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

Проверки Роскомнадзора по защите персональных данных: что и как проверяют

Любое появление инспектора, будь то плановая или внеплановая проверка, для бизнеса всегда сопряжено с определенными рисками. Лучше заранее убедиться в наличии всех необходимых документов, защищающих интересы компании, а если есть нарушения, внести исправления до того, как их обнаружит инспектор.

Еще важно разобраться в типах проверок и в порядке контрольных процедур. Тем более что с недавних пор действует риск-ориентированный подход, выделяются группы операторов по тяжести потенциальных негативных последствий, оценивается вероятность несоблюдения обязательных требований.

> В материале вместе разберемся, как по-новому проводит проверки Роскомнадзор: что проверяют, как часто и чьей инициативе, какие документы запрашивает инспектор. Подготовьтесь к проверке Роскомнадзора в 2023 году заранее, чтобы не пришлось платить крупный штраф за нарушение правил обработки персональных данных.

Содержание материала:

1. Виды проверок Роскомнадзора
2. Периодичность плановых проверок Роскомнадзора в 2023 году
3. Как проходит проверка по обработке персональных данных и что проверяют?
4. Оформление результатов проверки Роскомнадзора
5. Как подготовиться к проверке?

Виды проверок Роскомнадзора

Проверки Роскомнадзора бывают плановыми и внеплановыми, документарными и выездными. А с недавних пор появился такой вид проверок, как инспекционный визит.

Плановая проверка

О плановых проверках Роскомнадзор предупреждает заранее. За 3 дня по почте приходит уведомление, в котором указано, какого числа будет проверка. Но каждая компания может заранее узнать, включена ли она в список тех, кого будут проверять в текущем году. План проверок опубликован на сайте Роскомнадзора.

Готовое решение: Как проходят плановые документарные и выездные проверки Роскомнадзора в сфере персональных данных (КонсультантПлюс, 2023) {КонсультантПлюс}

Внеплановая проверка

Часто проводится по жалобам физических лиц. Например, люди могут жаловаться на нежелательную рекламную рассылку, SMS-спам, назойливые телефонные звонки. О внеплановой проверке Роскомнадзор предупреждает за 24 часа.

Готовое решение: Как Роскомнадзор проводит внеплановую выездную проверку в сфере персональных данных (КонсультантПлюс, 2023) {КонсультантПлюс}

Документарная проверка

В этом случае Роскомнадзор запрашивает список документов, копии которых необходимо отослать в территориальный орган Роскомнадзора. Документарная проверка проводится без выезда в организацию.

Выездная проверка

При выездной проверке в компанию приезжают инспекторы. Обычно несколько человек. Инспекторы на месте проверяют, как компания выполняет требования, установленные законом.

Инспекционный визит

Проводится по отношению к организациям, которые отнесены к категориям высокого и значительного риска, а также в отношении контролируемых лиц, приступающих к осуществлению деятельности в сфере обработки персональных данных. О таком визите бизнес должны уведомить не позднее чем за 5 рабочих дней до даты его проведения.

Роскомнадзор также может проводить профилактические мероприятия. К ним относятся:

1. информирование;
2. объявление предостережения;
3. консультирование;
4. профилактический визит;
5. обобщение правоприменительной практики.

В случае и с плановой, и с внеплановой проверкой у компании слишком мало времени на то, чтобы подготовиться и исправить все нарушения. Поэтому делать все нужно заранее.

Справка: Проверки и другие контрольные (надзорные) мероприятия Роскомнадзора в сфере персональных данных (КонсультантПлюс, 2023) {КонсультантПлюс}

Периодичность плановых проверок Роскомнадзора в 2023 году

Как уже говорилось, в 2023 году нет плановых проверок. Однако мораторий на проверки не касается работодателей:

1. которые используют объекты чрезвычайно высокого или высокого рисков;

2. которых по результатам контрольного мероприятия или проверки наказали по КоАП за грубое нарушение, приостановили деятельность или лицензию. При этом с даты окончания мероприятия или проверки прошло менее трех лет;

3. которые осуществляют лицензируемые виды деятельности в части контроля за тем, как они соблюдают лицензионные требования;

4. которые проверят на оказание аудиторских услуг и надзора в области использования атомной энергии.

