

ПЕРСОНАЛЬНЫЕ ДАННЫЕ: КАКИЕ ИЗМЕНЕНИЯ УЧЕСТЬ КОМПАНИЯМ С 1 СЕНТЯБРЯ ГОДА

Изменения коснулись широкого круга вопросов. Среди них: когда нужно уведомить о намерении обрабатывать персональные данные; что включать в локальные акты и как их правильно размещать на сайте компании; что делать, если произошла утечка данных.

1. СРОКИ ПРЕДОСТАВЛЕНИЯ ИНФОРМАЦИИ РОСКОНАДЗОРУ

Срок ответа ведомству сократили с 30 календарных [до 10 рабочих дней](#). Он может быть увеличен в пределах 5 рабочих дней на основании мотивированного уведомления.

2. УВЕДОМЛЕНИЕ ОБ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Из Закона о персональных данных [исключили](#) большинство случаев, когда компаниям не нужно было уведомлять Роскомнадзор о намерении начать обрабатывать персональные данные.

Таким образом, следует проинформировать ведомство, если компания собирается обрабатывать, в частности, персональные данные (ссылки ведут на утратившие силу нормы о случаях, когда уведомление не требовалось):

- [своих работников](#);
- [клиентов](#) (когда данные о них нужны исключительно для заключения и исполнения договоров);
- физлиц, которые [разрешили их распространять](#);
- физлиц — [только в части Ф.И.О.](#);
- физлиц — для [однократного пропуса](#) на территорию или в аналогичных целях.

Если для обработки персональных данных не используют средства автоматизации, уведомлять ведомство [не нужно](#). Например, данные о посетителях организации записывают в бумажный журнал при выдаче им разовых пропусков.

2. Скорректировали требования к содержанию уведомления. Если данные будут обрабатывать в разных целях, то **для каждой из них** [понадобится указать](#):

- категорию данных и их субъектов;
- правовое основание обработки;
- перечень действий с данными и способы их обработки.

Если у физлиц или юрлиц есть доступ к персональным данным в государственных (муниципальных) информационных системах или они обрабатывают данные из этих систем по договору, Ф.И.О. таких физлиц (наименование юрлиц) [нужно привести](#) в уведомлении.

3. В законе [закрепили](#) положение о том, что формы уведомлений должен установить Роскомнадзор (пока действует [рекомендуемая форма](#), которую можно заполнить и подать через [портал персональных данных](#)).

Роскомнадзор 1 сентября разъяснил рассмотренные изменения. Подробности в нашей [НОВОСТИ](#).

3. **ЛОКАЛЬНЫЕ АКТЫ ПО ВОПРОСАМ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ**

В законе [конкретизировали](#) требование о том, что локальные акты должны содержать:

- категории и перечни обрабатываемых данных;
- категории субъектов данных;
- способы и сроки обработки, хранения данных;
- порядок их уничтожения.

Эти положения нужно установить для каждой цели обработки данных.

Если компания собирает персональные данные граждан через свой сайт, проверьте, где именно на сайте опубликован документ о политике обработки данных и сведения о реализуемых компанией требованиях к их защите.

Такая информация [должна быть опубликована](#) в том числе на страницах сайта, где непосредственно идет сбор персональных данных (например, на страницах с формами, которые заполняют пользователи).

4. **ОБЯЗАННОСТИ В СЛУЧАЕ КОМПРОМЕТАЦИИ ПЕРСОНАЛЬНЫХ ДАННЫХ**

У компании есть [24 часа](#) с момента происшествия, чтобы сообщить в Роскомнадзор:

- об инциденте;
- его предполагаемой причине и вреде, причиненном субъектам данных;
- мерах по устранению последствий инцидента;
- представителе компании, который уполномочен взаимодействовать с Роскомнадзором по вопросам, связанным с происшествием.

У компании есть [72 часа](#) с момента инцидента, чтобы провести внутреннее расследование и сообщить в Роскомнадзор о его результатах, а также о виновниках (при наличии).

Компания [обязана](#) взаимодействовать с госсистемой обнаружения компьютерных атак ([ГосСОПКА](#)), в том числе направлять сообщения об утечке данных. Механизм взаимодействия определит ФСБ.

