КонсультантПлюс
надежная правовая поддержка

Бесплатный доступ
для изучения системы

ВАШ КОНСУЛЬТАНТ
Региональный информационный центр

Сайт: www.vkons.ru
E-mail: cons@vkons.ru
8 (800) 700-52-23
8 (843) 515-20-20

Практическое руководство для оператора персональных данных

Оператор персональных данных определяет состав персональных данных, подлежащих обработке, цель их обработки и непосредственно обрабатывает такие данные. К персональным данным относится любая информация об определенном (определяемом) физлице.
На оператора возлагается ряд обязанностей, например, уведомить Роскомнадзор об обработке персональных данных. За невыполнение обязанностей оператора могут привлечь к ответственности.

Уведомление об обработке персональных данных

Операторы должны уведомлять Роскомнадзор о начале или осуществлении любой обработки персональных данных **за исключением случаев, когда данные**:

- обрабатываются в целях защиты безопасности государства и общественного порядка,
- транспортной безопасности,
- или если оператор обрабатывает данные исключительно без средств автоматизации.

Как уведомить Роскомнадзор об обработке персональных данных?

Уведомление о намерении осуществлять обработку персональных данных нужно подать в Роскомнадзор до начала их обработки (ч. 1 ст. 22 Закона о персональных данных).

Составьте уведомление по форме, приведенной в Приложении № 1 к Приказу Роскомнадзора от 28.10.2022 N 180. В нем укажите, в частности (ч. 3, 3.1 ст. 22 Закона о персональных данных):

- свое наименование (фамилию, имя, отчество), адрес;
- цель обработки персональных данных. Для каждой цели необходимо указать ряд сведений, в частности: категории персональных данных, категории субъектов, способы обработки персональных данных;
- дату начала обработки персональных данных;
- срок или условие прекращения обработки персональных данных;
- сведения об обеспечении безопасности персональных данных в соответствии с установленными требованиями к защите таких данных.

ВАШ КОНСУЛЬТАНТ
ПОЛУЧИТЕ ДОСТУП К СИСТЕМЕ
КОНСУЛЬТАНТ ПЛЮС
ПОЗВОНИТЕ НАМ:
8 (800) 700-52-23
8 (843) 515-20-20

Уведомление должно быть подписано уполномоченным лицом (ч. 3 ст. 22 Закона о персональных данных).

Образец заполнения уведомления о намерении обрабатывать персональные данные

Роскомнадзор на основании этого уведомления в течение 30 дней с даты его поступления должен внести сведения в реестр операторов (ч. 4 ст. 22 Закона о персональных данных).

Как проверить наличие оператора в Реестре => Pd.rkn.gov.ru

Для наиболее точного и быстрого поиска в реестре достаточно указать ИНН организации на сайте: https://pd.rkn.gov.ru/.

> Скорректирован срок уведомления Роскомнадзора об изменении ранее поданных сведений об обработке персональных данных.
> Обо всех изменениях, которые произошли в течение месяца, нужно сообщить не позднее 15-го числа следующего месяца.

Как опубликовать политику обработки персональных данных

Вы обязаны опубликовать или иным образом обеспечить неограниченный доступ к вашей политике обработки персональных данных, к сведениям о реализуемых требованиях к защите таких данных. Документ можно разместить на вашем официальном сайте или на информационном стенде в офисе, если сайта у вас нет. Если же вы осуществляете сбор персональных данных с использованием информационно-телекоммуникационных сетей, то обязаны (ч. 2 ст. 18.1 Закона о персональных данных, Письмо Роскомнадзора от 19.10.2021 N 08-71063):

- опубликовать политику обработки персональных данных и сведения о реализуемых требованиях к защите персональных данных в соответствующей сети, в том числе на страницах принадлежащего вам сайта, с помощью которых собираются данные;
- обеспечить возможность доступа к этому документу с использованием средств такой сети.

По запросу Роскомнадзора вы должны представить документы, определяющие политику обработки персональных данных, и подтвердить, что приняли необходимые меры, в том числе в рамках политики обработки персональных данных (ч. 4 ст. 18.1 Закона о персональных данных).

Форма: Положение об обработке и защите персональных данных (в том числе в отношении персональных данных клиентов (контрагентов))

ВАШ КОНСУЛЬТАНТ
НЕ РАБОТАЕТ ССЫЛКА?
ПОЗВОНИТЕ НАМ:
8 (800) 700-52-23
8 (843) 515-20-20

Как изменится ответственность с 30 мая 2025 года

Ужесточается административная ответственность за утечку персональных данных и другие нарушения. За повторную утечку коммерческим организациям и ИП грозят оборотные штрафы. В правилах обработки персональных данных изменений нет.

