ВАШ КОНСУЛЬТАНТ
420021, г. Казань,
ул. Татарстан, д. 22/41, 8 этаж
Телефон: 8(800)700-52-23, 8(843)515-20-20
Email: cons@vkons.ru Сайт: www.vkons.ru

Чек-лист при работе с персональными данными: проверьте, все ли есть в компании

Не во всех компаниях налажена работа с персональными данными. Бывает, что необходимые документы отсутствуют полностью или когда-то специалист их оформлял, но уже многое изменилось.

Какие документы должны быть у всех, кто обрабатывает персональные данные? Кому придется направить в Роскомнадзор уведомление до 1 сентября 2022 года? Действительно ли выгоднее заплатить штраф?

В предлагаемом материале мы рассказали, как проверить, все ли готово в компании для успешной работы с персональными данными, описали новшества в законодательстве о ПД с 1 сентября 2022 года и оценили риски компании при ошибках и недочетах в работе с персональными данными, дав рекомендации по их устранению.

Содержание материала:

1. Что должно быть у всех, кто обрабатывает персональные данные?
2. Всем ли нужно уведомлять Роскомнадзор?
3. Какие штрафы грозят?
4. Что выгоднее: заплатить штраф или за оформление всех документов?

Что должно быть у всех, кто обрабатывает персональные данные?

Персональные данные (ПДн/ПД) – это личная информация о человеке, то есть о субъекте персональных данных. Это может быть адрес, ФИО, данные в аккаунтах в соцсетях, фото. Например, субъектом персональных данных становится посетитель сайта, заполнивший формы обратной связи для консультации, или будущий работник организации, предоставивший документы для оформления на работу.

Все компании и ИП, которые осуществляют обработку персональных данных, являются операторами ПД. Они собирают персональные данные, хранят их и вносят в различные базы.

Если компания или ИП не собирает никакие данные физических лиц, то она не является оператором. Например, если у ИП нет работников и он работает только с юридическими лицами и при этом не собирает и не хранит никаких данных физических лиц (допустим, ФИО курьеров). В этом случае можно не оформлять документы, связанные с обработкой персональных данных. Если в компании или у ИП есть работники, значит, они обрабатывают персональные данные.

Вот примерный список документов, которые должен иметь оператор персональных данных. Он составлен исходя из рекомендаций Роскомнадзора и собственного опыта в данной сфере (ссылки указаны на Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных»).

Документы:

1. уведомление об обработке персональных данных. Его нужно отправить в Роскомнадзор в момент начала обработки (п. 22 Закона №152-ФЗ);
2. приказ о назначении ответственного за организацию обработки персональных данных у оператора (подп. 1 ч. 1 ст. 18.1, ч. 1 ст. 22.1 Закона №152-ФЗ);
3. формы согласий и сами согласия субъектов персональных данных на обработку персональных данных (ст. 9 Закона №152-ФЗ);
4. политика (положение) об обработке персональных данных (ч. 2 ст. 18.1 Закона №152-ФЗ). При составлении положения можно взять за основу рекомендации Роскомнадзора;

5. документы, описывающие меры, предпринимаемые для защиты персональных данных. Они могут включать:

- инструкцию по контролю доступа в помещения, где проводится обработка персональных данных;
- инструкцию по парольной защите;
- инструкцию по антивирусной защите;
- инструкцию по порядку разрешительного доступа к персональным данным;
- положение о хранении носителей, содержащих персональных данные. Такими носителями могут быть флешка, диск, бумага;
- список помещений, где обрабатываются персональные данные;
- перечень средств защиты информации. В нем указываются названия средств защиты, их количество, производитель и информация о наличии сертификатов ФСТЭК и ФСБ (Постановление Правительства РФ от 01.11.2012 №1119, п. 8.12 Приказа ФСТЭК России от 18.02.2013 №21, подп. 2 ч. 2 ст. 19 Закона №152-ФЗ);

6. положение об обработке обращений и запросов, поступивших от субъектов персональных данных (п. 3 ч. 4 ст. 22.1 Закона №152-ФЗ). Его можно включить в политику об обработке персональных данных;

7. документ, устанавливающий требования к ведению журналов (реестров, книг), содержащих персональные данные, необходимые для однократного пропуска субъекта. Необходим, если в компании пропускной режим (п. 8 Постановления Правительства РФ от 15.09.2008 №687);

8. документ о классификации информационных систем. Например, информационными системами являются:

- 1С, в которой обрабатываются данные по сотрудникам, клиентам (в систему могут подгружать счета, договоры с клиентами);
- сайт, на котором есть форма обратной связи с клиентом, и др.

