



Персональные данные

Федеральный закон от 27.07.2006
N 152-ФЗ (в ред. от 06.02.2023) "О
персональных данных"

Персональные данные

Согласно Федеральному закону от 27.07.2006
N 152-ФЗ (в ред. от 06.02.2023) "О
персональных данных" персональные
данные - любая информация, относящаяся
к прямо или косвенно определенному или
определяемому физическому лицу
(субъекту персональных данных);

Персональные данные

- Персональные данные (ПДн) – это любая информация, прямо или косвенно относящаяся к физическому лицу, с помощью которой он может быть идентифицирован. Закрытого перечня таких данных не существует – к ним относят любые сведения, по которым можно идентифицировать человека: ФИО, паспортные данные, ИНН, СНИЛС, место работы и должность, сведения об образовании, имуществе и здоровье, cookie в браузере пользователя, семейное и социальное положение, а также изображение человека вкупе с другими данными. Для определения того, могут ли сведения идентифицировать человека важны скорее не сами данные, а их совокупность.

Персональные данные

- Закон о персональных данных нужен тем, чьи данные собирают, обрабатывают и хранят.
- Цель закона — защитить интересы и права этих людей.
- Нормы защиты персональных данных придумали не в России. Правила их обработки ООН описала еще в 1948 году во Всеобщей декларации прав человека. В 1981 году Совет Европы принял конвенцию по обработке персональных данных. А Россия ее ратифицировала в 2006 году и разработала свой закон.

Персональные данные

Что можно делать:

- Обрабатывать персональные данные

! Обработка персональных данных должна осуществляться на законной и справедливой основе

Персональные данные

Что нельзя делать с ПНд:

- обработка персональных данных в случаях, не предусмотренных законом, или несовместимая с целями сбора персональных данных;
- обработка персональных данных при отсутствии письменного согласия субъекта;
- неисполнение обязанности по опубликованию политики по обработке персональных данных.

Персональные данные

Статья 3. Основные понятия, используемые в Федеральном законе

- 1) **персональные данные** - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);
- 2) **оператор** - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

Персональные данные

Статья 3. Основные понятия, используемые в Федеральном законе

- 3) **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;
- 4) **автоматизированная обработка персональных данных** - обработка персональных данных с помощью средств вычислительной техники;
- 5) **распространение персональных данных** - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

Персональные данные

Статья 3. Основные понятия, используемые в Федеральном законе

- 6) **предоставление персональных данных** - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;
- 7) **блокирование персональных данных** - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);
- 8) **уничтожение персональных данных** - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

Персональные данные

Статья 3. Основные понятия, используемые в Федеральном законе

- 9) **обезличивание персональных данных** - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;
- 10) **информационная система персональных данных** - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;
- 11) **трансграничная передача персональных данных** - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

Персональные данные

Получить согласие на обработку персональных данных недостаточно. Нужно соблюдать семь принципов обработки и правильно оформлять внутренние документы.

- **Статья 5. Принципы обработки персональных данных**

1. Обработка персональных данных должна осуществляться на законной и справедливой основе.

Персональные данные

2. Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.
3. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.
4. Обработке подлежат только персональные данные, которые отвечают целям их обработки.

Персональные данные

5. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.
6. При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.

Персональные данные

7. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обработываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

И лучше сделать это один раз и с помощью юриста, чем платить штрафы государству и возмещать моральный вред.

Рекомендации по проведению комплекса необходимых мероприятий по защите ПДн

- Для соблюдения минимальных требований и недопущения серьезных претензий со стороны регуляторов (в первую очередь Роскомнадзора) рекомендуется проведение следующего комплекса мероприятий:
 1. Создание комиссии по проведению комплекса мероприятий по защите ПДн. Учитывая, что проведение данных работ включает широкий круг вопросов, в состав комиссии привлекаются лица, обладающие знаниями в сфере защиты информации, в области юриспруденции, работника кадровой службы, бухгалтера, системного администратора.

Рекомендации по проведению комплекса необходимых мероприятий по защите ПДн

2. Начинать работу по проведению комплекса мер по защите ПДн следует с проведения категорирования обрабатываемых персональных данных. Проще говоря, задачей данного этапа работы является выявление всех данных персонального характера, обрабатываемых в организации. Также на данном этапе необходимо оценить наличие согласий субъектов ПДн на обработку данных, проанализировать требуется ли для нужд организации хранение всех сведений персонального характера, а также определить перечень ответственных лиц.

