РОСКОМНАДЗОР

Актуальные вопросы в сфере обработки персональных данных

Управление Роскомнадзора по Томской области

2023

Нормативно-правовые акты, регулирующие деятельность по обработке персональных данных

1. Конституция РФ от 12.12.1993;
2. Конвенция о защите ФЛ при автоматизированной обработке ПД от 28.01.1981 № 108;
3. Трудовой кодекс РФ (глава 14);
4. ***Федеральный закон «О персональных данных» от 27.07.2006 №152-ФЗ» (далее – 152-ФЗ)***
5. Указ Президента РФ «О перечне сведений конфиденциального характера» от 06.03.1997 №188;
6. ***Постановление Правительства РФ «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» от 15.09.2008 № 687;***
7. Постановление Правительства РФ «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных» от 06.07.2008 № 512;
8. Постановление Правительства РФ «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 01.11.2012 № 1119;
9. Постановление Правительства РФ от 21.03.2012 №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».

Персональные данные (далее – ПД)

- любая информация, относящаяся к прямо или косвенно ***определенному*** или ***определяемому*** физическому лицу (субъекту персональных данных),

В том числе:

- *фамилия, имя, отчество;*
- *дата рождения;*
- *адрес местожительства;*
- *паспортные данные, СНИЛС, ИНН;*
- *социальное, имущественное, семейное положение;*
- *сведения о доходах, образовании, профессии*
- *номер банковской карты;*
- *фотографические изображения;*
- *и другие.*

Специальные категории персональных данных

- *расовая принадлежность;*
- *национальная принадлежность;*
- *религиозные убеждения;*
- *философские убеждения;*
- *политические взгляды;*
- *состояние здоровья;*
- *состояние интимной жизни.*

Биометрические персональные данные

Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных:

- *отпечатки пальцев;*
- *материалы ДНК;*
- *фото-видеоизображение и т.д...*

Обработка персональных данных

– любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая

- *сбор,*
- *запись,*
- *систематизацию,*
- *накопление,*
- *хранение,*
- *уточнение (обновление, изменение),*
- *извлечение,*
- *использование,*
- *передачу (распространение, предоставление, доступ),*
- *обезличивание,*
- *блокирование,*
- *удаление,*
- *уничтожение персональных данных.*

Кто такой оператор ПД?

Оператор персональных данных – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных.

Обязанности Операторов

- Представить **Уведомление**

  Оператор **до начала** обработки персональных данных обязан уведомить уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных. (ч. 1 ст. 22 152-ФЗ)

- Представить **Уведомление об изменении сведений, содержащихся в уведомлении**

  В случае изменения сведений, указанных в Уведомлении, Оператор обязан уведомить уполномоченный орган по защите прав субъектов персональных данных обо всех произошедших изменениях не позднее 15-го числа месяца, следующего за месяцем, в котором возникли такие изменения. В случае прекращения обработки персональных данных оператор обязан уведомить об этом уполномоченный орган по защите прав субъектов персональных данных в течение десяти рабочих дней с даты прекращения обработки персональных данных.(ч. 7 ст. 22 152-ФЗ)

Оператор вправе осуществлять обработку ПД без уведомления уполномоченного органа по защите прав субъектов ПД (ч.2 ст. 22 152-ФЗ):

- 1) включенных в государственные информационные системы персональных данных, созданные в целях защиты безопасности государства и общественного порядка;
- 2) в случае, если оператор осуществляет деятельность по обработке персональных данных исключительно без использования средств автоматизации;
- 2) обрабатываемых в случаях, предусмотренных законодательством 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.

Форма Уведомления / Уведомления об изменении сведений
установлена **Приказом Роскомнадзора от 28.10.2022 №180, вступившим в силу 26.12.2022**

Форму Уведомления/Уведомления об изменении сведений, содержащихся в уведомлении о намерении осуществлять обработку персональных данных, и рекомендации по заполнению можно найти на официальном сайте Управления Роскомнадзора по ТО: **https://70.rkn.gov.ru**

Оператору предоставлена возможность сформировать Уведомление в электронной форме и направить в его в территориальный орган Роскомнадзора одним из следующих способов:

1. сформировать Уведомление и направить в бумажном виде;

2. сформировать Уведомление и направить в электронном виде с использованием усиленной квалифицированной электронной подписи;

3. сформировать Уведомление и направить в электронном виде с использованием средств аутентификации ЕСИА.

