ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ: НОВЫЕ ТРЕБОВАНИЯ

И ОБЯЗАННОСТИ

Защита персональных данных в настоящий момент приобрела приоритетное значение. Поэтому в спешном порядке были подготовлены и приняты поправки в [Закон](https://login.consultant.ru/link/?req=doc&base=LAW&n=422875&date=15.11.2023) о персональных данных 152-ФЗ, большинство из которых вступили в силу с сентября 2022 года, а часть в марте 2023 года. У работодателей появились новые обязанности, законодатели сократили ряд сроков, ввели очередные запреты для операторов ПДн. Проанализирую новшества и расскажу, на что обратить внимание работодателям, операторам ПДн и рядовым гражданам.

Большинство норм Федерального [закона](https://login.consultant.ru/link/?req=doc&base=LAW&n=421898&date=15.11.2023) от 14.07.2022 N 266-ФЗ "О внесении изменений в Федеральный закон "О персональных данных", отдельные законодательные акты Российской Федерации и признании утратившей силу части четырнадцатой статьи 30 Федерального закона "О банках и банковской деятельности" вступили в силу с 1 сентября 2022 года. Некоторые положения вступили в силу с марта 2023 года.

Цель поправок - усиление защиты субъектов персональных данных и обеспечение неприкосновенности их частной жизни. Дело в том, что в последнее время появилось множество сервисов в Интернете, которые незаконно собирают, хранят и распространяют персональную информацию о гражданах, включая паспортные данные, сведения о недвижимости, перелетах и иные личные сведения. В частности, потеря анонимности, влекущая раскрытие персональных данных военнослужащих и их семей, создает непосредственную угрозу их жизни и безопасности в текущих непростых условиях.

Более того, нелегальные сервисы, как правило, расположены за пределами РФ и потому не подпадают под ее юрисдикцию. Трансграничная передача ПДн нашими законами практически не регулируется, а осуществляется большим количеством операторов повсеместно и в больших масштабах.

Рассмотрим подробнее, какие меры ввело государство для защиты персональных данных и что это значит для работодателей, операторов ПДн и рядовых граждан.

Теперь с Роскомнадзором должны быть согласованы все нормативные правовые акты РФ, затрагивающие вопросы:

- трансграничной передачи персональных данных;

- обработки специальных категорий данных (например, состояние здоровья человека);

- биометрических данных;

- персональных данных несовершеннолетних лиц;

- а также вопросы предоставления и распространения персональных данных, полученных в результате обезличивания.

У ведомства по [Закону](https://login.consultant.ru/link/?req=doc&base=LAW&n=422241&date=15.11.2023&dst=63&field=134) будет 30 дней на согласование проекта документа.

Новые запреты

В договор с субъектом персональных данных нельзя включать следующие условия ([п. 5 ч. 1 ст. 6](https://login.consultant.ru/link/?req=doc&base=LAW&n=422241&date=15.11.2023&dst=64&field=134) Закона N 152-ФЗ):

- ограничивающие его права и свободы. Например, на отзыв согласия на обработку ПДн или соблюдение дополнительных условий для такого отзыва, включая значительный срок, за который нужно подать уведомление оператору;

- устанавливающие случаи обработки ПДн несовершеннолетних лиц, если иное не предусмотрено законодательством РФ;

- допускающие в качестве условия заключения договора бездействие субъекта персональных данных. Например, раньше в договорах банковского вклада некоторые банки нередко включали условие, что при несогласии вкладчика с обработкой его персональных данных, включая биометрические, он должен прямо об этом в договоре написать, в ином случае согласие считается полученным. Теперь так делать нельзя.

Поручение по обработке ПДн

Новая редакция [ч. 3 ст. 6](https://login.consultant.ru/link/?req=doc&base=LAW&n=422241&date=15.11.2023&dst=65&field=134) Закона N 152-ФЗ более детально регламентирует вопросы поручения оператором обработки ПДн субъектов иным лицам, в том числе государственным и муниципальным органам власти. Лицо, которому поручается обработка, должно обеспечить базовые принципы обработки данных, их конфиденциальность, принимать меры к выполнению всех своих обязанностей.

В самом поручении на обработку нужно определить:

- перечень данных;

- перечень действий по их обработке;

- цели и иные обязательные требования;

- право оператора и обязанность лица, которому поручается обработка, предоставлять документы и информацию, подтверждающие выполнение обязательных требований.

Естественно, оператору не стоит ограничиваться только поручением, а рекомендуется заключить договор и оформить соответствующие отношения как обязательства.