Плановые проверки Роскомнадзора проводятся с учётом риск-ориентированного подхода. Для этого деятельность в связи с обработкой персональных данных всех организаций и ИП относят к определенной категории риска. Критерии, по которым деятельность относят к определенной категории риска, утвердили постановлением Правительства от 29.06.2021 № 1046. Категория риска зависит от показателя потенциального вреда, который могут причинить ценностям в сфере соблюдения требований к обработке персональных данных.

Выделяют следующие категории риска:

1. высокий — инспекционный визит или выездная проверка один раз в два года;

2. значительный — инспекционный визит или выездная проверка один раз в три года;

3. средний — инспекционный визит или документарная или выездная проверка не чаще чем один раз в четыре года;

4. умеренный — документарная или выездная проверка не чаще чем один раз в шесть лет.

Если деятельность в связи с обработкой персональных данных организации или индивидуального предпринимателя отнесли к категории низкого риска, то плановые надзорные мероприятия у них не проводят (п. 12 положения, утв. постановлением Правительства от 29.06.2021 № 1046).

Чаще всего проверяют операторов, которые:

1. обрабатывают персональные данные в государственных информационных системах;

2. собирают биометрические персональные данные и специальные категории таких данных;

3. передают персональные данные на территорию иностранного государства, которое не обеспечивает необходимую защиту субъекта данных;

4. обрабатывают персональные данные по поручению иностранного госоргана, юридического или физического лица.

Реестр проверок

Можно заранее узнать, нагрянет ли с визитом Роскомнадзор: план проверок утверждается заранее. Узнать, ждать ли проверяющих в текущем году, можно с помощью специального сервиса на сайте Генеральной прокуратуры.

Согласно критериям, которые применяет Роскомнадзор, график проверок может включать как организации, которые подали уведомление об обработке персональных данных в реестр операторов, так и те, кто уведомление не подавал. Чтобы узнать, внесли ли компанию в общий реестр операторов, вбейте в поиск наименование, ИНН и регистрационный номер компании.

Как проходит проверка по обработке персональных данных и что проверяют?

Роскомнадзор уполномочен проводить проверки операторов персональных данных. Ежегодно утверждают новый план мероприятий, выкладываемый в открытый доступ. В 2023 году ведомство проводит проверки по правилам, которые утвердили постановлением Правительства от 29.06.2021 № 1046. Федеральный государственный контроль осуществляют посредством:

1. инспекционного визита;
2. документарной проверки;
3. выездной проверки.

Срок, в течение которого Роскомнадзор и его органы проверят работодателя на обработку персданных, независимо от вида надзорного мероприятия длится не дольше 10 рабочих дней. При этом работодателя должны известить о нём за 24 часа. Для этого контролирующие органы направляют копию приказа о проверке по почте с уведомлением о вручении, по электронной почте с квалифицированной электронной подписью или любым удобным способом (п. 46, 51, 52 положения, утв. постановлением Правительства от 29.06.2021 № 1046).

Несмотря на то, что в 2023 году действует мораторий на проверки, это не значит, что инспекторы Роскомнадзора не смогут прийти в компанию. Запрет касается только плановых проверок, в то время как внеплановые надзорные мероприятия никто не отменял.

Более того, у Роскомнадзора в 2023 году есть основания для внепланового визита. Первое — сотрудники или другие физлица пожалуются на вас в Роскомнадзор. Второй — если будете направлять в Роскомнадзор недостоверные сведения в ответ на запросы (п. 1 Перечня, утв. приказом Минцифры от 15.11.2021 № 1187). До 10 ошибок простят, если их будет больше — придут с проверкой.