Нарушение	ИП, физлица	Должностные лица	Компании
Утечка персданных 1 000 — 10 000 чел.	Первичное - 100 - 200 тыс. руб. Повторное - 400 - 600 тыс. руб.	Первичное - 200 - 400 тыс. руб. Повторное - 800 тыс. руб. - 1,2 млн руб.	Первичное - 3 - 5 млн руб. Повторное - от 1% до 3% совокупного размера годовой выручки
Утечка персданных 10 000 — 100 000 чел.	Первичное - 200 — 300 тыс. руб. Повторное - 400 - 600 тыс. руб.	Первичное - 300 - 500 тыс. руб. Повторное - 800 тыс. руб. - 1,2 млн руб.	Первичное - 5 - 10 млн руб. Повторное - от 1% до 3% совокупного размера годовой выручки
Утечка персданных более 100 000 чел.	Первичное - 300 - 400 тыс. руб. Повторное - 400 - 600 тыс. руб.	Первичное - 400 - 600 тыс. руб. Повторное - 800 тыс. руб. - 1,2 млн руб.	Первичное - 10 - 15 млн руб. Повторное - от 1% до 3% совокупного размера годовой выручки
Утечка персданных спецкатегорий	Первичное - 300 - 400 тыс. руб. Повторное - 500 - 800 тыс. руб.	Первичное - 1 - 1,4 млн руб. Повторное - 1 - 2 млн руб.	
Утечка биометрических персданных	Первичное - 400 - 500 тыс. руб. Повторное - 500 - 800 тыс. руб.	Первичное - 1,3 - 1,5 млн руб. Повторное - 1 - 2 млн руб.	Первичное - 15 - 20 млн руб. Повторное - от 1% до 3% совокупного размера годовой выручки

Уведомление Роскомнадзора об инцидентах

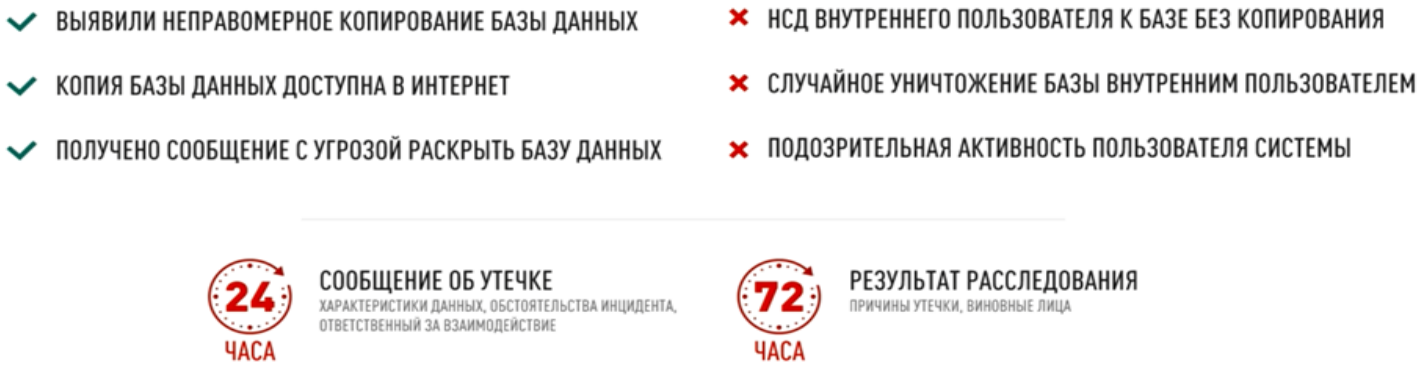
В случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных, оператор обязан с момента выявления такого инцидента оператором, уполномоченным органом по защите прав субъектов персональных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

КонсультантПлюс
надежная правовая поддержка

Бесплатный доступ
для изучения системы

ВАШ КОНСУЛЬТАНТ
Региональный информационный центр

Сайт: www.vkons.ru
E-mail: cons@vkons.ru
8 (800) 700-52-23
8 (843) 515-20-20



Ответственность за неуведомление

Статья	ИП, физлица	Должностные лица	Юридические лица
Неоповещение об утечке персональных данных	50 — 100 тыс. ₽	400 — 800 тыс. ₽	1 — 3 млн ₽

Соблюдение конфиденциальности

Операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

Оператор при обработке персональных данных обязан принимать необходимые **правовые, организационные и технические меры** или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним.