5. **ПОРУЧЕНИЕ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ ДРУГОМУ ЛИЦУ**

В поручении [нужно дополнительно отразить](#):

- перечень персональных данных;
- [обязанность](#) использовать для записи и хранения персональных данных базы данных на территории РФ;

- [меры](#), которые должен предпринять исполнитель для выполнения требований Закона о персональных данных;
- обязанность по запросу предоставлять в течение срока действия поручения информацию о соблюдении условий обработки персональных данных;
- обязанность уведомить о случаях компрометации обрабатываемых данных.

6. СОГЛАСИЕ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ

В число требований к согласию [включили](#) то, что оно должно быть предметным и однозначным.

Если получение согласия обязательно, компания [должна разъяснить](#) физлицу последствия не только отказа в предоставлении данных, но и отказа дать согласие на их обработку.

7. ПРЕДОСТАВЛЕНИЕ ИНФОРМАЦИИ ФИЗЛИЦАМ ОБ ОБРАБОТКЕ ИХ ДАННЫХ

Перечень сведений [дополнили](#) информацией о том, какими способами компания выполняет обязанности, предусмотренные Законом о персональных данных.

По запросу гражданина или его представителя сведения нужно предоставить в течение [10 рабочих дней](#). Срок может быть увеличен в пределах 5 рабочих дней на основании мотивированного уведомления. Ответ дается в той же форме, в какой поступил запрос, если в запросе не указано иное.

8. ОБЯЗАННОСТИ КОМПАНИИ, КОТОРАЯ ПОЛУЧИЛА ДАННЫЕ НЕ ОТ САМОГО ФИЗЛИЦА

В состав информации, которую по общему правилу организация обязана предоставить физлицу до начала обработки его данных, [включили](#) их перечень.

9. ПРЕКРАЩЕНИЕ ОБРАБОТКИ ДАННЫХ ПО ТРЕБОВАНИЮ ФИЗЛИЦА

У компании есть 10 рабочих дней с момента получения требования физлица, чтобы [прекратить обработку данных](#) о нем или обеспечить прекращение обработки (если ее ведет другое лицо). Срок можно продлить в пределах 5 рабочих дней на основании мотивированного уведомления.

10. ОСОБЕННОСТИ ОБРАБОТКИ ДАННЫХ ПОТРЕБИТЕЛЕЙ

1. По общему правилу продавец [не может отказать](#) потребителю в заключении, исполнении, изменении или расторжении договора из-за отказа потребителя предоставить персональные данные.

Есть два исключения:

- данные нужны для исполнения договора;
- предоставить данные требует закон.

За нарушение запрета [могут оштрафовать](#):

- должностных лиц на сумму от 5 тыс. до 10 тыс. руб.;
- юрлиц – от 30 тыс. до 50 тыс. руб.

2. Если потребитель потребует объяснить, почему из-за непредставления персональных данных ему отказали в заключении, исполнении, изменении или расторжении договора, ответить нужно в течение [7 дней](#), при устном запросе — [незамедлительно](#).

3. [Нельзя отказывать](#) в обслуживании физлицу, если оно не хочет предоставлять биометрические данные или соглашаться на обработку персональных данных, а закон не требует от компании получать такое согласие.

11. ТРЕБОВАНИЯ К ДОГОВОРУ, ДЛЯ ИСПОЛНЕНИЯ КОТОРОГО НУЖНЫ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

Договор [не может содержать](#) положения:

- ограничивающие права и свободы физлица;
- устанавливающие случаи обработки данных несовершеннолетних (если иное не предусмотрено законом);
- позволяющие заключать договор при бездействии физлица.

12. ИСПОЛЬЗОВАНИЕ ДАННЫХ ИНОСТРАННЫМИ ЛИЦАМИ

Положения Закона о персональных данных [распространили](#) на иностранные компании и физлиц, которые используют данные российских физлиц (например, по договору).

Если компания [передала данные](#) иностранной организации для обработки, ответственность перед физлицом несут обе организации.

13. ДОКУМЕНТЫ:

[Федеральный закон от 14.07.2022 N 266-ФЗ](#)

[Федеральный закон от 28.05.2022 N 145-ФЗ](#)

[Федеральный закон от 01.05.2022 N 135-ФЗ](#)