



Персональные данные: что нужно знать?



Персональные данные:
что нужно знать?

Информационно-правовое издание

Составитель:
М.А. Синкина

Компьютерная верстка:
М.А. Синкина

МБУК «Кирово-Чепецкая РЦБС»
613047 г. Кирово-Чепецк, ул. Сосновая, 1
E-mail: k-c-biblioteka@yandex.ru

Как защитить персональные данные в Сети:

- ⇒ Ограничьте объем информации о себе, находящейся в Интернете. Удалите лишние фотографии, видео, адреса, номера телефонов, дату рождения, сведения о родных и близких и иную личную информацию.
- ⇒ Не отправляйте видео и фотографии людям, с которыми вы познакомились в Интернете и не знаете их в реальной жизни.
- ⇒ Отправляя кому-либо свои персональные данные или конфиденциальную информацию, убедитесь в том, что адресат действительно тот, за кого себя выдает.
- ⇒ Если в сети Интернет кто-то просит предоставить ваши персональные данные, например, место жительства или номер школы, класса иные данные, посоветуйтесь с родителями или взрослым человеком, которому вы доверяете.
- ⇒ Используйте только сложные пароли, разные для разных учетных записей и сервисов.
- ⇒ Старайтесь периодически менять пароли.
- ⇒ Заведите себе два адреса электронной почты — частный, для переписки (приватный и малоизвестный, который вы никогда не публикуете в общедоступных источниках), и публичный — для открытой деятельности (форумов, чатов и так далее).
- ⇒ Проверьте и настройте доступ приложений к камере, микрофону, геолокации, галерее и файлам. Лучше воздержаться от предоставления избыточной информации о себе, ограничив доступ приложения только к тем данным, которые требуются для функционирования системы. Если приложение для чтения книг хочет получить доступ к вашей геолокации - это повод насторожиться.
- ⇒ Пользуйтесь антивирусным программным обеспечением.



Персональные данные!

ЧТО НУЖНО ЗНАТЬ?

информационно-правовое издание

Кирово-Чепецк, 2021

Составитель: М.А. Синкина

Издание проиллюстрировано рисунками детей из Кирово-Чепецкого района:

Иллюстраторы:

Бахтин Михаил, ст. Просница

Бахтина Снежана, ст. Просница

Глушков Георгий, с. Бурмакино

Злобина Мария, с. Селезениха

Кушнерова Олеся, с. Каринка

Кытманов Марк, п. Ключи

Мохова Александра, с. Селезениха

Пиков Егор, с. Каринка

Рохина Маргарита, с. Селезениха

Самылова Полина, с. Кстинино

Сивкова Анна, с. Бурмакино

Шишкина Диана, п. Ключм

Шмакова Майя, п. Ключи

Персональные данные: что нужно знать? : информационно-правовое издание / МБУК «Кирово-Чепецкая РЦБС», Публичный центр правовой информации ; сост. М.А. Синкина.—Кирово-Чепецк, 2021. — 16 с.

Как общаться в Сети:

- ⇒ Старайтесь не выкладывать в Интернет личную информацию (фотографии, видео, ФИО, дату рождения, адрес дома, номер школы, телефоны и иные данные) или существенно сократите объем данных, которые публикуете в Интернете.
- ⇒ Не выкладывайте личную информацию (совместные фотографии, видео, иные данные) о ваших друзьях в Интернет без их разрешения. Прежде чем разместить информацию о друзьях в Сети, узнайте, не возражают ли они, чтобы вы выложили данные.
- ⇒ Не отправляйте свои персональные данные, а также свои видео и фото людям, с которыми вы познакомились в Интернете, тем более если вы не знаете их в реальной жизни.
- ⇒ При общении с другими пользователями старайтесь быть вежливыми, деликатными, тактичными и дружелюбными. Не пишите грубостей, оскорблений, матерных слов – читать такие высказывания так же неприятно, как и слышать.
- ⇒ Старайтесь не реагировать на обидные комментарии, хамство и грубость других пользователей. Всегда пытайтесь уладить конфликты с пользователями мирным путем, переведите все в шутку или прекратите общение с агрессивными пользователями. Ни в коем случае не отвечайте на агрессию тем же способом.
- ⇒ Если решить проблему мирным путем не удалось, напишите жалобу администратору сайта, потребуйте заблокировать обидчика.
- ⇒ Если администратор сайта отказался вам помочь, прекратите пользоваться таким ресурсом и удалите оттуда свои данные.
- ⇒ Не используйте Сеть для распространения сплетен, угроз или хулиганства.
- ⇒ Если вы не совершеннолетний, не встречайтесь в реальной жизни с онлайн-знакомыми без разрешения родителей или в отсутствие взрослого человека. Если вы хотите встретиться с новым интернет-другом, постарайтесь пойти на встречу в сопровождении взрослого, которому вы доверяете.