Также на случай нарушения условий договора можно предусмотреть, что он в качестве имущественных потерь возместит все суммы штрафов, компенсаций и иных расходов и других убытков, которые возникнут в связи с предъявлением требований со стороны субъектов персональных данных и контролирующих органов ([ст. 406.1](https://login.consultant.ru/link/?req=doc&base=LAW&n=410706&date=15.11.2023&dst=10698&field=134) ГК РФ). Такое договорное условие позволит оператору ПДн создать источник возмещения за счет лица, которому поручена обработка ПДн.

К кому требования о распространении Пдн не относятся

Требования [ст. 10.1](https://login.consultant.ru/link/?req=doc&base=LAW&n=422241&date=15.11.2023&dst=34&field=134) Закона N 152-ФЗ об особенностях обработки ПДн путем распространения не применяются в случае обработки ПДн в целях выполнения возложенных законодательством Российской Федерации на государственные органы, муниципальные органы, а также на подведомственные таким органам организации функций, полномочий и обязанностей.

Форма согласия на распространение таких ПДн не утверждена, однако ее содержание можно определить на основании требований [ст. 10.1](https://login.consultant.ru/link/?req=doc&base=LAW&n=422875&date=15.11.2023&dst=34&field=134) Закона о ПДн и [Приказа](https://login.consultant.ru/link/?req=doc&base=LAW&n=382687&date=15.11.2023) Роскомнадзора N 18. Самое главное - согласие на распространение таких персональных данных оформляется отдельно от иных согласий.

Оператор должен предоставить субъекту возможность определить перечень персональных данных по каждой категории, указанной в согласии на обработку персональных данных, разрешенных гражданином для распространения. В документе должны быть указаны: Ф.И.О., контактная информация субъекта (телефон, электронная почта или почтовый адрес); сведения об операторе (наименование, адрес из ЕГРЮЛ, ИНН, ОГРН) и его информационных ресурсах (например: https://... http://www...); цели обработки персональных данных, их категории и перечень с выделением тех данных, для которых предусматриваются особые условия и запреты, связанные с обработкой, а также срок действия согласия.

Биометрические ПДн

Согласно новой [ч. 3 ст. 11](https://login.consultant.ru/link/?req=doc&base=LAW&n=422241&date=15.11.2023&dst=69&field=134) Закона N 152-ФЗ получение биометрических персональных данных обязательным не является. Подобное уточнение совсем не лишнее, учитывая, что банки и иные профессиональные участники рынка их собирают, но при этом многие из них, к сожалению, так и не научились должным образом их защищать.

Поэтому граждане теперь могут отказываться предоставлять биометрические данные. А организация будет не вправе на этом основании отказать в заключении договора. Такой отказ будет считаться незаконным (см. также информацию на сайте Минцифры России (<https://digital.gov.ru/ru/events/41802/)>).

Трансграничная передача ПДн

С 1 марта 2023 года начали действовать новые правила, приходится ориентироваться на перечень иностранных государств, которые обеспечивают адекватную защиту прав субъектов персональных данных, такой перечень формирует и ведет Роскомнадзор.

Кроме того, до начала трансграничной передачи данных о своем намерении это делать нужно будет уведомить Роскомнадзор. Уведомление придется подавать отдельным документом, а не вместе с общим уведомлением о намерении осуществлять обработку персональных данных. Это сделано для того, чтобы вовремя вмешаться и предотвратить возможные нарушения прав субъектов персональных данных. Очевидно.

Наиболее сложным нововведением является требование к оператору до подачи уведомления получить от органов власти иностранных государств, иностранных физических или юридических лиц сведения:

- о принимаемых мерах по защите прав субъектов персональных данных;

- о правовом регулировании ПДн в иностранном государстве;

- об органах власти иностранного государства, иностранных юридических и физических лицах, которым будут передаваться данные.

Причем Роскомнадзор может принять отказное решение, запрещающее трансграничную передачу данных, в целях защиты основ конституционного строя, безопасности жизни и здоровья граждан, а также в иных значимых целях. На принятие решения дается 10 рабочих дней (с момента поступления уведомления). При положительном решении регулятора оператор может осуществлять трансграничную передачу ПДн на тех территориях и в том объеме, которые указаны в решении Роскомнадзора.

Взаимодействие с ГосСОПКА

На оператора теперь возложена обязанность обеспечивать взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ - ГосСОПКА (см. [ст. 5](https://login.consultant.ru/link/?req=doc&base=LAW&n=220885&date=15.11.2023&dst=100028&field=134) Федерального закона от 26.07.2017 N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации"), включая информирование о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных ([ч. 12 ст. 19](https://login.consultant.ru/link/?req=doc&base=LAW&n=422875&date=15.11.2023&dst=77&field=134) Закона N 152-ФЗ).