Состав сведений, содержащихся в Уведомлении, изменился с 26.12.2022!

Основное изменение:

ч. 3.1. ст. 22 152-ФЗ: Оператор для каждой цели обработки персональных данных указывает категории персональных данных, категории субъектов, персональные данные которых обрабатываются, правовое основание обработки персональных данных, перечень действий с персональными данными, способы обработки персональных данных (часть 3.1 введена Федеральным законом от 14.07.2022 N 266-ФЗ).

с 01.03.2023 для Операторов, осуществляющих трансграничную передачу персональных данных, введена обязанность до начала осуществления деятельности по трансграничной передаче персональных данных уведомить уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять трансграничную передачу персональных данных (ст. 12 Федерального закона №152-ФЗ)

Меры, направленные на исполнение Оператором его законных обязанностей *(ч. 1 ст. 18.1)*

Оператор ***обязан*** принимать меры, **необходимые и достаточные** для обеспечения выполнения обязанностей, предусмотренных Федеральным законом № 152-ФЗ и принятыми в соответствии с ним нормативными правовыми актами.

Оператор **самостоятельно определяет состав и перечень мер**, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Федеральным законом № 152-ФЗ и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено федеральным законодательством.

ВАЖНО! Оператор при поступлении запроса от Уполномоченного органа по защите прав субъектов ПД **обязан представить документы и локальные акты**, и (или) **иным образом подтвердить принятие мер**, ***указанных в ч. 1 ст. 18.1 152-ФЗ***

Меры, направленные на исполнение Оператором его законных обязанностей

(ч. 1 ст. 18.1 Федерального закона №152-ФЗ)

1. ***Назначение*** оператором, являющимся юридическим лицом, ***ответственного за организацию*** обработки ПД;
2. ***Издание*** оператором, являющимся юридическим лицом, документов, определяющих ***политику оператора в отношении обработки ПД***, локальных актов по вопросам обработки ПД, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства РФ, устранение последствий таких нарушений;
3. ***Применение*** правовых, организационных и технических ***мер по обеспечению безопасности*** ПД в соответствии со ст. 19 (при использовании информационных систем) ;
4. ***Осуществление внутреннего контроля и (или) аудита*** соответствия обработки ПД Федеральному закону № 152-ФЗ и принятым в соответствии с ним нормативным правовым актам, требованиям к защите ПД, политике оператора в отношении обработки ПД, локальным актам оператора;
5. ***Оценка вреда***, который может быть причинен субъектам ПД в случае нарушения Федерального закона № 152-ФЗ, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом № 152-ФЗ ;
6. ***Ознакомление работников*** оператора, *непосредственно осуществляющих обработку ПД*, ***с положениями законодательства*** РФ о ПД, в том числе требованиями к защите ПД, документами, определяющими политику оператора в отношении обработки ПД, локальными актами по вопросам обработки ПД, и (или) обучение указанных работников.

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

- Оператор, осуществляющий сбор ПД ***с использованием информационно-телекоммуникационных сетей***, ***обязан опубликовать в соответствующей информационно-телекоммуникационной сети документ, определяющий его политику*** в отношении обработки ПД, и сведения о реализуемых требованиях к защите ПД, а также ***обеспечить возможность доступа к указанному документу с использованием средств соответствующей информационно-телекоммуникационной сети***.

Меры по обеспечению безопасности ПД при их обработке, осуществляемой **без** использования средств автоматизации

- Обработка ПД, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в **отношении каждой категории** ПД ***можно было определить места хранения ПД*** (материальных носителей) ***и установить перечень лиц***, осуществляющих обработку ПД либо имеющих к ним доступ.
- Необходимо обеспечивать ***раздельное хранение*** ПД (материальных носителей), обработка которых осуществляется в различных целях.
- При хранении материальных носителей **должны соблюдаться условия, обеспечивающие сохранность** ПД и **исключающие несанкционированный** к ним доступ. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются оператором.