какой фирмы она сделана. Либо замажьте или зачеркните часть данных, например вашу подпись.

Как мы оставляем персональные данные в сети Интернет?

Каждое наше действие, совершаемое в сети Интернет, оставляет определенный цифровой след.

Такие следы оставляет информация, которую вы добровольно размещаете в сети Интернет, например, фотографии в социальных сетях, высказывания на форумах, «лайки» новостей и многое другое.

Кроме того, цифровые следы оставляет та информация, о наличии которой вы можете и не подозревать, например, информация о посещенных сайтах, о совершенных покупках, о вашем географическом месторасположении и пр.

Если обработать всю эту информацию, то получится очень точный портрет («профайл»), который можно использовать для принятия решений в отношении конкретного человека. Например, направить ему адресную рекламу в соответствии с предпочтениями, «лайками» или отказать в поступлении на работу и пр.

Сегодня информационные технологии позволяют обрабатывать и анализировать огромные объемы данных для выявления новой информации, представляющей ценность для принятия различных решений.

Представьте себе данные о следах всех пользователей сети Интернет России или другой страны, которые они оставили за последние 10 лет.

Этот колоссальный объем информации, подлежащий обработке и анализу, получил название Big Data или Большие данные.

При этом Большие данные получают не только благодаря Вашим цифровым следам, их добывают из иных источников, например, с помощью датчиков погоды или геолокационных систем.



В последние годы вопрос о персональных данных стал крайне острым ввиду активной цифровизации, а следовательно, и с ростом рисков по утечке и мошенническом использовании информации.



Что такое персональные данные и что к ним относят?

Персональные данные — это любая информация, прямо или косвенно относящаяся к физическому лицу, и позволяющая его определить.

К персональным данным, согласно данному закону, относят:

- ⇒ фамилия, имя, отчество;
- ⇒ место, дата рождения;
- ⇒ место постоянной или временной регистрации;
- ⇒ фотография или видеозапись человека, позволяющие идентифицировать человека;
- ⇒ сведения о детях, родственниках, семейном положении;
- ⇒ сведения о заработной плате;
- ⇒ оценка навыков, личностных качеств;
- ⇒ индивидуальные личные данные (раса, национальность, политические или религиозные взгляды, философские убеждения; состояние здоровья);
- ⇒ информация о судимостях, или их отсутствии;
- ⇒ номер телефона, адрес электронной почты, иные идентификаторы в соц. сетях или мессенджерах;
- ⇒ паспортные данные, СНИЛС, ИНН;
- ⇒ биометрические данные.

Но стоит учитывать, что некоторые из этих данных сами по себе, без связи с другими данными, персональными являться не могут. Если номер телефона сам по себе не является персональными данными, то в базе оператора, с указанием ФИО владельца — является. Адрес электронной почты в формате petrov_sergey_1987@mail.ru — тоже относится к персональным данным, как и ФИО, с привязкой к ИНН, номеру телефона или месту регистрации.



Также существует классификация персональных данных. Их подразделяют на:

- ⇒ общедоступные;
- ⇒ специальные;
- ⇒ биометрические;
- ⇒ иные.

Общедоступные — те, на доступ к которым дано согласие субъекта персональных данных, а не те, которые можно найти в общем доступе в интернете.

Специальные — информация о расе, национальности и религии; политических и философских взглядах, здоровье, подробностях личной жизни, судимостях.

Биометрические — информация о физиологических и биологических особенностях человека. Это отпечатки пальцев, генетическая информация, рисунок радужной оболочки глаз, образцы голоса, фотографии.

К иным данным относится все остальное. Это и электронная почта или геолокация, информация о принадлежности к определенной социальной группе, стаж работы и пр.