Порядок такого взаимодействия определён приказом ФСБ России от 13.02.2023 № 77. Такая мера позволяет повысить гарантии информационной безопасности нашей страны в целом за счет эффективной и слаженной защиты всех ее информационных элементов на самых различных уровнях, а также позволяет более плотно вовлечь операторов в юридически значимые для органов власти процессы.

Оператор обязан незамедлительно сигнализировать о компьютерных инцидентах, повлекших неправомерную передачу ПДн.

В данном случае рассматривается статус оператор ПДн: оператор, который взаимодействует с Национальным координационным центром по компьютерным инцидентам (НКЦКИ), и который не взаимодействует.

В течение 24 часов с момента обнаружения инцидента обязан направить информацию об инциденте, путем заполнения формы на официальном сайте Роскомнадзора в информационно-телекоммуникационной сети «Интернет».

В течение 72 часов – уведомление о результатах внутреннего расследования, а также сведения о лицах, действия которых стали причиной инцидента. Уведомление заполняется также на официальном сайте Роскомнадзора.

Новые сроки

Оператору персональных данных стоит иметь в виду, что с 1 сентября 2022 года сократились сроки некоторых действий ([ч. 1](https://login.consultant.ru/link/?req=doc&base=LAW&n=422875&date=15.11.2023&dst=80&field=134), [2](https://login.consultant.ru/link/?req=doc&base=LAW&n=422875&date=15.11.2023&dst=81&field=134), [4 ст. 20](https://login.consultant.ru/link/?req=doc&base=LAW&n=422875&date=15.11.2023&dst=82&field=134) Закона N 152-ФЗ) с 30 до 10 рабочих дней. Так, оператору в этот период необходимо:

- ответить на обращение субъекта персональных данных по поводу того, обрабатывает ли он его данные, и если да, то предоставить к ним доступ;

- дать мотивированный ответ об отказе предоставить информацию о наличии обрабатываемых ПДн;

- сообщить Роскомнадзору необходимые сведения по его запросу.

При обращении субъекта ПДн к оператору с требованием прекратить их обработку последний обязан это сделать в течение 10 рабочих дней. Этот срок может быть продлен, но не более чем на пять рабочих дней, при этом придется направить гражданину мотивированное уведомление с указанием причин такой меры ([ч. 5.1 ст. 21](https://login.consultant.ru/link/?req=doc&base=LAW&n=422875&date=15.11.2023&dst=86&field=134) Закон N 152-ФЗ). Невыполнение данных требований будет свидетельствовать о нарушении закона со стороны оператора, в связи с чем Роскомнадзор может его привлечь к административной ответственности по [ст. 13.11](https://login.consultant.ru/link/?req=doc&base=LAW&n=427416&date=15.11.2023&dst=7755&field=134) КоАП РФ.

Чем подтвердить факт удаления персональных данных?

Персональные данные нужно уничтожать, если они собраны незаконно, если достигнуты цели их сбора и если этого требует сам владелец данных. Роскомнадзор издал приказ от 28.10.2022 № 179 «Об утверждении требований к подтверждению уничтожения персональных данных».

Уничтожение персональных данных означает уничтожение документов, в которых эти данные хранятся. Бумажные документы могут быть сожжены, измельчены на шредере и т.п. Электронные - удалены, затерты и т.п.

Как правило, персональные данные хранятся с момента их получения до момента, когда утрачена цель их обработки. После этого в течение 30 дней персональные данные должны быть уничтожены ([ч. 4](https://login.consultant.ru/link/?req=doc&base=LAW&n=422875&date=15.11.2023&dst=100401&field=134), [5 ст. 21](https://login.consultant.ru/link/?req=doc&base=LAW&n=422875&date=15.11.2023&dst=100402&field=134) Закона N 152-ФЗ). Кроме того, сами работники, в первую очередь уволенные, могут потребовать прекратить хранение их персональных данных.

В каких случаях персональные данные нужно уничтожить:

- их обработали неправомерно ([ч. 3 ст. 21](https://login.consultant.ru/link/?req=doc&base=LAW&n=422875&date=15.11.2023&dst=100400&field=134) Закона N 152-ФЗ);

- достигнуты цели, ради которых собирались и обрабатывались данные ([ч. 4 ст. 21](https://login.consultant.ru/link/?req=doc&base=LAW&n=422875&date=15.11.2023&dst=100401&field=134) Закона N 152-ФЗ);

- владелец данных требует уничтожить их ([ч. 1 ст. 14](https://login.consultant.ru/link/?req=doc&base=LAW&n=422875&date=15.11.2023&dst=100318&field=134), [ч. 3 ст. 20](https://login.consultant.ru/link/?req=doc&base=LAW&n=422875&date=15.11.2023&dst=100395&field=134) Закона N 152-ФЗ);

- владелец данных отзывает согласие на обработку данных ([ч. 5 ст. 21](https://login.consultant.ru/link/?req=doc&base=LAW&n=422875&date=15.11.2023&dst=100402&field=134) Закона N 152-ФЗ).