Внеплановую проверку проводят по конкретным основаниям:

1. работодатель не исполнил или частично исполнил предписание об устранении нарушений;
2. сотрудник сообщил в ведомство о нарушении;

3. президент и/или правительство поручили провести инспекцию;

4. прокурор инициировал проверку;

5. руководитель Роскомнадзора или его территориального органа вынес такое решение по итогам рассмотрения докладной записки.

Обратите внимание!

В 2023 году появилось новое основание для внеплановой проверки Роскомнадзора. Оно касается аккредитованных IT-компаний, которое допустят утечку персональных данных в интернет (постановление Правительства от 04.02.2023 № 161).

С 1 июля 2021 года плановую выездную проверку могут заменить инспекционным визитом. Он проходит на территории работодателя без предварительного уведомления и длится один рабочий день. В ходе визита проверяющий вправе проводить осмотр, опрос, запрашивать письменные объяснения, а также истребовать документы (ст. 70 Федерального закона от 31.07.2020 № 248-ФЗ, п. 43, 44 положения, утв. постановлением Правительства от 29.06.2021 № 1046).

Работодатель обязан представить инспекторам все необходимые документы и информацию и создать нужные условия для работы. Кроме того, он должен обеспечить доступ проверяющих в помещения и к оборудованию, с помощью которого осуществляют обработку персональных данных.

Что проверяет Роскомнадзор?

1. Уведомление об обработке персональных данных (ПД) и соответствие указанной в нем информации. Роскомнадзор отслеживает актуальность уведомления, поэтому в случае смены цели обработки персональных данных или ответственного лица необходимо предупреждать федеральную службу

2. Перечень работников, допущенных к обработке ПД, и их осведомленность о положениях законодательства РФ о работе с персональными данными и локальных актах организации

3. Пакет учредительных документов предприятия

4. Соглашения о неразглашении ПД, заверенные подписями сотрудников

5. Документы, определяющие порядок обработки, уничтожения, учета, защиты, передачи, а также место хранения ПД, их соответствие действующему законодательству. В организации должны регулярно проводиться внутренние мероприятия по проверке и защите персональных данных, данные должны уничтожаться по достижении цели их получения и обработки, а доступ к помещениям и носителям информации должен быть контролируемым. Причем все эти действия должны быть подкреплены документально.

6. Должностные инструкции и приказы о назначении сотрудников, ответственных за организацию работы с ПД

7. Типовые формы документов, содержащих ПД

8. Перечни используемых средств защиты информации

9. Журналы учёта носителей персональных данных, инструктажей по информационной безопасности и т.д.

10. Наличие разрешения на обработку специальных категорий персональных данных.

11. Соблюдение условий Положения о локализации хранения персональных данных.

На что обращают внимание проверяющие

Первое, на что обратят внимание, - подавала ли компания уведомление в Роскомнадзор, если она не попадает под исключения.

Если уведомление было подано в Роскомнадзор, при проверке инспекторы будут ориентироваться на него и сравнивать его с реальными процессами обработки персональных данных в компании. Если информация не соответствует действительности, например, после подачи уведомления в компании поменялся ответственный за организацию обработки персональных данных, ее могут оштрафовать за то, что в Роскомнадзор вовремя не было отправлено информационное письмо о произошедшем изменении.

Роскомнадзор просматривает сайт компании. Если на сайте организован сбор информации (ФИО, телефон, электронный адрес пользователя), но не опубликована политика компании в отношении обработки персональных данных, компанию могут оштрафовать.

Во время проверки Роскомнадзор может попросить формы документов, в которых

содержатся персональные данные. Например, это могут быть анкеты для соискателей вакантных должностей. Сами формы нужно подготовить заранее. Инспекторам также может быть интересна форма согласия на обработку персональных данных.