ВАШ КОНСУЛЬТАНТ

НЕ РАБОТАЕТ ССЫЛКА?
ПОЗВОНИТЕ НАМ:

8 (800) 700-52-23
8 (843) 515-20-20

КонсультантПлюс
надежная правовая поддержка

Бесплатный доступ
для изучения системы

ВАШ КОНСУЛЬТАНТ
Региональный информационный центр

Сайт: www.vkons.ru
E-mail: cons@vkons.ru
8 (800) 700-52-23
8 (843) 515-20-20

Что является персональными данными

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

Практически каждая организация сталкивается с персональными данными физлиц. Поскольку законодательство не содержит конкретного перечня персональных данных, к таковым может быть отнесена любая информация о гражданах, в частности:

- фамилия, имя, отчество;
- пол, возраст;
- образование, квалификация и т.п.;
- контактная информация (адрес, номер телефона и т.п.);
- семейное положение, наличие детей;
- факты биографии;
- финансовое положение;
- фотография, используемая для установления личности (Письма Роскомнадзора от 10.02.2020 N 08АП-6782, Минцифры России от 17.07.2020 N ОП-П24-070-19433).

Персональные данные работника - любая информация о человеке, имеющаяся у работодателя. Это Ф.И.О. и другие паспортные данные, ИНН, СНИЛС, номер телефона, сведения об образовании, зарплате и других доходах, и т.д. (ст. 3 Закона N 152-ФЗ, Письмо Минкомсвязи от 28.08.2020 N ЛБ-С-074-24059).

Фотографии, аудио- и видеозаписи, отпечатки пальцев являются биометрическими персональными данными (Письмо Роскомнадзора от 10.02.2020 N 08АП-6782).

ВАШ КОНСУЛЬТАНТ
ПОЛУЧИТЕ ДОСТУП К СИСТЕМЕ
КОНСУЛЬТАНТ ПЛЮС
ПОЗВОНИТЕ НАМ:
8 (800) 700-52-23
8 (843) 515-20-20

КонсультантПлюс
надежная правовая поддержка

Бесплатный доступ
для изучения системы

ВАШ КОНСУЛЬТАНТ
Региональный информационный центр

Сайт: www.vkons.ru
E-mail: cons@vkons.ru
8 (800) 700-52-23
8 (843) 515-20-20

Этапы действий по защите персональных данных

1) Определить цели обработки персональных данных:

- Ведение кадрового и бухгалтерского учета
- Обеспечение соблюдения трудового законодательства РФ
- Обеспечение соблюдения налогового законодательства РФ
- Обеспечение соблюдения пенсионного законодательства РФ
- Обеспечение соблюдения страхового законодательства РФ
- Обеспечение соблюдения законодательства РФ в сфере здравоохранения
- Участие лица в конституционном, гражданском, административном, уголовном судопроизводстве, судопроизводстве в арбитражных судах
- Добровольное медицинское страхование
- Обеспечение пропускного режима на территорию оператора
- Подбор персонала (соискателей) на вакантные должности оператора
- Иная цель

2) Назначение ответственного за организацию обработки ПД:

Лицо, ответственное за организацию обработки персональных данных, в частности, обязано:

- осуществлять внутренний контроль за соблюдением оператором и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;
- доводить до сведения работников оператора положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;
- организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.

3) Правовые меры – какие документы нужны:

- Документ, определяющий политику в отношении обработки персональных данных, определяющий **для каждой цели обработки**:
  - содержание обрабатываемых персональных данных;
  - категории субъектов;
  - сроки их обработки и хранения;
  - порядок уничтожения при достижении целей обработки

ВАШ КОНСУЛЬТАНТ
ПОЛУЧИТЕ ДОСТУП К СИСТЕМЕ
КОНСУЛЬТАНТ ПЛЮС
ПОЗВОНИТЕ НАМ:
8 (800) 700-52-23
8 (843) 515-20-20

- Правила рассмотрения запросов субъектов персональных данных
- Правила осуществления внутреннего контроля
- Акт оценки вреда (приказ Роскомнадзора № 178)

4) Технические меры (примеры)

- Идентификация и аутентификация субъектов доступа и объектов доступа
- Управление доступом субъектов доступа к объектам доступа
- Ограничение программной среды
- Защита машинных носителей ПДн
- Регистрация событий безопасности
- Антивирусная защита
- Обнаружение вторжений
- Контроль (анализ) защищенности ПДн
- Обеспечение целостности ИС и ПДн
- Обеспечение доступности ПДн
- Защита среды виртуализации
- Защита технических средств
- Защита ИС, ее средств, систем связи и передачи данных
- Выявление инцидентов и реагирование на них

5) Ознакомление и (или) обучение работников

Работники и их представители должны быть ознакомлены под роспись с документами работодателя, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области.