- **Ваши данные могут использовать для незаконных финансовых операций.** Чтобы снять ограничения в некоторых платежных системах, достаточно предъявить фото паспорта. В этом случае вы рискуете стать участником дел о незаконной торговле или финансировании терроризма.

- **За публикацию неоднозначной фотографии и комментария в социальной сети вы можете стать жертвой кибербуллинга.**

И это еще далеко не полный перечень «неприятностей», которые могут случиться, если мы не будем серьезно относиться к защите персональных данных.

Как защитить реквизиты на карте?

Из данных карты можно сообщать только ее номер. Имя, фамилию, срок действия и код безопасности сообщать не стоит никому и никогда. Если пришел смс-код от банка, его тоже нельзя сообщать другим людям.

Если вдруг вы оставили свою карту без присмотра, сразу перевыпускайте. Чтобы снизить риск кражи персональных данных в интернете, заведите карту для офлайна с отключенными платежами в интернете. И подключите смс-банк либо push-уведомления об операциях!

Что делать, если просят копию паспорта?

Предоставлять паспортные сведения можно только проверенным людям и компаниям, когда паспорт действительно необходим. Например, без этих данных не обойтись, если оформляете договор аренды или хотите оформить кредит. В менее важных случаях лучше отказать в предоставлении данных паспорта.

Лучше не давать делать копии всех страниц паспорта: первой страницы и страницы с пропиской вполне достаточно. Для защиты персональных данных по возможности напишите на копии паспорта, для



Как нам могут навредить, используя наши персональные данные?

- ФИО и номера телефонов — номера часто запрашивают на сайтах для авторизации, но некоторые пользователи не раздумывая вводят и свои реальные фамилии с именами. Тот же «комплект» может быть скопирован, например, из адресной книги компании.



Утечка базы данных сотрудников с телефонами и электронными адресами может быть использована для проникновения в информационные системы компании или же дальнейшего персонального мошенничества, так как позволяет обратиться к человеку персонализировано, войти с ним в контакт, заставить открыть заражённую ссылку или же получить другую ценную информацию.

- Иногда мы сами охотно делимся своими конфиденциальными данными — осталось их только взять и использовать. Были, когда счастливики, летящие в отпуск, выкладывали в соцсеть свои посадочные талоны, а потом сильно жалели об этом. **Зная вашу фамилию и номер билета можно попасть в вашу учетную запись. И, например, аннулировать регистрацию или полет.** Гораздо хуже, если авиакомпания при вводе этих данных дает полный доступ к аккаунту, где указаны номера телефонов, адрес электронной почты, номера паспорта и бонусной карты.

- **На ваше имя могут оформить кредит или микрозайм.** Мошенникам достанутся деньги, а вам — звонки коллекторов и обязанность погасить долг. Конечно, такой кредит можно оспорить в суде, но вы потратите время и нервы.

- **Вы можете стать учредителем фирмы-однодневки.** Паспортных данных достаточно, чтобы зарегистрировать на ваше имя ООО или открыть ИП. Фирмы-однодневки используются для отмывания денег и организации преднамеренного или фиктивного банкротства, ответственность за которые несет в том числе учредитель.

Стоит упомянуть, кто является субъектом персональных данных, а кто оператором. Соответственно, субъект — физическое лицо, чьи данные обрабатывают. К примеру, собирают и хранят. А оператор персональных данных — юридические лица, государственные организации или ведомства. Они данные собирают, обрабатывают, хранят, передают и уничтожают.

Что надо знать если вы оператор персональных данных?

Любой договор с физлицом, содержащий его личные данные (а он и будет их содержать, если это не публичная оферта), должен в обязательном порядке содержать раздел о персональных данных. Без письменного согласия человека, обработка персональных данных оператором, а также их передача третьим лицам — запрещена.

Обработка персональных данных — это вообще любые действия, которые с совершают. Сюда входит:

- ⇒ сбор;
- ⇒ передача;
- ⇒ запись;
- ⇒ хранение;
- ⇒ извлечение;
- ⇒ изменение;
- ⇒ обезличивание;
- ⇒ анализ;
- ⇒ удаление.

В свою очередь, обработка может осуществляться тремя путями:

Автоматизированная — с помощью средств вычислительной техники. Это компьютеры, телефоны и другие электронные устройства, базы данных, криптографические средства защиты, программы, скрипты.

