

Персональные данные: что нужно сделать компаниям и на что важно обратить внимание

1. Проверить поручение на обработку персональных данных

В Законе конкретизированы требования ко всем обработчикам, как к отечественным, так и к иностранным. В ч. 3 ст. 6 указано, что именно должно быть определено в поручении на обработку (перечень персональных данных, перечень действий с персональными данными, цели их обработки и т.д.). Российский обработчик несет ответственность перед оператором, а тот, в свою очередь, перед субъектами. В случае если иностранное физическое или юридическое лицо является обработчиком, оно будет нести совместную с оператором ответственность перед субъектами персональных данных (ч. 6, ст. 6).

2. Отказаться от избыточного сбора биометрии

У субъекта появилось право отказать в предоставлении биометрических персональных данных. С сентября 2022 г. предоставление биометрических персональных данных не может быть обязательным, за исключением случаев, предусмотренных ч. 2 ст. 11 Закона. При этом оператор не вправе отказывать в обслуживании субъекту, который отказался предоставлять биометрические персональные данные и (или) согласие на их обработку (ч. 3, ст. 11).

3. Проверить договоры с субъектами персональных данных

Обратите внимание на изменения в ст. 6: теперь заключаемый с субъектом персональных данных договор не может содержать положения, ограничивающие права и свободы субъекта персональных данных, устанавливающие случаи обработки персональных данных несовершеннолетних, а также положения, допускающие в качестве условия заключения договора бездействие субъекта персональных данных.

4. Проверить формы согласий

Согласие на обработку персональных данных должно быть конкретным, предметным, информированным, сознательным и однозначным (ст. 9). Если предоставление персональных данных и (или) получение оператором согласия на обработку персональных данных являются обязательными, то оператор обязан разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные и (или) дать согласие на их обработку (ст. 18).

5. Проверить формы уведомлений субъектов

До начала обработки персональных данных, полученных не от субъекта персональных данных, оператор обязан предоставить субъекту персональных данных перечень важной информации об этом процессе, включающий цель обработки, наименование оператора, а с сентября в обязательном порядке еще и перечень персональных данных ([ч. 3, ст. 18](#)).

6. Проверить регламент ответов на запросы субъектов

В какие сроки нужно отвечать на запросы субъекта? К сожалению, срок сократился до 10 рабочих дней, он может быть продлен, но не более чем на пять рабочих дней в случае направления оператором в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации. Оператор также должен предоставлять по запросу информацию о способах исполнения оператором обязанностей, установленных [ст. 18.1](#) Закона ([ст. 14, ст. 20](#)). Требование об уничтожении персональных данных тоже должно быть выполнено в 10-дневный срок.

7. Назначить лицо, ответственное за организацию обработки персональных данных

8. Проверить комплект документов

Документы не могут содержать положения, ограничивающие права субъектов персональных данных, а также возлагающие на операторов не предусмотренные законодательством Российской Федерации полномочия и обязанности. В комплект документов должны входить:

- политика оператора в отношении обработки персональных данных;
- локальные акты по вопросам обработки персональных данных, определяющие для каждой цели обработки персональных данных категории и перечень обрабатываемых персональных данных, категории субъектов, способы, сроки их обработки и хранения;
- порядок уничтожения персональных данных при достижении целей их обработки или при наступлении иных законных оснований;
- локальные акты, устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений.

Теперь подлежат обязательному согласованию нормативные правовые акты по отдельным вопросам, касающимся обработки персональных данных, принятые государственными органами, Банком России, органами местного самоуправления, если указанные нормативные правовые акты регулируют отношения, связанные с осуществлением трансграничной передачи персональных данных, обработкой специальных категорий персональных данных, биометрических персональных данных, персональных данных несовершеннолетних, предоставлением, распространением персональных данных,

полученных в результате обезличивания ([ст. 4](#)).

9. Проверить регламент внутреннего аудита соответствия обработки персональных данных

10. Издать регламент оценки вреда субъектам персональных данных

11. Проверить регламент ознакомления работников с требованиями законодательства и локальных нормативных актов

12. Проверить регламент обучения работников

13. Разместить политику в отношении обработки персональных данных на своем сайте

Оператор, осуществляющий сбор персональных данных с использованием сайта, обязан опубликовать на страницах сайта политику в отношении обработки персональных данных ([ст. 18.1](#)).

14. Проверить уведомление об обработке персональных данных

Можно ли не подавать уведомление? Исключений осталось совсем немного ([ст. 22](#)).

Осталось лишь три случая:

- государственные информационные системы персональных данных, созданные в целях защиты безопасности государства и общественного порядка;
- обработка персональных данных исключительно без использования средств автоматизации;
- обработка в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности.

Изменились требования к содержанию уведомления. Теперь вся необходимая информация указывается оператором для каждой цели отдельно ([ст. 22](#)). Дополнительно потребуется указать фамилию, имя, отчество физического лица или наименование юридического лица, имеющих доступ и (или) осуществляющих на основании договора обработку персональных данных, содержащихся в государственных и муниципальных информационных системах. Формы уведомлений (об обработке, о внесении изменений, о прекращении обработки) устанавливаются Роскомнадзором.

15. Проверить регламент реагирования на инциденты

Добавлена обязанность уведомления Роскомнадзора в случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных ([ч. 3.1 ст. 21](#)). Времени не так уж много: 24 часа на информирование регулятора, 72 часа на исправление ситуации. Оператор также обязан передать информацию в ГосСОПКА ([ст. 19](#)).

16. Уведомить Роскомнадзор о трансграничной передаче

Оператор до начала осуществления деятельности по трансграничной передаче персональных данных обязан будет уведомить Роскомнадзор о своем намерении осуществлять трансграничную передачу персональных данных. Уведомление направляется в виде документа на бумажном носителе или в форме электронного документа и подписывается уполномоченным лицом. В [ст. 12](#) указаны требования к уведомлению.

Оператор до подачи уведомления обязан будет получить от иностранных лиц следующие сведения:

- сведения о принимаемых мерах по защите передаваемых персональных данных и об условиях прекращения их обработки;
- информацию о правовом регулировании в области персональных данных иностранного государства и т.д. Решение о запрещении или об ограничении трансграничной передачи персональных данных будет принято Роскомнадзором по результатам рассмотрения уведомления.

17. Провести оценку возможного вреда

18. Разработать регламент уничтожения скомпрометированных персональных данных

19. Периодически проверять актуальность сведений в уведомлении

В случае изменения сведений, указанных в уведомлении, оператор не позднее 15-го числа месяца, следующего за месяцем, в котором возникли такие изменения, обязан будет уведомить Роскомнадзор обо всех произошедших за указанный период изменениях. В случае прекращения обработки персональных данных оператор обязан будет уведомить об этом в течение 10 рабочих дней с даты прекращения обработки персональных данных ([ст. 22](#)).

20. Актуализировать регламент реагирования на инциденты

21. Отслеживать изменения законодательства