Роскомнадзор обращает особое внимание на обработку специальных категорий персональных данных. К ним относится информация о расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, интимной жизни. Такие данные можно собирать только с письменного согласия человека и только на законных основаниях, например, если информация о состоянии здоровья работника нужна работодателю для понимания того, сможет ли он выполнять свои трудовые функции.

Если компания передает персональные данные другим компаниям (например, банкам в рамках зарплатного проекта), то следует обратить внимание на то, как составлен договор с этими компаниями. Согласно ч. 3 ст. 6 152-ФЗ, в договоре должно быть прописано следующее: с какой целью передаются персональные данные другой компании, какие действия она будет совершать с ними, обязанность компании обеспечивать конфиденциальность и безопасность полученных персональных данных. В договоре должно быть указано, что компания, которой передаются персональные данные, принимает правовые, организационные и технические меры для защиты персональных данных.

Помещения, в которых обрабатываются персональные данные, должны быть обеспечены контролируемым доступом. Это значит, что, например, клиент банка не должен иметь возможности подсмотреть персональные данные. Они могут быть доступны только работникам, которые имеют допуск к их обработке.

Также нужно обеспечить раздельное хранение документов, содержащих персональные данные разных физических лиц. То есть личные данные работников должны храниться отдельно от договоров с клиентами. Это могут быть запираемые шкафы или сейфы. В конце рабочего дня документы должны быть убраны. Если Роскомнадзор во время проверки увидит разбросанные документы с персональными данными на столах работников, к компании возникнут вопросы.

Оформление результатов проверки Роскомнадзора

По результатам проверки составляют письменный акт. В нём перечисляют все выявленные нарушения и меры ответственности, применяемые к оператору. Представителя организации знакомят с актом под подпись, а в случае отказа отправляют заверенный акт заказным письмом с уведомлением о вручении. Кроме того, на основании акта выдается предписание об устранении нарушений и протокол об административной ответственности.

Обратите внимание!

В течение 10 рабочих дней с момента получения предписания подать возражение в письменной форме в территориальное управление Роскомнадзора. Подтвердите обоснованность возражений документами и письменными свидетельскими показаниями. Недействительными считаются результаты любой проверки, проведенной с грубыми нарушениями (ст. 20 закона №294-ФЗ).

7 грубых нарушений процедуры проверки Роскомнадзора по персональным данным:

1. отсутствие реальных оснований для проведения контролирующего мероприятия;
2. привлечение экспертов, не аккредитованных в установленном порядке;
3. арушение срока уведомления о предстоящей инспекции;
4. проведение внеплановой выездной проверки по анонимным обращениям;
5. нарушение продолжительности мероприятия (не более 10 рабочих дней в общем случае, не более 50 часов для малого предприятия, не более 15 часов для микропредприятия);
6. запрос документов, не имеющих отношения к предмету проверки;
7. непредставление итогового акта в письменном виде.

Как подготовиться к проверке?

Так как аудит бывает плановым и внеплановым, организациям рекомендуется всегда быть наготове. Кроме того, есть несколько мер, которые помогают подготовиться и пройти аудит.

1. Можно прибегнуть к помощи сторонних специалистов, которые осуществляют сбор необходимой информации, разработку и утверждение пакета документации. Этот метод подходит для тех, кто только начинает работу. В законодательной базе регулярно фиксируются изменения, а федеральная служба строго следит за соблюдением требований законодательства.

2. Самостоятельная подготовка к аудиту не всегда проходит успешно, так как отсутствие квалифицированных специалистов и знаний тонкостей законодательства приводят к ошибкам.

