ПДн от субъекта ПДн или Роскомнадзора, то вам нужно будет реагировать на них гораздо быстрее.

Срок ответа на запрос с 01.09.2022	Срок ответа на запрос до 31.08.2022
10 рабочих дней.	30 календарных дней
Срок можно продлить на 5 рабочих дней, если вы письменно объясните субъекту ПДн, почему вы продлеваете срок ответа.	

Основание: п. 12 ст. 1 Закона 226-ФЗ

Где будет закреплено: ст. 20 Закона о ПДн

8. Появилась обязанность уведомлять Роскомнадзор об утечках ПДн

В случае утечки ПДн оператор должен уведомлять Роскомнадзор об утечках ПДн, которые привели к нарушению прав субъектов ПДн. Недостаточно просто уведомить Роскомнадзор об утечке. Нужно предоставить информацию в сжатые сроки:

В течение 24 часов с момента утечки	В течение 72 часов с момента утечки
– о факте утечки; – о предполагаемых причинах; – о предполагаемом вреде правам субъектов ПДн; – о принятых мерах по устранению последствий утечки; – о работнике оператора, уполномоченном на взаимодействие с Роскомнадзором.	– о результатах внутреннего расследования утечки; – о лицах, действия которых привели к утечке (если такие лица есть).

Пока непонятно, по какой форме нужно уведомлять Роскомнадзор. Возможно, он утвердит собственную форму.

Основание: подп. “а”, “б” п. 13 ст. 1 Закона 226-ФЗ

Где будет закреплено: ч. 3.1 ст. 21 Закона о ПДн

9. Появилась обязанность уведомлять о компьютерных инцидентах

Оператор должен будет передавать сведения о компьютерных инцидентах, которые привели к неправомерной передаче ПДн. Эти сведения нужно будет передавать в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ (ГосСОПКА).

Пока ФСБ не утвердила регламент взаимодействия с ГосСОПКА.

Основание: п. 11 ст. 1 Закона 226-ФЗ

Где будет закреплено: ч. 12-14 ст. 19 Закона о ПДн

10. Установили срок для прекращения обработки ПДн, если вы осуществляли ее без согласия субъекта

Оператор должен прекратить обработку ПДн в течение 10 рабочих дней со дня получения такого требования субъекта ПДн. Этот срок можно продлить на 5 рабочих дней, если вы письменно объясните субъекту ПДн, почему продлеваете срок.

Эти сроки применяются, если вы обрабатывали ПДн без согласия субъекта (например, в целях исполнения договора, заключенного с субъектом ПДн).

Раньше в Законе о ПДн был установлен только срок прекращения обработки ПДн, если субъект отозвал согласие на обработку ПДн. Это срок не изменился и составляет 30 дней со дня отзыва согласия.

Основание: подп. “б” п. 13 ст. 1 Закона 226-ФЗ

Где будет закреплено: ч. 5.1 ст. 21 Закона о ПДн

Рекомендации

1. Если вы еще не включились в реестр операторов, примите решение, будете ли вы уведомлять Роскомнадзор об обработке ПДн работников и клиентов.

Обращаем внимание, что за неуведомление Роскомнадзора предусмотрен штраф по ст. 19.7 КоАП РФ в размере от 3 000 до 5 000 рублей для юридических лиц.

2. Внесите изменения в политику в отношении обработки ПДн, в локальные нормативные акты об обработке ПДн и в формы согласий на обработку ПДн:

- 2.1. В политике в отношении обработки ПДн и в согласии на обработку ПДн определите для каждой цели обработки ПДн:

- категории и перечень обрабатываемых ПДн;
- категории субъектов, ПДн которых обрабатываются;
- способы, сроки обработки и хранения ПДн;

- порядок уничтожения ПДн.
- 2.2. Установите актуальные сроки ответов на запросы субъектов ПДн и Роскомнадзора.
- 2.3. Разместите ссылку на политику в отношении обработки ПДн на каждой странице сайта, на которой вы собираете ПДн.
- 3. Проверьте оферты, типовые формы договоров с гражданами и уже заключенные договоры.
 - 3.1. Исключите из договоров условия, которые:
 - ограничивают права и свободы субъекта ПДн;
 - устанавливают случаи обработки ПДн несовершеннолетних, если иное не предусмотрено законодательством РФ;
 - допускают в качестве условия заключения договора бездействие субъекта ПДн.
 - 3.2. Исключите из договоров условия, которые позволяют отказать в обслуживании гражданина, который не предоставляет биометрические ПДн.
- 4. В поручения на обработку ПДн добавьте новые обязанности обработчика.
- 5. Разработайте внутренний регламент уведомления Роскомнадзора об утечках и их расследовании.