Рекомендации по проведению комплекса необходимых мероприятий по защите ПДн

3. Определение характеристики ИСПДн. На данном этапе необходимо определить конфигурации и топологии ИСПДн, физические, функциональные и технологические связи как внутри системы, так и с другими системами различного уровня и назначения, определить технические и программные средства, используемые в ИСПДн.
4. Определение перечня угроз в части соблюдения безопасности информации, их актуальность (рекомендуется привлечение экспертов по информационной безопасности), разработка модели угроз и определение класса ИСПДн.

Рекомендации по проведению комплекса необходимых мероприятий по защите ПДн

5. Подготовка и направление уведомление в Роскомнадзор с целью включения в реестр операторов.
6. Разработка порядка работы с ПДн. В случае необходимости разработать и провести комплекс дополнительных мероприятий по защите ПДн, в том числе по технической защите ПДн (приобрести и настроить необходимые технические средства и программное обеспечение). Разработанный порядок должен обеспечивать своевременное предоставление информации в случае получения запросов из Роскомнадзора (7 раб. дней) или непосредственно от физических лиц - субъектов ПДн (10 раб. дней).

Рекомендации по проведению комплекса необходимых мероприятий по защите ПДн

7. Подготовка и утверждение комплекта организационно-распорядительной документации.

В наличии должны быть:

- Приказ о назначении ответственного должностного лица/подразделения;
- Положение о защите ПДн;
- Приказы о допуске, перечень допущенных сотрудников;
- Журналы учета носителей информации.

8. Доведение до сотрудников порядка работы со сведениями о персональных данных, в том числе обучение сотрудников.

9. Планирование и проведение контрольных мероприятий по защите ПДн.

Ответственность за нарушение закона о персональных данных

- **Статья 13.11. Нарушение законодательства Российской Федерации в области персональных данных**
 1. Обработка персональных данных в случаях, не предусмотренных законодательством Российской Федерации в области персональных данных, либо обработка персональных данных, несовместимая с целями сбора персональных данных, за исключением случаев, предусмотренных частью 2 настоящей статьи, если эти действия не содержат уголовно наказуемого деяния, -
влечет предупреждение или наложение административного штрафа на граждан в размере от одной тысячи до трех тысяч рублей; на должностных лиц - от пяти тысяч до десяти тысяч рублей; на юридических лиц - от тридцати тысяч до пятидесяти тысяч рублей.

Ответственность за нарушение закона о персональных данных

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

влечет наложение административного штрафа на граждан в размере от трех тысяч до пяти тысяч рублей; на должностных лиц - от десяти тысяч до двадцати тысяч рублей; на юридических лиц - от пятнадцати тысяч до семидесяти пяти тысяч рублей.

Ответственность за нарушение закона о персональных данных

3. Невыполнение оператором предусмотренной законодательством Российской Федерации в области персональных данных обязанности по опубликованию или обеспечению иным образом неограниченного доступа к документу, определяющему политику оператора в отношении обработки персональных данных, или сведениям о реализуемых требованиях к защите персональных данных -
- влечет предупреждение или наложение административного штрафа на граждан в размере от семисот до одной тысячи пятисот рублей; на должностных лиц - от трех тысяч до шести тысяч рублей; на индивидуальных предпринимателей - от пяти тысяч до десяти тысяч рублей; на юридических лиц - от пятнадцати тысяч до тридцати тысяч рублей.*

Ответственность за нарушение закона о персональных данных

4. Невыполнение оператором предусмотренной законодательством Российской Федерации в области персональных данных обязанности по предоставлению субъекту персональных данных информации, касающейся обработки его персональных данных, -
- влечет предупреждение или наложение административного штрафа на граждан в размере от одной тысячи до двух тысяч рублей; на должностных лиц - от четырех тысяч до шести тысяч рублей; на индивидуальных предпринимателей - от десяти тысяч до пятнадцати тысяч рублей; на юридических лиц - от двадцати тысяч до сорока тысяч рублей.*

