# ***Защити свои персональные данные***

Отношения, связанные с обработкой персональных данных, регулирует Федеральный закон № 152-ФЗ «О персональных данных» (далее – Закон №152-ФЗ), действие которого направлено на защиту прав и свобод человека и гражданина при обработке его персональных данных

При этом в законе № 152-ФЗ нет точного определения, что относится к персональным данным человека, есть только указание на возможность идентификации человека по этим данным.

***То, что точно позволяет идентифицировать физическое лицо, — это:***

— паспортные данные,

— реквизиты банковского счета,

— ИНН,

— СНИЛС и др.

Некоторые данные о человеке, к примеру номер телефона или его имя, по отдельности не позволяют его идентифицировать, однако если у компании есть доступ к ним в совокупности, это сделать просто.

Например, по имени «Иван Петров» нельзя определить личность, но если мы знаем его место работы мы уже сможем найти его среди сотрудников этой компании.

Что же чаще всего входит в персональные данные физического лица?

**Что входит в персональные данные?**

➕ Имя, фамилия, отчество

➕ Контактная информация: адрес, номера телефонов, email, почтовые адреса.

➕ Идентификационные номера: номера паспорта, ИНН, СНИЛС и другие идентификационные коды.

➕ Информация о местоположении человека: GPS-координаты.

➕ Финансовая информация: банковские реквизиты, номера карт, информация о доходах, расходах, кредитах.

➕ Медицинская информация: данные о здоровье и медицинская история.

➕ Информация о работе и образовании: место работы, должность, образование.

➕ Фото человека.

***Согласно российскому законодательству, обработка персональных данных, за некоторыми исключениями, требует согласия субъекта.***

Согласие является инструментом, который позволяет субъекту контролировать, как его персональные данные обрабатываются, и защищает его права на неприкосновенность частной жизни, личную и семейную тайну.

Дети — несовершеннолетние граждане, поэтому согласно ч. 1 ст. 64 Семейного кодекса их права защищают родители и законные представители. Давая согласие, родитель подтверждает, что такая обработка является законной и не нарушает права ребенка.

Несовершеннолетние в возрасте от 14 до 18 лет обладают всеми правами и обязанностями субъекта персональных данных и вправе самостоятельно давать осознанное согласие на обработку своих персональных данных при получении образовательных услуг.

***Что такое согласие на обработку персональных данных?***

Согласие на обработку персональных данных — это однозначное разрешение от конкретного человека на то, чтобы компания могла обрабатывать его персональные данные.

Согласие на обработку персональных данных должно соответствовать следующим критериям:

✅ Должно быть четко указано, для каких целей данные будут использоваться. Это может быть предоставление определенных услуг, рассылка или реклама.

✅ Человек должен явно выразить согласие на обработку своих персональных данных.

✅ Должно быть указано, какие конкретные данные будут собираться: имя, адрес, номер телефона, адрес электронной почты и т. д.

✅ Указаны сроки обработки персональных данных.

✅ Прописаны права пользователя на доступ к данным, право на исправление неточностей, право на удаление данных и др.

✅ Если данные будут передаваться третьим лицам, это также должно быть указано в согласии.

✅ Нужно получить отдельное согласие на маркетинговые коммуникации.

Если данные будут использоваться для маркетинговых целей, пользователь должен дать отдельное согласие на это.

✅ Указана возможность отменить согласие.

✅ Указаны контактные данные оператора.

Должны быть предоставлены контактные данные ответственного лица, чтобы пользователь мог обратиться с вопросами или запросами.

✅ Оформлено информированное согласие.

***Согласие должно быть предложено*** ***после того, как человек получил всю необходимую информацию и полностью понимает, как его данные будут использоваться.***

Использование персональных данных без согласия, умышленные незаконные сбор, обработка, хранение или предоставление персональных данных физического лица либо нарушение его прав, связанных с обработкой персональных данных, — влекут наложение штрафа в размере до пятидесяти базовых величин (ч. 1 ст. 23.7 КоАП).

