Статья №2.

Информирование и просвещение населения по вопросам защиты прав потребителей

Цифровой мир: надёжные смарт-устройства» –
девиз Всемирного дня прав потребителей на 2019 год

Ежегодно Международная Федерация потребительских организаций (CI) выбирает девиз всемирного дня защиты прав потребителей, который традиционно отмечается 15 марта и в 2019 году он проходит под девизом «Trusted Smart Products» - Цифровой мир: надежные смарт-устройства.

Словосочетание смарт-устройства прочно закрепилось в нашем словаре, и применяем мы его по отношению к современным сложным технологическим устройствам: смарт-телевидение, смартфон, смарт часы и т.д. В переводе с английского слово "смарт" означает умный, быстрый, сообразительный.

Смарт-устройство представляет собой электронное устройство, как правило, связанное с другими устройствами или сетями с помощью различных беспроводных протоколов, таких как Bluetooth, NFC, Wi-Fi, и т.д. Смарт-устройства могут работать в интерактивном режиме и автономно.

Таким образом, общим для всех устройств, названия которых мы произносим с добавлением слова смарт, является обилие выполняемых функций и возможность их расширения за счёт установки новых приложений. Такая возможность обусловлена тем, что устройства работают под контролем мобильных операционных систем.

По мере того, как все больше граждан подключаются к Интернету во всех уголках планеты, смарт-устройства становятся повседневной реальностью для потребителей, что знаменует коренное изменение процесса взаимодействия людей с "умной" электроникой, гаджетами и продвинутыми услугами.

Появление "умных" технологий приносит много возможностей для потребителей, однако существуют некоторые серьезные причины для беспокойства: сетевая уязвимость или утечка информации. Бывает, нарушается конфиденциальность личных данных, люди не знают о возможных рисках и о том, кто несет ответственность при возникновении убытков. Цифровые технологии уже третий год подряд формируют тематику Всемирного дня прав потребителей.

Главным трендом роста потребительского рынка становится цифровизация общества, появление культуры не только оплаты услуг и товаров онлайн, но и активное использование новых технологий распознавания лиц и отпечатков пальцев, геолокационных и облачных сервисов, связанных между собой цифровых продуктов и смарт-устройств, виртуальных помощников, обладающих искусственным интеллектом.

Сегодня цифровые технологии изменили характер многих услуг и продуктов, так как встроенное программное обеспечение содержится во всё возрастающем количестве потребительских товаров.

В этой связи является закономерным, что в Стратегии государственной политики Российской Федерации в области защиты прав потребителей на период до 2030 года поставлены четкие задачи в области защиты прав потребителей. Важно, чтобы потребители обладали набором базовых прав и знаний, чтобы они были защищены.

Важно, чтобы потребители обладали набором базовых, неснижаемых прав, независимо от того, касается это, например, приобретения офлайн товаров и услуг или покупок в сети Интернет. Тем более, что по мере глобального развития сегмента электронной коммерции и вовлечения в нее все большего числа активных пользователей сети Интернет потребуется не только изменение законодательства, но и реализация иных мер, которые для потребителей новой цифровой эпохи обеспечат достаточный уровень защиты, комфорта и безопасности при совершении дистанционных покупок.

Предстоящий Всемирный день прав потребителей будет хорошим поводом еще раз обратить внимание на то, что прогресс цифровых технологий должен прежде всего учитывать разносторонние интересы потребителей: это и право на качество и безопасность «умной электроники», и право знать о том, как собирается, обрабатывается и используется личная информация.

Разглашение личной информации запрещено по действующему законодательству России.

Исключение – наличие собственного согласия. Под персональными данными подразумевается данные как напрямую связанные с человеком, так и косвенно.

Что значит разглашение персональных данных с точки зрения закона?

Персональные данные – это любая информация, прямо или косвенно относящаяся к определенному физическому лицу, а их обработка – это любое действие, совершаемое с персональными данными.