6) Контроль

Контроль за выполнением требований к защите персональных данных при их обработке в информационных системах организуется и проводится оператором (уполномоченным лицом) самостоятельно и (или) с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации.

Указанный контроль проводится не реже 1 раза в 3 года в сроки, определяемые оператором (уполномоченным лицом).

КонсультантПлюс
надежная правовая поддержка

Бесплатный доступ
для изучения системы

ВАШ КОНСУЛЬТАНТ
Региональный информационный центр

Сайт: www.vkons.ru
E-mail: cons@vkons.ru
8 (800) 700-52-23
8 (843) 515-20-20

Уничтожение персональных данных

Регулирующий документ:
Приказ Роскомнадзора от 28.10.2022 № 179 «Об утверждении Требований к подтверждению уничтожения персональных данных».

- Подтверждением будет являться акт об уничтожении ПД либо выгрузка из журнала (лог-файл)
- Оба способа являются достоверным способом подтверждения
- В случае, если в лог-файле нельзя предусмотреть все сведения, недостающие сведения вносятся в акт
- Указанные документы подлежат хранению в течение 3 лет с момента уничтожения ПД
- Вступил в силу с 1 марта 2023 г. и действует до 1 марта 2029 г.

Надлежащее обеспечение прав субъектов персональных данных

При получении от субъекта персональных данных обращения с требованием о прекращении обработки персональных данных оператору необходимо:

- В течение 10 рабочих дней прекратить обработку персональных данных (ч. 5.1. ст. 21 ФЗ № 152).
- Принять меры по уничтожению персональных данных в соответствии с порядком, утвержденным приказом Роскомнадзора от 28.10.2022 № 179.

Исключение: случаи, предусмотренные пунктами 2-11 ч. 1 ст. 6, ч. 2 ст. 10, ч. 2 ст. 11 ФЗ № 152.

При получении от субъекта персональных данных запроса, направленного на основании ст. 14 ФЗ № 152 оператору необходимо в течение 10 рабочих дней (с даты получения запроса) дать субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных.

При получении запроса Роскомнадзора оператору необходимо в течение 10 рабочих дней (с даты получения запроса) направить в Роскомнадзор запрашиваемую информацию.

Допускается продление срока не более, чем на 5 рабочих дней при условии направления мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

ВАШ КОНСУЛЬТАНТ
ПОЛУЧИТЕ ДОСТУП К СИСТЕМЕ
КОНСУЛЬТАНТ ПЛЮС
ПОЗВОНИТЕ НАМ:
8 (800) 700-52-23
8 (843) 515-20-20

Нарушения, выявляемые в ходе мероприятия по контролю без взаимодействия с контролируемым лицом и как их не допустить:

Нарушение	Меры по предотвращению
Отсутствие оператора в реестре операторов, осуществляющих обработку ПДн (ч. 1 ст. 22 ФЗ «О персональных данных»)	Направить Уведомление в Роскомнадзор через Портал персональных данных (pd.rkn.gov.ru)
Отсутствие правовых оснований на сбор и обработку персональных данных на сайте оператора (ч. 1 ст.6 ФЗ «О персональных данных», Ч. 1 ст. 9 ФЗ «О персональных данных»)	**1)** Наличие согласия на обработку ПД через различные формы сбора на сайте, **2)** Наличие согласия на обработку ПД, осуществляющую посредством метрических систем, **3)** Соблюдение требований к содержанию согласия, **4)** Корректное указание целей обработки
Распространение персональных данных (ч. 1 ст.10.1 ФЗ «О персональных данных»)	Наличие согласия на обработку ПД, разрешенных субъектом персональных данных для распространения (Приказ Роскомнадзора от 24.02.2021 № 18)
Нарушение требований по размещению документа, определяющего политику оператора в отношении обработки персональных данных (ч. 2 ст.18.1 ФЗ «О персональных данных»)	**1)** Размещение документа на всех страницах сайта, с использованием которых осуществляется сбор персональных данных, **2)** Размещение в документе, определяющего политику оператора в отношении обработки персональных данных всех положений, предусмотренных п. 2 ч. 1 ст. 18.1 ФЗ «О персональных данных»
Нарушение требований по локализации Баз данных (ч. 5 ст.18 ФЗ «О персональных данных»)	Сбор персональных данных с использованием баз данных сайта, находящихся на территории Российской Федерации
Нарушение требований по трансграничной передаче персональных данных (ст.12 ФЗ «О персональных данных»)	Осуществлять обработку персональных данных, посредством отечественных сервисов, в том числе метрических программ