При классификации информационных систем нужно учитывать:

- Приказ ФСТЭК России от 18.02.2013 №21;
- Приказ ФСТЭК России от 11.02.2013 №17 (для госучреждений);
- Постановление Правительства РФ от 01.11.2012 №1119;

9. список лиц, которым необходим доступ к персональным данным (п. «в» ст. 13 Постановления Правительства от 01.11.2012 №1119, п. 8 ч. 2 ст. 19 Закона №152-ФЗ);

10. положение об обработке персональных данных работников;

11. обязательства работников о неразглашении персональных данных (ст. 90 ТК РФ);

12. модели угроз. В этом документе указывается, как именно стоит защищать данные, какие угрозы со стороны злоумышленников возможны в отношении данных и т. д. Его обязательно нужно составлять на каждую информационную систему, в которой производится обработка персональных данных.

Для подготовки этого документа нужно учитывать:

- Постановление Правительства РФ от 01.11.2012 №1119;
- Методику оценки угроз безопасности информации, утв. ФСТЭК 05.02.2021;
- Базовую модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утв. ФСТЭК 15.02.2008.

Данный перечень включает основные документы, которые должны быть у оператора персональных данных. Также могут быть и другие документы, например:

1. журнал учета проверок контролирующими органами (Роскомнадзором);
2. поручение на обработку персональных данных, если ПД передаются другим лицам (ч. 3 ст. 6 Закона №152-ФЗ). Например, при передаче компании, которая ведет бухгалтерию на аутсорсинге.

Обратите внимание! Нужно ознакомить работников с документами, которые регулируют в компании обработку персональных данных. Желательно также провести обучение и зафиксировать этот факт. Такое требование содержится в п. 6 ч. 1 ст. 18.1 Закона №152-ФЗ.

Всем ли нужно уведомлять Роскомнадзор?

Компании и ИП, которые обрабатывают персональные данные, должны соблюдать правила обработки, однако не всем нужно уведомлять Роскомнадзор о том, что она ведется. До 1 сентября 2022 года действует прежний обширный список случаев, когда можно не уведомлять Роскомнадзор (поправки введены Федеральным законом от 14.07.2022 №266-ФЗ). Однако после этой даты он резко сократится (п. 22 Закона №152-ФЗ в редакции Федерального закона от 14.07.2022 №266-ФЗ).

Так, с 1 сентября 2022 года можно не уведомлять Роскомнадзор об обработке персональных данных, только если:

1. персональные данные включены в государственные электронные ресурсы, которые созданы для защиты безопасности государства и общественного порядка;
2. оператор обрабатывает персональные данные исключительно без использования средств автоматизации, то есть на бумаге;
3. это предусмотрено законами о транспортной безопасности, для обеспечения безопасности транспортного комплекса государства, защиты общества в этой сфере.

Таким образом, после 1 сентября 2022 года останется совсем мало случаев, когда можно будет не уведомлять Роскомнадзор об обработке персональных данных. Например, потребуется отправлять уведомление в Роскомнадзор, даже если компания обрабатывает только ПД своих сотрудников или собирает данные для выдачи одноразовых пропусков.

Разберем несколько ситуаций.

1. Компания получает только личные данные своих сотрудников и не передает их третьим лицам. До 1 сентября 2022 года можно не уведомлять Роскомнадзор, но после этой даты уведомление Роскомнадзора в этой ситуации станет обязательным. Кроме того, если работодатель передает данные сотрудника третьим лицам (например, для оформления зарплатного проекта, ДМС), то в любом случае требуется направить в Роскомнадзор уведомление об обработке персональных данных.

2. Компания собирает на проходной личные данные посетителей и работников. Если

пропуск нужен посетителю для многократного использования, то нужно уведомлять Роскомнадзор об обработке персональных данных. Если данные требуются для однократного пропуска посетителям, то до 1 сентября 2022 года сообщать об обработке ПД в Роскомнадзор не требуется. Но к этой дате в любом случае потребуется отправить уведомление.

В случае с работниками, если данные не передаются третьим лицам и организациям, а пропуск – многократный, то сообщать в Роскомнадзор не нужно до 1 сентября 2022 года (после этой даты уведомления станут обязательными). Но если сведения предоставляются третьей стороне (например, ЧОП, осуществляющему пропускной режим), то уведомление регулятора в любом случае обязательно.

3. Компания собирает фото клиентов. Это биометрические персональные данные, поэтому уведомление Роскомнадзора об обработке персональных данных является обязательным.