152-м Федеральным Законом оговаривается термин «персональные сведения». Имеются в виду данные о гражданах, которыми обладают работодатели, организации, структуры и объединения. Информацию предоставляют нанятые работники, клиенты, заявители и т.д.
Частной информацией могут служить сведения о:

- регистрации;
- паспортных реквизитах;
- образовании;
- наличии судимостей;
- месте трудоустройства;
- детализации телефонных звонков и переписки;
- перенесенных заболеваниях;
- личной жизни;
- родственных связях и родственниках;
- членах семьи;
- материальном положении и доходах;
- наличии имущества;
- прочее.

Обработка персональных данных всегда должна ограничиваться достижением конкретных, заранее определенных и законных целей. При обработке персональных данных нужно обеспечить 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.

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. Обрабатываемые 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.

При сборе персональных данных, в том числе посредством сети Интернет, оператор обязан обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации. Вышеупомянутый Федеральный Закон устанавливает процедуру получения доступа к личной информации. Статья под номером 5 требует соблюдение тайны. Распространяются сведения в соответствии с законодательством и на основании его принципов. Иначе в действие вступает иная статья, теперь уже Уголовного Кодекса России (№137).

Добровольная передача личных данных работодателю предполагает наличие доступа к ним ограниченному числу должностных лиц. Таковыми могут быть:

- учредители;
- генеральный директор;
- начальник структурного подразделения, цеха, отдела;
- сотрудники отдела кадров;
- работники расчетного отдела;
- главный и рядовые бухгалтеры;
- штатные юристы.

Использование сведений не по назначению приводит в действие по отношению к нарушителю статью 137-ю УК РФ.

Среднестатистический россиянин часто сталкивается с понятием конфиденциальной информации, но многие не знают, что этот термин закреплен на законодательном уровне и за

незаконное распространение грозят наказания. Конфиденциальные данные налагают на всех держателей определенные обязанности.

Если они не соблюдаются, то житель Российской Федерации имеет полное право предъявить претензии по этому поводу.

Распространять данные запрещено, использовать их можно только в целях, согласованных с обладателем. Например, когда заявитель обращается в банк за кредитом и предоставляет пакет документов, то финансовая организация должна использовать полученную информацию только для проверки платежеспособности претендента на кредит.

Согласно Указу Президента России от 6 марта 1997 года с дополнениями от 23 сентября 2015 года, персональные данные являются конфиденциальной информацией.

За разглашение информации и распространение документов, содержавших конфиденциальную информацию, гражданин может быть привлечен к дисциплинарной, материальной, административной и уголовной ответственности в зависимости о тяжести проступка.

Распространение данных, доступ к которым был ограничен федеральным законом, влечет за собой административную ответственность (статья 13.14 Кодекса РФ об административных правонарушениях).

Статья 13.14 КоАП РФ. Разглашение информации с ограниченным доступом

Разглашение информации, доступ к которой ограничен федеральным законом (за исключением случаев, если разглашение такой информации влечет уголовную ответственность), лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей, за исключением случаев, предусмотренных частью1 статьи 14.33 настоящего Кодекса, — влечет наложение административного штрафа на граждан в размере от пятисот до одной тысячи рублей; на должностных лиц — от четырех тысяч до пяти тысяч рублей.

Как видите, законодательство Российской Федерации защищает конфиденциальность информации, а граждане, столкнувшиеся с нарушениями, могут отстоять свои права и получить компенсацию. Пользуйтесь своими возможностями, как известно, информация в современном мире уже стала одним из самых дорогостоящих капиталов, и его необходимо беречь.

Нарушение конфиденциальности персональных данных.

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 (ст.7 Федерального закона от 27.07.2006 №152-ФЗ "О персональных данных").