Акт об уничтожении персональных данных должен содержать:

- наименование или Ф.И.О. (при наличии) и адрес оператора;

- наименование или Ф.И.О. (при наличии), адрес лица, осуществляющего обработку персональных данных субъекта персональных данных по поручению оператора (если обработка поручена такому лицу);

- Ф.И.О. (при наличии) субъекта или иную информацию, относящуюся к определенному физическому лицу, чьи персональные данные были уничтожены;

- Ф.И.О. (при наличии), должности лиц, уничтоживших персональные данные субъекта персональных данных, а также их подписи;

- перечень уничтоженных персональных данных;

- наименование уничтоженного материального носителя, содержащего персональные данные, с указанием количества листов в отношении каждого материального носителя (в случае обработки персональных данных без использования средств автоматизации);

- наименование информационной системы персональных данных, из которой были уничтожены персональные данные субъекта персональных данных (в случае обработки персональных данных с использованием средств автоматизации);

- способ уничтожения персональных данных;

- причину уничтожения персональных данных;

- дату уничтожения персональных данных.

Акт может быть оформлен на бумаге или в электронном формате (ЭЦП).

Если персональные данные обрабатывались в собственной электронной системе или БД, нужно составить акт уничтожения и выгрузку данных из журнала регистрации событий в информационной системе персональных данных.

Файл должен содержать:

- Ф.И.О. (при наличии) субъекта или иную информацию, относящуюся к определенному физическому лиц;

- перечень уничтоженных данных;

- причину уничтожения персональных данных.

Уведомление об обработке персональных данных

Оператор до начала обработки персональных данных [обязан](https://login.consultant.ru/link/?req=doc&base=LAW&n=310343&date=09.03.2023&dst=100012&field=134) уведомить РКН о своем намерении осуществлять обработку персональных данных, за исключением случаев:

если осуществляется обработка ПДн, включенных в государственные информационные системы персональных данных, созданные в целях защиты безопасности государства и общественного порядка;

если оператор осуществляет деятельность по обработке персональных данных исключительно без использования средств автоматизации;

и в случаях, предусмотренных [законодательством](https://login.consultant.ru/link/?req=doc&base=LAW&n=174687&date=09.03.2023&dst=4&field=134) Российской Федерации о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

Во всех остальных случаях уведомление ОБЯЗАТЕЛЬНО!!!

Новые формы уведомления утверждены приказом РКН от 28.10.2022 № 180.

Сроков переподачи уведомлений по новой форме пока нет, но есть сроки уведомления РКН об изменениях данных, содержащихся в уведомлениях: не позднее 15 числа месяца, следующего за месяцем, в котором произошли изменения. Уведомление направляется в виде документа на бумажном носителе или в форме электронного документа и подписывается уполномоченным лицом. Уведомление необходимо заполнять на официальном сайте Роскомнадзора.

В случае прекращения обработки персональных данных оператор обязан уведомить РКН в течение 10 рабочих дней с даты прекращения обработки персональных данных.

Меры, направленные на обеспечение выполнения оператором обязанностей, предусмотренных настоящим Федеральным законом

1. Оператор обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей. Оператор самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей. К таким мерам, в частности, относятся:

1) назначение оператором, являющимся юридическим лицом, ответственного за организацию обработки персональных данных;

2) издание оператором, являющимся юридическим лицом, документов, определяющих политику оператора в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, определяющих для каждой цели обработки персональных данных категории и перечень обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, способы, сроки их обработки и хранения, порядок уничтожения персональных данных при достижении целей их обработки или при наступлении иных законных оснований, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений. Такие документы и локальные акты не могут содержать положения, ограничивающие права субъектов персональных данных, а также возлагающие на операторов не предусмотренные законодательством Российской Федерации полномочия и обязанности;

3) применение правовых, организационных и технических мер по обеспечению безопасности ПДн;

4) осуществление внутреннего контроля и (или) аудита;

5) оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения 152-ФЗ. Приказом РКН от 27.10.2022 № 178 определены требования к этой оценке. Требованиями определяется 3 степени вреда: высокий, средний, низкий. Каждая из степеней расписана. Позиция РКН: если возможный вред не соответствует ни одной из определённых степеней вреда, оценка все равно должна быть проведена (указывается, что вред не может быть причинён). Данная оценка должна быть проведена до 01.03.2023.