Ответственность за нарушение закона о персональных данных

5. Невыполнение оператором в сроки, установленные законодательством Российской Федерации в области персональных данных, требования субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных об уточнении персональных данных, их блокировании или уничтожении в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, -
- влечет предупреждение или наложение административного штрафа на граждан в размере от одной тысячи до двух тысяч рублей; на должностных лиц - от четырех тысяч до десяти тысяч рублей; на индивидуальных предпринимателей - от десяти тысяч до двадцати тысяч рублей; на юридических лиц - от двадцати пяти тысяч до сорока пяти тысяч рублей.*

Ответственность за нарушение закона о персональных данных

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

влечет наложение административного штрафа на граждан в размере от семисот до двух тысяч рублей; на должностных лиц - от четырех тысяч до десяти тысяч рублей; на индивидуальных предпринимателей - от десяти тысяч до двадцати тысяч рублей; на юридических лиц - от двадцати пяти тысяч до пятидесяти тысяч рублей.

Ответственность за нарушение закона о персональных данных

7. Невыполнение оператором, являющимся государственным или муниципальным органом, предусмотренной законодательством Российской Федерации в области персональных данных обязанности по обезличиванию персональных данных либо несоблюдение установленных требований или методов по обезличиванию персональных данных -
- влечет предупреждение или наложение административного штрафа на должностных лиц в размере от трех тысяч до шести тысяч рублей.*

Ответственность за нарушение закона о персональных данных

8. Невыполнение оператором при сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети "Интернет", предусмотренной законодательством Российской Федерации в области персональных данных обязанности по обеспечению записи, систематизации, накопления, хранения, уточнения (обновления, изменения) или извлечения персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, - *влечет наложение административного штрафа на граждан в размере от тридцати тысяч до пятидесяти тысяч рублей; на должностных лиц - от ста тысяч до двухсот тысяч рублей; на юридических лиц - от одного миллиона до шести миллионов рублей.*

(часть 8 введена Федеральным законом от 02.12.2019 N 405-ФЗ)

Ответственность за нарушение закона о персональных данных

9. Повторное совершение административного правонарушения, предусмотренного частью 8 настоящей статьи, -

влечет наложение административного штрафа на граждан в размере от пятидесяти тысяч до ста тысяч рублей; на должностных лиц - от пятисот тысяч до восьмисот тысяч рублей; на юридических лиц - от шести миллионов до восемнадцати миллионов рублей.

(часть 9 введена Федеральным законом от 02.12.2019 N 405-ФЗ)

ЧаВо

- У меня есть электронные почты друзей, список контактов в телефоне, аккаунты разных людей в соцсетях. Получается, я тоже оператор и должен получать согласие этих людей на то, чтобы хранить и удалять их данные?
- Я делаю сайт для клиента, обрабатываю и храню данные на своей стороне. При этом владелец сайта не обязан быть оператором персональных данных?
- А если получаешь только имя без фамилии и номер телефона, это тоже попадает под персональные данные? А если только номер телефона?

ЧаВо

- Как правильно получить согласие на обработку персональных данных на сайте? Можно взять шаблон с сайта какой-то крупной компании?
- То есть если человек специально опубликовался для каких-то рекламных целей, то это не считается персональными данными? На «Авито», например.
- Вот публикую я пост в соц. сети и упоминаю своего друга — значит, я данные обрабатываю? Кэш поста хранится на телефоне, значит, я данные храню? А если сделаю репост , то я их еще и предоставляю третьей стороне. И как с этим жить?

Источник: <https://journal.tinkoff.ru/slozhno/personal-data/>

ЧаВо

- **Могу ли я не регистрироваться в Роскомнадзоре, если поменяю поле в форме обратной связи с «Ваше имя» на «Ваша компания»?**
- **Если на столбе объявление «Куплю рога оленя, 8 800..., Геннадий», то этот столб можно оштрафовать?**
- **А если у нас сайт на английском?**
- **Закон о персональных данных нужно соблюдать, если сайт используется для работы на территории РФ. Теоретически Роскомнадзор имеет право и может его заблокировать.**

ИТОГ

1. Персональные данные — это любые сведения о физическом лице
2. Оператор по обработке персональных — это лицо, осуществляющее их обработку
3. Все сайты должны опубликовать Политику конфиденциальности
4. На обработку персональных данных требуется письменное согласие
5. Каждый оператор ПДн должен быть включен в реестр Роскомнадзора
(<https://rkn.gov.ru/personal-data/register/>)