Нарушение конфиденциальности персональных данных потенциально не обратимо (ставшие публичными персональные данные невозможно снова сделать конфиденциальными), поэтому даже не повлекшее морального вреда такое нарушение является грубым нарушением норм Федерального закона "О персональных данных".

Случайное или преднамеренное неправомерное действие физического лица в отношении персональных данных, следствием которых является нарушение безопасности персональных данных при ее обработке техническими средствами в информационных системах персональных данных, вызывающее негативные последствия (ущерб/вред) субъекту персональных данных.

При нарушении конфиденциальности персональных данных в информационных системах персональных данных возможны следующие деструктивные действия:

- утечка информации;
- несанкционированное копирование;
- перехват информации в каналах передачи данных;
- разглашение (публикация) защищаемой информации.

Угрозы конфиденциальности персональных данных - это утечка, перехват, съем, копирование, хищение и разглашение персональных данных.

Таким образом, с учетом вышеизложенного, под нарушением конфиденциальности персональных данных понимается факт реализации деструктивных действий (копирование, неправомерное распространение).

В законодательстве Российской Федерации предусмотрена ответственность за нарушение конфиденциальности персональных данных:

- неправомерное копирование персональных данных (ч.6 ст.13.11 КоАП РФ, ст.272 УК РФ);
- неправомерное предоставление и распространение персональных данных (ч.6 ст.13.11 КоАП РФ, ст.137 УК РФ);
- разглашение персональных данных работника (п.6 "в" ст.81 ТК РФ);

- разглашение персональных данных (ст.13.14 КоАП РФ, п.3 "в" ч.1 ст.37 Федерального закона от 27.07.2004 №79-ФЗ "О государственной гражданской службе Российской Федерации");
- разглашение (публикация) персональных данных в СМИ, а также в информационно-телекоммуникационных сетях (ч.7 ст. 13.15 КоАП РФ, ст.137 УК РФ).

Ужесточилась ответственность за нарушение законодательства о персональных данных.

Теперь же к административной ответственности оператора привлекут только в случае наступления неблагоприятных последствий, связанных с невыполнением условий, обеспечивающих сохранность данных при хранении материальных носителей. В качестве примеров неблагоприятных последствий ч. 6 ст. 13.11 КоАП РФ называет неправомерный или случайный доступ к персональным данным, их уничтожение, изменение, блокирование, копирование, предоставление, распространение.

Если гражданин заметил личные данные (ФИО, адрес, телефонный номер или даже паспортные данные) на стороннем ресурсе, стоит немедленно обратиться в Роскомнадзор с соответствующей жалобой, ведь распространение личной информации без разрешения владельца запрещено федеральным законодательством.

Если все условия будут соблюдены, Роскомнадзор составит протокол об административном правонарушении со стороны ресурса. Жалобу можно составить при помощи свободной формы.

Для оформления гражданину потребуются:

- ФИО, место прописки и номер телефона;
- название организации, ссылка на официальный вебсайт.

В составленной жалобе опишите все нарушения, замеченные со стороны ресурса. Приветствуются ссылки на законы, подтверждающие правоту жертвы. Распространенная ошибка — выражение своего эмоционального состояния в документе, а также наличие никому не нужной брани.

Обратите внимание! Обязательным пунктом является мера ответственности, которую должен понести нарушитель административного кодекса Российской Федерации. Также следует исключить грамматические ошибки, нецензурную брань, все эти факторы будут только отвлекать от сути, и ни к чему хорошему это не приведет.

В качестве доказательств следует использовать:

- запись беседы по телефону;
- видеоматериалы;
- информация, опубликованная в газетах;
- фотоматериалы, подтверждающие факт нарушения законов;
- скриншоты сайтов;

Предстоящий Всемирный день прав потребителей будет хорошим поводом еще раз обратить внимание на то, что прогресс цифровых технологий должен прежде всего учитывать разносторонние интересы потребителей: это и право на качество и безопасность «умной электроники», и право знать о том, как собирается, обрабатывается и используется личная информация.