Утечка персональных данных представляет серьезную угрозу как для отдельных лиц, так и для организаций. Для физических лиц это может привести к краже личной информации, финансовому мошенничеству, шантажу и другим неприятным последствиям.

В частности, мошенник, установив контакт с ребенком, может отправить ему ссылку или файл и попросить открыть, чтобы «выполнить задание» и получить за это подарки. Часто ссылка имитирует страницу банковского сайта. Мошенники в качестве задания могут попросить ребенка ввести на этой странице данные банковских карт родителей.

С использованием чужих паспортных данных мошенники могут зарегистрировать компанию, которая будет заниматься незаконной деятельностью. При этом, формально, владелец паспорта числится директором такой фирмы и несет ответственность за её действия.

***Зачем мошенники взламывают Госуслуги?***  
  
Мошенники часто используют украденные личные данные для оформления кредитов. Это могут быть данные паспорта, СНИЛС или другие документы, которые можно получить через взлом аккаунтов, почтовых ящиков. При помощи сайтов-ловушек мошенники могут выманивать у граждан реквизиты банковских карт. Такой вид мошенничества называется "фишинг".  
Ваш номер телефона может быть использован для получения доступа к большему количеству ваших персональных данных . Если вы не предпримете необходимые шаги для его защиты, хакеры могут захватить ваши учетные записи, запустить фишинговые атаки и украсть ваши личные данные. Ограничение разрешений приложений, добавление PIN-кода к вашей SIM-карте и использование биометрии — отличные первые шаги.

Современным мошенникам бывает достаточно только номера карты и срока её действия, чтобы получить доступ к средствам. Старайтесь никому не говорить несколько реквизитов сразу. Чем больше информации известно злоумышленникам, тем выше риск остаться без денег. Номер, фамилия и имя держателя или номер и срок действия.

Однозначно нельзя никому говорить паспортные данные (серия, номер, кем выдан и так далее), тем более фотокопии паспорта, если вы не хотите, чтобы на вас оформили кредит или даже зарегистрировали компанию. Кроме того, вспомните, кому вы посылали копии своего паспорта. Все ли эти люди надёжны?

Мошенники часто используют украденные личные данные для оформления кредитов. Это могут быть данные паспорта, СНИЛС или другие документы, которые можно получить через взлом аккаунтов или фишинг.

***Как понять, что на тебя взяли кредит через Госуслуги?***

Самым надежным способом узнать о наличии кредитов, взятых на ваше имя, является запрос вашей кредитной истории. Кредитная история покажет все кредиты, которые были оформлены на вас, включая даты и суммы кредитов.

Сделать это можно на портале Госуслуг. Для этого необходимо выбрать раздел «Услуги», затем «Справки и выписки», потом «Сведения о бюро кредитных историй» либо вместо этого сразу ввести в строке поиска запрос «узнать своё БКИ».

С 1 марта 2025 года появилась возможность установить на себя запрет на взятие любого кредита в режиме онлайн или офлайн. В первом случае нужно зайти на портал «Госуслуги», во втором — в любое удобное отделение МФЦ.

Подайте заявление и прикрепите данные СНИЛС.

***Как установить запрет на получение кредитов в режиме онлайн?***

1. Перейдите к услуге
2. Проверьте ваши данные: ФИО, серию и номер паспорта, ИНН
3. Выберите, какой вид запрета хотите установить: полный или частичный
4. Проверьте сформированное заявление и подпишите его при помощи электронной подписи
5. Отправьте заявление

***Можно ли аннулировать кредит, взятый мошенниками?***

Обратитесь в банк или МФО с письменным заявлением о мошенничестве и потребуйте аннулировать кредитный договор. Форму заявления запросите в банке или МФО. Приложите к заявлению: талон‑уведомление из полиции

Утечка личных данных чревата последствиями. Оставляя данные о себе в учреждениях, магазинах, помните: мошенники могут использовать их против вас.

