

Персональные данные в общем доступе. Как избежать распространения и привлечь к ответственности нарушителя?

RTM TECHNOLOGIES – первая экспертная компания, специализирующаяся на проведении нормативных и нормативно-технических экспертиз в области ИБ и ИТ.

СОДЕРЖАНИЕ

- 01** Зачем сайты (операторы) собирают ПДн?
- 02** Обработка ПДн онлайн-платформами (или сайтами), легитимность, риски и пути их нивелирования.
- 03** Особенности предоставления согласия на обработку ПДн онлайн, возможность и легитимность предоставления согласия на обработку биометрических ПДн онлайн
- 04** Как защитить себя владельцу сайта с помощью политики конфиденциальности и правил обработки ПДн?
- 05** Чем обусловлено внесение изменений в ФЗ-152 и издание Роскомнадзор Приказа от 24.02.2021 №18 «Об утверждении требований к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения»? В чем особенности «распространения» ПДн как вида обработки ПДн, почему именно «распространение»?
- 06** Сравнение требований к форме и содержанию согласий по ФЗ-152 и по Приказу №18. Отличия, особенности порядка предоставления/получения
- 07** Запуск Роскомнадзор информационной системы для сбора согласий на обработку разрешенных для распространения персональных данных: для кого это нужно, что сделано, что планируется, каков функционал, в чем риски участников взаимодействия и как их исключить?

1. ЗАЧЕМ САЙТЫ (ОПЕРАТОРЫ) СОБИРАЮТ ПДН?

152-ФЗ «О персональных данных»:

Персональные данные – это любая информация, относящаяся прямо или косвенно к определённому, или определяемому физическому лицу.

Оператор - государственный или муниципальный, 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.

2. ОБРАБОТКА ПДН ОНЛАЙН-ПЛАТФОРМАМИ (ИЛИ САЙТАМИ), ЛЕГИТИМНОСТЬ, РИСКИ И ПУТИ ИХ НИВЕЛИРОВАНИЯ

Размер штрафа по ст. 13.11. КоАП РФ варьируется:

- для граждан – от 700 до 100 000 рублей;
- для должностных лиц – от 3 000 до 800 000 рублей;
- для юридических лиц – от 15 000 до 18 000 000 рублей.

2. ОБРАБОТКА ПДН ОНЛАЙН-ПЛАТФОРМАМИ (ИЛИ САЙТАМИ), ЛЕГИТИМНОСТЬ, РИСКИ И ПУТИ ИХ НИВЕЛИРОВАНИЯ

Наиболее распространенные примеры:

- На Интернет-ресурсе, принадлежащем Gandi SAS, Роскомнадзор выявил нарушение, а именно, при проставлении «галочки» о согласии на обработку персональных данных, клиенту не предоставляется информация относительно оператора, обрабатывающего персональные данные, кроме того, персональные данные граждан РФ обрабатываются на территории США, отсутствует документ, определяющий политику оператора в отношении обработки персональных данных и сведения о реализуемых требованиях к защите персональных данных (ч.5 ст.18 №152-ФЗ О персональных данных). По результатам рассмотрения дела, деятельность Интернет-ресурса признана незаконной и нарушающей права граждан на неприкосновенность частной жизни, личную и семейную тайну, осуществляемой с нарушением законодательства РФ в области персональных данных. Интернет-ресурс включен в Реестр нарушителей прав субъектов персональных данных.
- В рамках мероприятия систематического наблюдения в сети Интернет Роскомнадзор проведена проверка и обнаружено, что компания с доменным именем <https://twitter.com> осуществляет сбор персональных данных граждан Российской Федерации, не обеспечив их обработку с использованием баз данных, находящихся на территории Российской Федерации, чем нарушило ч. 5 ст. 18 №152-ФЗ О персональных данных. В 2020 году компания Твиттер, Инк. (Twitter Inc.) признана виновной в совершении правонарушения (по ч.6 ст.13.11 КоАП) и назначен штраф - 4 000 000 руб.