4. Для заказа нужно сообщить ФИО, адрес электронной почты, адрес для доставки. Если эти данные нужны исключительно для исполнения условий договора, они не передаются третьим лицам и еще не наступило 1 сентября 2022 года, то уведомление Роскомнадзора не требуется. А вот когда компания передает сведения курьеру, который не является ее сотрудником, отправлять уведомление в Роскомнадзор нужно обязательно – так было и до поправок, которые вступают в силу 1 сентября 2022 года.

5. На сайте есть форма обратной связи и нужно заполнять ФИО и телефон или только телефон. До 1 сентября 2022 года можно не уведомлять Роскомнадзор, если данные не передаются третьим лицам, но если сведения поступают рекламным агентам для маркетинговых целей, тогда сообщить об обработке нужно. После 1 сентября уведомлять Роскомнадзор нужно независимо от того, передаются сведения третьим лицам или нет.

Если же компания собирает только данные о номере телефона клиента (без ФИО), то не нужно отправлять в Роскомнадзор уведомление (в том числе после 1 сентября 2022 года), так как сам по себе номер телефона не характеризует субъекта персональных данных.

6. Компания собирает cookies. Нужно отправить в Роскомнадзор уведомление об обработке персональных данных (Определение Мосгорсуда от 10.11.2016 по делу №33-38783/2016).

Допустим, компания давно собирает персональные данные. Когда она начинала работать, у нее не было обязанности направлять в Роскомнадзор уведомления об обработке ПД, например, потому, что организация собирала персональные данные сотрудников и никуда эти данные не направляла. Но с 1 сентября 2022 года вступают в силу поправки, согласно которым при обработке персональных данных сотрудников нужно уведомлять Роскомнадзор о начале обработки ПД (введены Федеральным законом от 14.07.2022 №266-ФЗ). Следовательно, этой компании нужно до 1 сентября направить такое уведомление, несмотря на то, что она давно работает и обрабатывает такие персональные данные.

Какие штрафы грозят?

Нарушение	Наказание	Норма КоАП РФ
Обработка персональных данных не предусмотрена законом или несовместима с целями сбора данных (например, в положении указаны одни цели для сбора данных, а их собирают и для других, допустим, для маркетинговых целей)	Штраф: - для должностных лиц – от 10 000 до 20 000 рублей; - для юрлица – от 60 000 до 100 000 рублей.	Ч. 1 ст. 13.11
Нет согласия субъекта или есть другие нарушения обработки персональных данных (например, компания неправильно хранит данные субъекта при их обработке на бумаге, бумажный носитель не убирают в шкаф (сейф))	Штраф: - для должностных лиц – от 20 000 до 40 000 рублей; - для юрлица – от 30 000 до 150 000 рублей.	Ч. 2 ст. 13.11
Оператор не предоставил доступ к политике по обработке персональных данных (например, не опубликовал на сайте)	Штраф: - для должностных лиц – от 6 000 до 12 000 рублей; - для ИП – от 10 000 до 20 000 рублей; - для юрлица – от 30 000 до 60 000 рублей.	Ч. 3 ст. 13.11
Оператор не предоставляет субъекту персональных данных информацию, которая касается обработки его ПД	Штраф: - для должностных лиц – от 8 000 до 12 000 рублей; - для ИП – от 20 000 до 30 000 рублей;	Ч. 4 ст. 13.11

	- для юрлица – от 40 000 до 80 000 рублей.	
Оператор не выполняет в срок требования субъекта персональных данных, его представителя либо Роскомнадзора об уточнении ПД, их блокировании или уничтожении	Штраф: - для должностных лиц – от 8 000 до 20 000 рублей; - для ИП – от 20 000 до 40 000 рублей; - для юрлица – от 50 000 до 90 000 рублей.	Ч. 5 ст. 13.11
Оператор не выполнил при обработке ПД на бумажных носителях обязанности по соблюдению условий, обеспечивающих их сохранность и исключающих незаконный к ним доступ, если это повлекло доступ к данным	Штраф: - для должностных лиц – от 8 000 до 20 000 рублей; - для ИП – от 20 000 до 40 000 рублей; - для юрлица – от 50 000 до 100 000 рублей.	Ч. 6 ст. 13.11
Оператор обрабатывает персональные данные с использованием баз данных, находящихся за пределами территории РФ	Штраф: - для должностных лиц – от 100 000 до 200 000 рублей; - для юрлица – от 1 млн. до 6 млн. рублей.	Ч. 8 ст. 13.11
Оператор не предоставил или несвоевременно предоставил в Роскомнадзор сведения (либо в неполном объеме или в искаженном виде)	Штраф: - для должностных лиц – от 300 до 500 рублей; - для юрлица – от 3 000 до 5 000 рублей.	Ст. 19.7

Важно!