***Если вдруг вы потеряли паспорт или его украли, в срочном порядке нужно писать заявление в полицию***.

Следует обратить внимание, что мошенники всё чаще используют персональные данные граждан в своих целях. Они крадут их через интернет, увеличилось число заявок на получение банковских карт от чужого имени, в связи с чем необходимо использовать уникальные пароли для максимально возможного количества учётных записей в интернете. Лучше завести отдельный пароль для каждой из них.

При этом ***нельзя хранить логины и пароли в своём смартфоне*** — в виде заметки или электронного сообщения. Если устройство будет потеряно, данные попадут в руки аферистов.

Стоит проверять, нет ли ваших данных в открытом доступе. Для этого ряд ресурсов предлагает сервисы, которые могут мониторить интернет. В случае упоминания в сети ваших персональных данных вы получите уведомление. Выявив такой факт, вам стоит обратиться в Роскомнадзор, который обяжет владельцев ресурсов, где информация о вас выставлена напоказ, убрать её.

***!!! Не открывайте ссылки и вложенные файлы в письмах и SMS - сообщений от незнакомцев.***

Сегодня Центробанк отмечает участившиеся случаи краж денег при помощи смартфонов, телефонов, планшетов.

Устройства заражаются вредоносными программами и вирусами через спам-рассылку SMS-сообщений или сообщений по электронной почте. Стоит человеку перейти по вредоносной ссылке, как вирус устанавливается на его устройство.

А дальше вирусы отправляют SMS-сообщения от вашего имени на короткие номера, перехватывают одноразовые коды подтверждения, приходящие на мобильное устройство для дополнительного подтверждения операции. А также формируют и отправляют от имени пользователя распоряжения на перевод денег для оплаты товаров и услуг. При этом вредоносная программа скрывает от клиента уведомления от банка о списании денежных средств.

Банк России рекомендует: установите антивирусное программное обеспечение с регулярно обновляемыми базами и не переходите по ссылкам из недостоверных источников.

***!!! Банковские карты: пароли храним при себе***

- Ещё один вид мошенничества — массовые e-mail-рассылки, якобы от вашего банка. Цель аферистов — заманить получателей сообщений на сайты-ловушки, на которых под различными предлогами мошенники попытаются получить персональные данные — идентификатор и пароль для входа в интернет-банк, кодовые слова банковских карт, номера банковских карт, пин-коды, CVV и прочую информацию.   
Получателям писем будут настойчиво рекомендовать открыть вложенные файлы или перейти по ссылкам. Делать этого нельзя — файлы содержат вирусы.  
  
Но для опытного мошенника не составит труда выяснить пин-код карты лично у доверчивого гражданина. Например, на ваш номер приходит SMS-сообщение с незнакомого номера, где вас информируют о проблемах с картой. И просят срочно перезвонить.  
  
- Мошенники присылают сообщение, что карта заблокирована, и предлагают позвонить на номер. Люди в панике начинают звонить и выяснять. Как только человек позвонил, они его будут держать до последнего. Человек начинает делать то, что ему говорят: подойдите к банкомату, наберите комбинацию цифр, сейчас вам придёт код.  
  
***!!! Главная рекомендация:*** ни в коем случае не перезванивайте на указанные номера. Просто игнорируйте сообщения. И уж, конечно, не нужно идти к банкомату и предпринимать какие-либо действия. Помните: реальные сотрудники банка никогда не будут спрашивать у клиента реквизиты карты, пароль и другую важную информацию.  
  
Сегодня и правоохранительные органы, и банки не устают повторять: не сообщайте незнакомцам личные данные, а также данные банковских карт. Даже продвинутые системы безопасности в банках не помогут, если игнорировать простые правила.

***Поэтому:***  
- прикрывайте клавиатуру банкомата рукой, когда вводите пин-код;  
  
- подключайте SMS-сервис "Мобильный банк" только на свой номер телефона, переводите деньги только известным вам получателям;  
  
- помните: вход в зоны самообслуживания не требует ввода пин-кода вашей карты.