Если Вы все решили сделать сами, самостоятельно, то придется выполнить несколько шагов:

1. определите, кто будет следить за выполнением законодательства в области персональных данных. Часто малый и средний бизнес делегирует эту функцию бухгалтеру, кадровику или юристу. Реже ее берет на себя руководитель. В крупных компаниях вопросами защиты информации может заниматься целый отдел;

2. назначьте ответственного за организацию обработки персональных данных в компании. Скорее всего, это будет тот же человек, который занимается вопросами персональных данных;

3. изучите процесс обработки персональных данных в компании, например, какие персональные данные компания собирает, в каких целях. Компания может собирать персональные данные работников для выполнения трудового законодательства или данные клиентов для выполнения заключенных с ними договоров, ей также могут понадобиться персональные данные соискателей на вакантные должности. Возможно, компания передает эти данные в другую организацию, и тогда возникнет вопрос о получении согласия на передачу персональных данных;

4. на основе полученной информации разработайте пакет документов, включающий политику компании в отношении обработки персональных данных, положение

о неавтоматизированной обработке, приказ о назначении ответственных и ряд других приказов, инструкций и актов. Разработанные документы необходимо утвердить;

5. обязательно ознакомьте с утвержденными документами всех работников, которые имеют к ним отношение. Например, с положением по неавтоматизированной обработке нужно ознакомить только тех работников, которые работают непосредственно с бумажными документами, содержащими персональные данные;

6. основной документ — политику компании в отношении обработки персональных данных — разместите в общедоступном месте, чтобы каждый желающий мог ее прочесть. Лучше всего копию документа разместить на информационном стенде. Если у компании есть сайт, на котором собираются персональные данные пользователей, например, ФИО, телефон и электронные адреса для регистрации, то на сайте также нужно разместить политику, причем там, где она будет заметна пользователю;

7. подайте уведомление в Роскомнадзор об обработке персональных данных. Это можно сделать тремя способами: в бумажном варианте, а также в электронном — на сайте Роскомнадзора или через портал Госуслуг.

Ведомство рассмотрит ваше уведомление и добавит компанию в реестр операторов в течение 30 дней. Присутствие компании в реестре свидетельствует не только о выполнении одного из требований Федерального закона № 152-ФЗ, но и о добропорядочности и прозрачности деятельности компании, что важно для контрагентов.

Вот 3 простых шага для подготовки к проверке Роскомнадзора в 2023 году.

Шаг 1. Проверьте условия хранения электронных и бумажных носителей, содержащих персональные данные. Базы для хранения электронных данных должны иметь многоуровневую систему защиты, сейфы и шкафы для хранения документов — устанавливаться в помещениях ограниченного доступа и снабжаться надежными замками.

Шаг 2. Убедитесь, что на предприятии разработаны все необходимые локальные нормативные акты, ведут учётные журналы, налажен контроль доступа к персональным данным сотрудников.

Шаг 3. Ознакомьте персонал под подпись с положением о защите персональных данных и

другими внутрикорпоративными документами, регулирующими данную сферу. Назначьте ответственного сотрудника письменным приказом.

Важно!

При выявлении нарушений федеральная служба по надзору в сфере связи оформляет акт с предписанием об устранении и передает информацию в суд. Нарушения в области персональных данных караются штрафами от Роскомнадзора в размере до 200 000 рублей должностным лицам, до 6 000 000 рублей – организациям.

Дополнительные полезные материалы из СПС «КонсультантПлюс»:

- *Справка: Проверки и другие контрольные (надзорные) мероприятия Роскомнадзора в сфере персональных данных (КонсультантПлюс, 2023) {КонсультантПлюс}*
- *Готовое решение: Как Роскомнадзор контролирует соблюдение требований в сфере персональных данных (КонсультантПлюс, 2023) {КонсультантПлюс}*
- *Готовое решение: Как проходят плановые документарные и выездные проверки Роскомнадзора в сфере персональных данных (КонсультантПлюс, 2023) {КонсультантПлюс}*
- *Готовое решение: Как Роскомнадзор проводит внеплановую выездную проверку в сфере персональных данных (КонсультантПлюс, 2023) {КонсультантПлюс}*
- *Последние изменения: Проверки Роскомнадзора (контроль (надзор) за соблюдением законодательства о защите персональных данных) (КонсультантПлюс, 2023) {КонсультантПлюс}*