Требования к обработке ПД

1. Оператор обязан обеспечить обработку ПД граждан РФ с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, предусмотренных Федеральным законом № 152-ФЗ; (п.5 ст.18 152-ФЗ)
2. Операторы и иные лица, получившие доступ к ПД, обязаны не раскрывать третьим лицам и не распространять ПД без согласия субъекта ПД, если иное не предусмотрено федеральным законом. (ст. 7 152-ФЗ)
3. Оператор вправе поручить обработку ПД другому лицу **с согласия** субъекта ПД, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, либо путем принятия государственным или муниципальным органом соответствующего акта. Лицо, осуществляющее обработку ПД по поручению оператора, обязано соблюдать принципы и правила обработки ПД, предусмотренные Федеральным законом № 152-ФЗ.

Лица, ответственные за организацию обработки персональных данных

- Лицо, ответственное за организацию обработки персональных данных, в частности, *обязано*:
  1. **осуществлять внутренний контроль за соблюдением** оператором и его работниками **законодательства РФ** о ПД, в том числе требований к защите ПД;
  2. **доводить до сведения** работников оператора **положения законодательства** РФ о ПД, локальных актов по вопросам обработки ПД, требований к защите ПД;
  3. **организовывать прием и обработку обращений и запросов** субъектов ПД или их представителей и (или) **осуществлять контроль за приемом и обработкой** таких обращений и запросов

Согласие на обработку персональных данных субъекта ПД

Согласно ч. 1 ст. 9 Федерального закона №152-ФЗ субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку персональных данных должно быть конкретным, предметным, информированным, сознательным и однозначным. Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем **в любой позволяющей подтвердить факт его получения форме,** если иное не установлено федеральным законом

Согласие на обработку персональных данных субъекта ПД

Требуется **всегда**,

за исключением случаев, установленных в ч. 1 ст. 6 Федерального закона №152-ФЗ

Письменное согласие на обработку персональных данных

- В случаях, предусмотренных федеральным законом, обработка персональных данных **осуществляется только с согласия в письменной форме** (или в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью):

– включение в общедоступные источники персональных данных (в том числе справочники, адресные книги) (ст. 8 Федерального закона № 152-ФЗ);

– обработка специальных категорий персональных данных (ст. 10 Федерального закона № 152-ФЗ);

– обработка персональных данных, разрешенных субъектом персональных данных для распространения (ст. 10.1 Федерального закона № 152-ФЗ);

– обработка биометрических персональных данных (ст. 11 Федерального закона № 152-ФЗ);

– трансграничная передача персональных данных на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных данных (ст. 12 Федерального закона № 152-ФЗ);

– принятие решения на основании исключительно автоматизированной обработки персональных данных, порождающего юридические последствия в отношении субъекта персональных данных или иным образом затрагивающее его права (ст. 16 Федерального закона № 152-ФЗ).

Требования к письменному согласию указаны в ч. 4 ст. 9 Федерального закона №152-ФЗ.

Письменное согласие,

содержащее **НЕ ВСЕ** указанные сведения,

признается **НЕ соответствующим** законодательству.

Особенности обработки персональных данных, разрешенных субъектом персональных данных для распространения

(ст. 10.1 Федерального закона № 152-ФЗ, введена в действие с 01.03.2021)

- Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения, оформляется **отдельно** от иных согласий субъекта персональных данных на обработку его персональных данных.
- **В случае раскрытия персональных данных неопределенному кругу лиц самим субъектом персональных данных** без предоставления оператору согласия, предусмотренного настоящей статьей, обязанность предоставить доказательства законности последующего распространения или иной обработки таких персональных данных лежит на каждом лице, осуществившем их распространение или иную обработку.
- **Требования к содержанию согласия** на обработку персональных данных, разрешенных субъектом персональных данных для распространения, определены Приказом Роскомнадзора от 24.02.2021 №18.
- Требование получения отдельного согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения, **не применяются** в случае обработки персональных данных в целях выполнения возложенных законодательством Российской Федерации на государственные органы, муниципальные органы, а также на подведомственные таким органам организации функций, полномочий и обязанностей.