6) ознакомление работников оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, и (или) обучение указанных работников.

2. Оператор обязан опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных.

Оператор, осуществляющий сбор персональных данных с использованием Интернета, обязан опубликовать на страницах, с использованием которых осуществляется сбор персональных данных, документ, определяющий его политику в отношении обработки персональных данных.

3. Правительство Российской Федерации устанавливает [перечень](https://login.consultant.ru/link/?req=doc&base=LAW&n=322830&date=09.03.2023&dst=100008&field=134) мер, направленных на обеспечение выполнения обязанностей, предусмотренных настоящим Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами. Это постановление Правительства Российской Федерации от 21 марта 2012 года № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

4. Оператор обязан подтвердить принятие мер, по запросу уполномоченного органа по защите прав субъектов персональных данных. Напомню это 10 рабочих дней.

Меры по обеспечению безопасности персональных данных при их обработке

Обеспечение безопасности персональных данных достигается, в частности:

1) определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России 05.02.2021 разработала новую методику оценки угроз безопасности информации; Методики и модель 2007 года признаны утратившими силу.

2) применением организационных и технических мер при их обработке в информационных системах персональных данных;

3) применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

4) оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

5) учетом машинных носителей персональных данных;

6) обнаружением фактов несанкционированного доступа к персональным данным и принятием мер, в том числе мер по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные системы персональных данных и по реагированию на компьютерные инциденты в них;

7) восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

8) установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

9) контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

3. Правительство Российской Федерации с учетом возможного вреда субъекту персональных данных, объема и содержания обрабатываемых персональных данных, вида деятельности, при осуществлении которого обрабатываются персональные данные, актуальности угроз безопасности персональных данных устанавливает:

1) [уровни защищенности](https://login.consultant.ru/link/?req=doc&base=LAW&n=137356&date=09.03.2023&dst=100025&field=134) персональных данных при их обработке в информационных системах персональных данных в зависимости от угроз безопасности этих данных (ПП от 01.11.2012 № 1119);

2) [требования](https://login.consultant.ru/link/?req=doc&base=LAW&n=137356&date=09.03.2023&dst=100009&field=134) к защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;

3) [требования](https://login.consultant.ru/link/?req=doc&base=LAW&n=140009&date=09.03.2023&dst=100009&field=134) к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных.

**Так же хочу обратить Ваше внимание на следующее:**

1. С 13 сентября 2021 года по инициативе Роскомнадзора создан Центр правовой помощи гражданам в цифровой среде. Юристы Центра оказывают бесплатную консультацию, помогают:

* прекратить незаконную обработку и распространение персональных данных граждан;
* аннулировать кредиты, оформленные мошенническим путем;
* подготовить документы в органы правопорядка, прокуратуру, операторам персональных данных, в суды и кредитные организации;
* защитить интересы человека в суде, если обращения в другие организации не помогли;
* добиться компенсации морального вреда.

2. Приказом Минцифры России от 17.08.2023 № 720 установлен новый индикатор риска, выявление которого может **привести к проверке, а именно:**

Если  РКН обнаружил хотя бы 3 расхождения между данными, которые оператор опубликовал на своем сайте в силу обязанности и информацией из уведомлений о намерении обрабатывать персональные данные и (или) осуществлять их трансграничную передачу, он может  провести внеплановую проверку (по согласованию с прокуратурой).

3. Не забываем, что при предоставлении государственных и муниципальных услуг, выполнении государственного или муниципального задания, **существует запрет** на использование принадлежащих иностранным юридическим лицам и (или) иностранным гражданам информационных систем для передачи платежных документов и (или) предоставления информации, содержащей персональные данные граждан Российской Федерации, данные о переводах денежных средств в рамках применяемых форм безналичных расчетов, сведения, необходимые для осуществления платежей и (или) сведения о счетах (вкладах) граждан Российской Федерации в банках. (Административный штраф: на должностных лиц: от 30 тыс. рублей до 50 тыс. рублей; на юридических лиц: от 100 тыс. рублей до 700 тыс. рублей).

В него вошли:

1. Discord;

2. Microsoft Teams;

3. Skype;

4. Snapchat;

5. Telegram;

6. Threema;

7. Viber;

8. WhatsApp;

9. WeChat.

4. По состоянию на сегодня с 1 января 2024 года планируется снятие моратория на проведение проверок.