Смешанная — обработка человеком при участии средств вычислительной техники. Например, когда в бухгалтерии



вбивают в программу данные из бумажного заявления на отпуск.

Неавтоматизированная — без автоматизации.

После того, как персональные данные обработаны они отправляются на хранение в архив. Это может быть и отдельное специализированное помещение (если речь о бумажных документах) и электронное хранилище (например, облачное). В любом случае вам впоследствии нужно иметь возможность оперативно найти данные и уничтожить их (по требованию субъекта) или передать (в силу закона).



В каком порядке должна осуществляться обработка персональных данных физлиц

До начала обработки данных вам нужно определить ее цель. Это важно, поскольку обработка должна соответствовать этой цели. В частности, вы не можете запрашивать данные, не связанные с этой целью. Например, получать у лица, с которым вы заключаете договор, персональные данные членов его семьи.

Если вы используете персональные данные граждан только для заключения и исполнения договоров с ними и никому их не передаете, то вам не нужно получать согласие гражданина на обработку данных и уведомлять о ней Роскомнадзор.

Какой должна быть цель обработки персональных данных

Цель должна быть:

1) законной;

2) заранее определенной. Еще до начала обработки вы должны определиться с целью, которую вы преследуете, и довести ее до гражданина, чьи данные получаете. Для этого укажите цель в согласии на обработку персональных данных. Рекомендуем также закрепить ее в локальном акте, посвященном обработке данных (Рекомендации Роскомнадзора). Лучше, если цель обработки будет соответствовать той деятельности, которую вы фак-

1 ст. 272 УК РФ);

⇒ неправомерный отказ должностного лица в представлении гражданину документов и материалов, собранных в установленном порядке и непосредственно затрагивающих его права и свободы гражданина (ст. 140 УК РФ).

Учтите, что к уголовной ответственности могут привлечь только физическое лицо (ст. 19 УК РФ). Однако привлечение виновного физического лица к уголовной ответственности не освобождает от административной ответственности организацию (ч. 3 ст. 2.1 КоАП РФ).

Что надо знать если вы субъект персональных данных?

Ваши персональные данные — ваша собственность. К ним относятся информация паспорта, банковской карты — эту информацию вы часто оставляете в интернете. А еще доступ к вашим персональным данным — хлеб для мошенников.



Чтобы обезопасить себя от кражи данных, лучше знать наверняка, что можно сообщать другим людям, а какими персональными данными опасно делиться.

Информация о людях, их привычках и действиях нужна компаниям, чтобы продавать продукты или анализировать покупательскую способность. Но эти данные помогают в том числе и преступникам.

Многие люди неосознанно оставляют персональные данные на различных сайтах: например, когда регистрируются на какое-нибудь мероприятие или указывают свои данные в комментариях под постом или оставляют копии своих документов в различных организациях. Всю эту информацию могут использовать злоумышленники.

Административная ответственность установлена:

- ⇒ за нарушение правил обработки персональных данных;
- ⇒ неисполнение обязанностей при взаимодействии с гражданином - субъектом персональных данных;
- ⇒ невыполнение требований по защите персональных данных;
- ⇒ неисполнение обязанностей при взаимодействии с Роскомнадзором.



Если в ходе проверки будет выявлено несколько нарушений, к ответственности вас привлекут за каждое из них. Также обратите внимание, что к ответственности за нарушение могут одновременно привлечь и организацию, и виновное физическое лицо (ч. 3 ст. 2.1 КоАП РФ).

Основной вид административного наказания за нарушение законодательства о персональных данных - штраф. Его размер зависит от конкретного нарушения. Например, максимальный штраф для организации за обработку персональных данных без письменного согласия гражданина, когда согласие требуется, или за отсутствие в нем всех необходимых сведений составляет 150 000 руб., за повторное правонарушение - 500 000 руб. (ч. 2, 2.1 ст. 13.11 КоАП РФ).

Специальной нормы об ответственности за нарушение Закона о персональных данных в Уголовном кодексе РФ нет. Однако действия лица, нарушившего правила работы с персональными данными, могут образовать состав преступления из числа предусмотренных Уголовным кодексом РФ.

В частности, уголовная ответственность установлена:

- ⇒ за незаконное соби́рание или распространение сведений о частной жизни лица, составляющих его личную и семейную тайну, без его согласия (ч. 1 ст. 137 УК РФ);
- ⇒ неправомерный доступ к компьютерной информации, в результате которого произошло уничтожение, блокирование, модификация (изменение) или копирование информации (ч.