2. ОБРАБОТКА ПДН ОНЛАЙН-ПЛАТФОРМАМИ (ИЛИ САЙТАМИ), ЛЕГИТИМНОСТЬ, РИСКИ И ПУТИ ИХ НИВЕЛИРОВАНИЯ

Документы для сайта:

- Политика конфиденциальности
- Правила работы с ПДн
- Согласие на обработку ПДн

Рекомендации - на сайте Роскомнадзора <https://rkn.gov.ru/>

Кейс из практики:

Роскомнадзор обратился с запросом в Автосалон об обязанности уведомления об обработке персональных данных и необходимости регистрации в реестре в качестве оператора.

Автосалон, посчитал, что подпадает под исключения, предусмотренные ч.2 ст. 22 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», в соответствии с которыми вправе осуществлять обработку персональных данных без уведомления уполномоченного органа (трудовые отношения с работниками, в связи с заключением договора купли-продажи, в целях однократного пропуска субъекта персональных данных на территорию Автосалона), о чем уведомил Роскомнадзор информационным письмом.

Однако, в ответ Роскомнадзор направил разъяснения, согласно которым, Автосалон обязан зарегистрироваться в реестре, так как его вид деятельности предполагает взаимодействие с дилерами при поставке автомобилей, в том числе, для конкретного клиента, предоставление клиентам услуг по гарантийному и техническому обслуживанию транспортных средств, услуг страхования, где Автосалон выступает в качестве посредника, без заключения прямого договора с покупателем, кроме того реализована услуга тест-драйва, где персональные данные собираются на основании заявки, без договора.

Таким образом, Уполномоченный орган напрямую указал, что необходимость в регистрации в реестре операторов отсутствует в одном случае – если бы заключались только прямые договоры с покупателями, без сопутствующих и посреднических услуг.

После чего Автосалон был вынужден направить уведомление о регистрации в качестве оператора.

3. ОСОБЕННОСТИ ПРЕДОСТАВЛЕНИЯ СОГЛАСИЯ НА ОБРАБОТКУ ПДН ОНЛАЙН, ВОЗМОЖНОСТЬ И ЛЕГИТИМНОСТЬ ПРЕДОСТАВЛЕНИЯ СОГЛАСИЯ НА ОБРАБОТКУ БИОМЕТРИЧЕСКИХ ПДН ОНЛАЙН

Например, **ошибкой будет написать в согласии:**

«Пользователь ознакомлен и согласен с тем, что передача его персональных данных может осуществляться Маркетплейс в объеме, необходимом для получения Пользователем доступа к Платформе, любым третьим лицам, в том числе, осуществляющим техническое обслуживание сайта и поддержку Пользователя»

Отдельный вопрос представляет собой возможность предоставления согласия на обработку биометрических ПДн в сети «Интернет».

Согласно статье 11 №152-ФЗ, такое согласие должно быть получено в письменной форме. Статья 9 №152-ФЗ приравнивает к письменной форме электронный документ, подписанный электронной подписью.

Требования к такому электронному документу установлены № 63-ФЗ «Об электронной подписи».

К самому содержанию согласия на обработку биометрических ПДн установлен перечень обязательных сведений: паспортные данные субъекта и его представителя, данные об операторе, цель обработки данных, перечень ПДн и действий с ними, срок действия согласия и подпись субъекта (ч.4 ст. 9 №152-ФЗ).

Обратим внимание, что ФЗ-152 не предусматривает возможность подтверждения определенными действиями согласия на обработку персональных данных (конклюдентного подтверждения). Например, приобретая товар в Маркетплейс, мы можем вводить в веб-формы свои персональные данные, подтверждая тем самым готовность купить товары. Заполнение таких форм само по себе нельзя рассматривать в качестве согласия на обработку персональных данных, согласие в такой форме не принимается и необходимо прибегать к заполнению специальных форм.