Основные изменения, внесенные в Федеральный закон №152-ФЗ Федеральным законом от 14.07.2022 N 266-ФЗ

- **Введена ч. 3.1. ст. 21, устанавливающая обязанности Оператора в случае утечек персональных данных: Приказ Роскомнадзора от 14.11.2022 №187**

В случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных, оператор обязан с момента выявления такого инцидента оператором, уполномоченным органом по защите прав субъектов персональных данных или иным заинтересованным лицом уведомить уполномоченный орган по защите прав субъектов персональных данных:

1) в течение двадцати четырех часов о произошедшем инциденте, о предполагаемых причинах, повлекших нарушение прав субъектов персональных данных, и предполагаемом вреде, нанесенном правам субъектов персональных данных, о принятых мерах по устранению последствий соответствующего инцидента, а также предоставить сведения о лице, уполномоченном оператором на взаимодействие с уполномоченным органом по защите прав субъектов персональных данных, по вопросам, связанным с выявленным инцидентом;

2) в течение семидесяти двух часов о результатах внутреннего расследования выявленного инцидента, а также предоставить сведения о лицах, действия которых стали причиной выявленного инцидента (при наличии).

- **Введена ч. 7 ст. 22, устанавливающая требования к подтверждению уничтожения персональных данных**

Подтверждение уничтожения персональных данных осуществляется в соответствии с требованиями, установленными уполномоченным органом по защите прав субъектов персональных данных **(приказ Роскомнадзора от 22.10.2022 №179).**

- **ч. 2 ст. 18.1 устанавливает требования к Политике Оператора:**

для каждой цели обработки персональных должны быть указаны 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.

Ответственность за нарушения в области персональных данных

Нарушение требований законодательства в области персональных данных влечет гражданскую, уголовную, административную, дисциплинарную ответственность юридических физических и должностных лиц.

Ответственность Оператора по ст. 13.11 КоАП РФ

НАРУШЕНИЕ 1 (ч. 1 ст. 13.11 КоАП РФ):

Обработка ПД *в случаях, не предусмотренных законодательством* РФ в области ПД, либо обработка ПД, *несовместимая с целями сбора ПД*, за исключением случаев, предусмотренных законом, если эти действия не содержат уголовно наказуемого деяния.

На основании ч. 3.5 ст. 28.1 КоАП РФ привлечение к административной ответственности возможно без проведения контрольных (надзорных) мероприятий (КНМ) в случае поступления от Оператора данных, подтверждающих наличие события правонарушения)

(ч.1.1 ст. 13.11 КоАП РФ: повторное совершение административного правонарушения, предусмотренного ч.1 ст. 13.11 КоАП РФ)

НАРУШЕНИЕ 2 (ч. 2 ст. 13.11 КоАП РФ):

Обработка Персональных данных без согласия в письменной форме

Обработка ПД *без согласия в письменной форме* субъекта ПД на обработку его ПД в случаях, когда такое согласие должно быть получено в соответствии с законодательством Российской Федерации в области персональных данных, за исключением случаев, предусмотренных ст. 17.13. КоАП РФ, если эти действия не содержат уголовно наказуемого деяния, либо обработка ПД с нарушением установленных законодательством Российской Федерации в области ПД *требований к составу сведений,* включаемых в согласие в письменной форме субъекта ПД на обработку его персональных данных, -

На основании ч. 3.5 ст. 28.1 КоАП РФ привлечение к административной ответственности возможно без проведения контрольных (надзорных) мероприятий (КНМ) в случае поступления от Оператора данных, подтверждающих наличие события правонарушения)

(ч.2.1 ст. 13.11 КоАП РФ: повторное совершение административного правонарушения, предусмотренного ч.2 ст. 13.11 КоАП РФ)

НАРУШЕНИЕ 3 (ч. 3 ст. 13.11 КоАП РФ):

Непредоставление доступа к Политике по обработке персональных данных

Невыполнение оператором предусмотренной законодательством РФ в области ПД *обязанности по опубликованию* или *обеспечению иным образом неограниченного доступа* к документу, определяющему политику оператора в отношении обработки ПД, или сведениям о реализуемых требованиях к защите ПД –

НАРУШЕНИЕ 4 (ч. 4 ст. 13.11 КоАП РФ):

Сокрытие информации

Невыполнение оператором предусмотренной законодательством Российской Федерации в области персональных данных *обязанности по предоставлению* субъекту персональных данных информации, касающейся обработки его персональных данных