тически осуществляете и которая предусмотрена вашими учредительными документами;

3) конкретной. Чтобы у контролирующих органов не было повода придаться к вам, рекомендуем не использовать абстрактные формулировки, а указать цель максимально конкретно. Например, если вы хотите повысить продажи путем СМС-рассылки, в качестве цели должно быть указано не "повышение продаж", а "осуществление рекламной СМС-рассылки".

Как обеспечить целевую обработку персональных данных

Чтобы обработка данных была целевой, удостоверьтесь в том, что (ч. 3 - 7 ст. 5 Закона о персональных данных):

1) содержание и объем данных соответствуют целям их обработки, то есть вы не обрабатываете избыточные данные. Избыточным может быть признано получение данных, никак не связанных с оказываемыми услугами. Например, если салон красоты просит клиентов сообщить их имущественное положение или образование;

2) у вас созданы отдельные базы для персональных данных, обработка которых осуществляется в целях, не совместимых между собой. В частности, рекомендуем иметь отдельные базы для сотрудников и клиентов;

3) вы обеспечиваете точность и достаточность, а при необходимости и актуальность данных по отношению к целям их обработки. Например, время от времени актуализируете базу телефонных номеров клиентов, обновляете полученные ранее копии документов. В противном случае вы рискуете нарушить закон. Например, это произойдет, если сменился владелец телефонного номера, а вы продолжаете отправлять на него рекламные сообщения,



хотя новый владелец своего согласия на это не давал.

Также вы должны обеспечить удаление или уточнение неполных или неточных данных;

4) вы уничтожаете либо обезличиваете данные, если цели обработки достигнуты или утрачена необходимость в их достижении (если законом не предусмотрено иное). В частности, не рекомендуем хранить документы, содержащие персональные данные, дольше, чем это необходимо в целях бухгалтерского и налогового учета.



Что должен делать оператор при получении персональных данных от физлица

У оператора при сборе персональных данных возникают следующие основные обязанности (ч. 1, 2 ст. 18 Закона о персональных данных):

1) предоставить информацию гражданину, если он об этом просит. Речь идет о сведениях, указанных в ч. 7 ст. 14 Закона о персональных данных. В частности, вы должны сообщить, кто, на каком основании, с какой целью и какими способами будет обрабатывать его данные;

2) разъяснить последствия отказа предоставить данные, если их предоставление является обязательным в соответствии с федеральным законом. Например, если при покупке SIM-карты гражданин отказывается предоставить свои паспортные данные, то последствие, как правило, выражается в отказе предоставить услугу. Факт разъяснения рекомендуем оформить документально, например получить с гражданина расписку о том, что он его получил.

Какие сведения относятся к биометрическим персональным данным

Биометрические персональные данные - это такие сведения

о физиологических и биологических особенностях человека, по которым можно установить его личность (ч. 1 ст. 11 Закона о персональных данных).

Какие именно сведения являются биометрическими персональными данными, Закон о персональных данных не определяет. Конкретного исчерпывающего перечня таких сведений нет и в нормативных документах.

Как правило, к биометрическим персональным данным относят, например (Письма Минцифры России от 17.07.2020 N ОП-П24-070-19433, Роскомнадзора от 10.02.2020 N 08АП-6782):

- ⇒ фотографическое изображение человека;
- ⇒ видеоизображение человека;
- ⇒ дактилоскопические данные;
- ⇒ информация о радужной оболочке глаза;
- ⇒ результаты анализов ДНК;
- ⇒ данные о голосе.

Кто и какую ответственность несет за нарушение законодательства о персональных данных

Если вы обрабатываете персональные данные граждан (клиентов, сотрудников), то за нарушения по работе с этими данными вас могут привлечь прежде всего к административной ответственности. Например, административный штраф может быть назначен за сбор персональных данных в ненадлежащих целях.

Гражданско-правовая ответственность наступит, если вы причинили убытки или моральный вред гражданину. Своих сотрудников, допустивших нарушение, вы можете привлечь к дисциплинарной и материальной ответственности. Как работодатель вы отвечаете за нарушение правил работы с персональными данными работников.

Если действия физлица содержат признаки преступления, то его могут привлечь к уголовной ответственности.