4. КАК ЗАЩИТИТЬ СЕБЯ ВЛАДЕЛЬЦУ САЙТА С ПОМОЩЬЮ ПОЛИТИКИ КОНФИДЕНЦИАЛЬНОСТИ И ПРАВИЛ ОБРАБОТКИ ПДН?

С политикой конфиденциальности компании пользователя необходимо ознакомить до начала процедуры регистрации, равно как и с правилами работы с персональными данными. А перед отправкой анкетных данных на сайте пользователь должен дать согласие на обработку персональных данных (обязательно отдельный чекбокс или отдельная кнопка).

5. ЧЕМ ОБУСЛОВЛЕНО ВНЕСЕНИЕ ИЗМЕНЕНИЙ В ФЗ-152 И ИЗДАНИЕ РОСКОМНАДЗОР ПРИКАЗА ОТ 24.02.2021 №18?

Чем обусловлено внесение изменений в ФЗ-152 и издание Роскомнадзор Приказа от 24.02.2021 №18 «Об утверждении требований к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения»? В чем особенности «распространения» ПДн как вида обработки ПДн, почему именно «распространение»?

С 1 сентября 2021 года вступает в законную силу **Приказ Роскомнадзора от 24 февраля 2021 г. №18 «Об утверждении требований к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения»**, изданный во исполнение ФЗ-152, а точнее – во исполнение его мартовских изменений.

1 марта 2021 года вступили в силу изменения в **Федеральный закон № 152-ФЗ от 27.07.2006 года «О персональных данных»**.

Если лицо дало согласие на обработку, но не дало согласие на распространение, то оператор может только хранить, систематизировать, использовать ПДн, но не публиковать такую информацию в открытых источниках или передавать ее третьим лицам.

6. СРАВНЕНИЕ ТРЕБОВАНИЙ К ФОРМЕ И СОДЕРЖАНИЮ СОГЛАСИЙ ПО ФЗ-152 И ПО ПРИКАЗУ №18. ОТЛИЧИЯ, ОСОБЕННОСТИ ПОРЯДКА ПРЕДОСТАВЛЕНИЯ/ПОЛУЧЕНИЯ

В согласии клиент вправе установить, в том числе:

- запрет передачи (кроме предоставления доступа) сведений оператором неограниченному кругу лиц;
- запрет обработки (кроме получения доступа) сведений неограниченным кругом лиц;
- условия обработки (кроме получения доступа) сведений неограниченным кругом лиц.

7. ЗАПУСК РОСКОМНАДЗОР ИНФОРМАЦИОННОЙ СИСТЕМЫ ДЛЯ СБОРА СОГЛАСИЙ НА ОБРАБОТКУ ПДН

Запуск Роскомнадзор информационной системы для сбора согласий на обработку разрешенных для распространения персональных данных: для кого это нужно, что сделано, что планируется, каков функционал, в чем риски участников взаимодействия и как их исключить?

Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 21 июня 2021 г. № 106 «Об утверждении Правил использования информационной системы Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций, в том числе порядка взаимодействия субъекта персональных данных с оператором»

Физическому лицу нужно будет заверить согласие электронной подписью, после чего оператору станут доступны данные:

- о факте предоставления согласия;
- об одной или нескольких целях обработки личной информации;
- о категориях и перечне данных, которые разрешили обрабатывать.

ГОТОВЫ ОТВЕТИТЬ НА ВАШИ ВОПРОСЫ!

Хомякова Елена Сергеевна

Более 20 лет работы в сфере юриспруденции и IT
Более 1000 проектов в сфере инновационных решений
Директор правового департамента RTM Group



+7 (495) 197-64-95



info@rtmtech.ru



<https://rtmtech.ru>



GroupRTM



rtm.group



@GroupRtm



rtm.group.Russia



t.me/kurilka_ib