Если компанию оштрафовали, но она оплачивает штраф в течение 20 дней, то она может заплатить половину суммы

(ч. 3.4 – 1 ст. 4.1 КоАП РФ в редакции Федерального закона от 14.07.2022 №290-ФЗ). А при совершении правонарушения впервые штраф заменяется на предупреждение (ч. 1 ст. 4.11 КоАП РФ в редакции Федерального закона от 14.07.2022 №290-ФЗ). Еще нужно помнить, что за повторные нарушения штрафы, наоборот, гораздо выше.

Проводит ли Роскомнадзор проверки в 2022 году?

В 2022 году Роскомнадзор не проводит плановые проверки и надзорные мероприятия в компаниях и ИП, осуществляющих обработку персональных данных (п. 1 Постановления Правительства РФ от 10.03.2022 №336), но внеплановую проверку могут провести. Так, проверки по заявлениям и жалобам физических лиц-субъектов персональных данных активно идут, поэтому надеяться на отсутствие контроля не приходится.

Что выгоднее: заплатить штраф или за оформление всех документов?

Многие считают, что выгоднее заплатить штраф, чем потратить деньги на оформление всего комплекта документов, необходимых при обработке персональных данных, а Роскомнадзор штрафует редко.

На самом деле нужно учитывать, что достаточно одной жалобы клиента в Роскомнадзор, чтобы инициировать проверку, а штрафы будут считать за каждое нарушение.

Например, есть интернет-магазин, который продает строительные материалы. На его сайте можно приобрести товар, но для этого покупатель должен указать свои персональные данные: ФИО, адрес для доставки, номер телефона, адрес электронной почты. Также предусмотрена форма обратной связи для клиентов, которые могут поинтересоваться у сотрудников интернет-магазина о дополнительных свойствах продаваемого товара.

На сайте отсутствуют необходимые документы по защите персональных данных: согласие на обработку и политика по обработке персональных данных. Также интернет-магазин игнорирует запросы клиентов по поводу обработки их данных.

Верхнего потолка суммы в данном случае нет, поэтому посчитаем только минимальный штраф для юрлица в таком случае:

1. нет согласия на обработку персональных данных – от 30 000 рублей (такой штраф будет, если нарушение совершено впервые, за повторное нарушение штрафы будут выше – для юрлиц от 300 000 рублей. Каждый случай считается индивидуально, то есть указанный размер штрафа можно получить как за нескольких клиентов, которые не дали согласия на обработку данных, так и за одного);
2. нет политики об обработке персональных данных – от 30 000 рублей;
3. компания не отвечает на запросы клиентов-физлиц по поводу обработки персональных данных – от 40 000 рублей за каждую жалобу в Роскомнадзор.

При этом стоимость оформления документов у сторонних специалистов – от 60 000 до 150 000 рублей, а периодическая корректировка документации и поддержание в актуальном состоянии составят около 40 000 – 50 000 в год.

Если нанимать отдельного специалиста в компанию, то это от 40 000 до 150 000 рублей в

месяц в зависимости от региона и объема работы.

Дополнительные полезные материалы из СПС «КонсультантПлюс»:

- *Обзор: "Планируют ввести новые требования к обработке персональных данных" (КонсультантПлюс, 2022) {КонсультантПлюс}*
- *Обзор: "Основные изменения в КоАП РФ в 2022 году" (КонсультантПлюс, 2022) {КонсультантПлюс}*
- *Готовое решение: Каковы обязанности оператора персональных данных (КонсультантПлюс, 2022) {КонсультантПлюс}*
- *Готовое решение: Какие существуют требования к обработке персональных данных работников организации (КонсультантПлюс, 2022) {КонсультантПлюс}*
- *Готовое решение: В каком порядке должна осуществляться обработка персональных данных физлиц (КонсультантПлюс, 2022) {КонсультантПлюс}*
- *Готовое решение: Кто и какую ответственность несет за нарушение законодательства о персональных данных (КонсультантПлюс, 2022) {КонсультантПлюс}*
- *Готовое решение: Как Роскомнадзор контролирует соблюдение требований в сфере персональных данных (КонсультантПлюс, 2022) {КонсультантПлюс}*
- *Готовое решение: Как Роскомнадзор проводит внеплановую выездную проверку в сфере персональных данных (КонсультантПлюс, 2022) {КонсультантПлюс}*