На основании ч. 3.5 ст. 28.1 КоАП РФ привлечение к административной ответственности возможно без проведения контрольных (надзорных) мероприятий (КНМ) в случае поступления от Оператора данных, подтверждающих наличие события правонарушения)

НАРУШЕНИЕ 5 (ч. 5 ст. 13.11 КоАП РФ):

Невыполнение оператором в сроки, установленные законодательством РФ в области ПД, *требования* субъекта ПД или его представителя либо уполномоченного органа по защите прав субъектов ПД *об уточнении* ПД, *их блокировании или уничтожении* в случае, если ПД являются *неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки*, -

(ч.5.1 ст. 13.11 КоАП РФ: повторное совершение административного правонарушения, предусмотренного ч.5 ст. 13.11 КоАП РФ)

НАРУШЕНИЕ 6 (ч. 6 ст. 13.11 КоАП РФ):

Нарушение требований к сохранности Персональных данных

Невыполнение оператором при обработке ПД без использования средств автоматизации *обязанности по соблюдению условий*, *обеспечивающих* в соответствии с законодательством РФ в области ПД *сохранность ПД* при хранении материальных носителей ПД и исключающих несанкционированный к ним доступ, *если это повлекло* неправомерный или случайный доступ к ПД, их уничтожение, изменение, блокирование, копирование, предоставление, распространение либо иные неправомерные действия в отношении ПД, при отсутствии признаков уголовно наказуемого деяния

На основании ч. 3.5 ст. 28.1 КоАП РФ привлечение к административной ответственности возможно без проведения контрольных (надзорных) мероприятий (КНМ) в случае поступления материалов, подтверждающих наличие события правонарушения, из правоохранительных органов, государственных органов, органов местного самоуправления, общественного объединения)

НАРУШЕНИЕ 7 (ч. 7 ст. 13.11 КоАП РФ):

Нарушение порядка обезличивания Персональных данных

Невыполнение оператором, являющимся государственным или муниципальным органом, предусмотренной законодательством РФ в области ПД обязанности по обезличиванию ПД либо несоблюдение установленных требований или методов по обезличиванию ПД –

НАРУШЕНИЕ 8 (ч. 8 ст. 13.11 КоАП РФ):

Невыполнение обязанности по использованию баз данных, находящихся на территории РФ

Невыполнение оператором при сборе ПД, в том числе посредством информационно-телекоммуникационной сети "Интернет", предусмотренной законодательством РФ в области ПД обязанности по обеспечению записи, систематизации, накопления, хранения, уточнения (обновления, изменения) или извлечения ПД граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации

(ч.9 ст. 13.11 КоАП РФ: повторное совершение административного правонарушения, предусмотренного ч.8 ст. 13.11 КоАП РФ)

КОДЕКС ДОБРОСОВЕСТНЫХ ПРАКТИК

В ноябре 2016 года в городе Москве состоялась VII Международная конференция «Защита персональных данных», на которой прошла презентация проекта «Цифровой дом».

В рамках проекта «Цифровой дом», цель которого - создание безопасной и комфортной цифровой среды, был подписан Кодекс добросовестных практик в сети Интернет (далее – Кодекс), направленный на формирование и обеспечение реализации условий для взаимодействия граждан, государства, общества и бизнеса. Текст Кодекса, а также список его подписантов (http://pd.rkn.gov.ru/code/signatory/), размещены на Портале персональных данных Уполномоченного органа по защите прав субъектов персональных данных в разделе «Кодекс добросовестных практик» (http://pd.rkn.gov.ru/code/). ***Кодекс открыт для присоединения к нему любой заинтересованной стороны.***

Подписавшие Кодекс организации подтверждают свою готовность содействовать обеспечению безопасного информационного пространства в сети Интернет на основе требований законодательства Российской Федерации, положений международных договоров, рекомендаций уполномоченных органов государственной власти, а также создания, развития и внедрения мероприятий по формированию культуры безопасного поведения в Сети.

РОСКОМНАДЗОР

СПАСИБО ЗА ВНИМАНИЕ!

Начальник отдела по защите прав субъектов персональных данных Управления Роскомнадзора по Томской области Ермальчук Елена Владимировна, тел. +7(3822)609004, e-mail: eev.rkn70@yandex.ru