

Что такое персональные данные?

Персональные данные – это любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных). То есть практически любая информация, которую пользователь указывает на сайте при регистрации или заполнении формы, попадает под действие ФЗ № 152.

Помимо информации, которую пользователь сам указывает на сайте, Роскомнадзор и суды стали относить к персональным данным также данные о поведении пользователя на сайте, cookie, сведения о его геопозиции и IP-адрес. Результатом таких изменений стала нашумевшая в ноябре 2016 года [блокировка в России](#) рекрутингового сервиса LinkedIn.

То есть, если на вашем сайте в форме обратной связи есть поле «Имя» или «Представьтесь», то вместе с автоматически передаваемыми cookie и другими метаданными, это будет являться персональными данными, а вы – оператором персональных данных.

Хотите вы этого или нет, но если на вашем сайте накапливаются, хранятся или каким-то образом используются в работе персональные данные, то, с точки зрения закона, вы признаетесь оператором персональных данных и обязаны обрабатывать их в соответствии с ФЗ № 152 «О персональных данных».

Ужесточение законодательства по персональным данным

Как мы уже писали выше, с 1 июля 2017 года вступят [поправки](#), которые ужесточат процедуры накопления, обработки и хранения персональных данных, а также увеличат штрафы. На сколько именно и за какие правонарушения – рассмотрим в таблице.

Номер статьи и текст	Сумма штрафа	В каких случаях накладывается штраф
ч.1 ст.13.11. Обработка персональных данных в случаях, не предусмотренных законодательством Российской Федерации в области персональных данных, либо обработка персональных данных, несовместимая с целями сбора персональных данных, если эти действия не содержат уголовно-наказуемого деяния	От 30 000 рублей до 50 000 рублей на юридических лиц	1. Когда через сайт собираются сканы паспортов и иных документов. Сканы документов являются избыточной информацией. 2. Обработка не в тех целях, когда это требуется (например, взяли для исполнения договора, но попутно рассылает email-рассылки)
ч.2 ст.13.11. Обработка персональных	От 15 000 рублей	1. Сбор, хранение и обработка

данных без согласия в письменной форме субъекта персональных данных на обработку его персональных данных в случаях, когда такое согласие должно быть получено в соответствии с законодательством Российской Федерации в области персональных данных, если эти действия не содержат уголовно наказуемого деяния, либо обработка персональных данных с нарушением установленных законодательством Российской Федерации в области персональных данных требований к составу сведений, включаемых в согласие в письменной форме субъекта персональных данных на обработку его персональных данных	до 75 000 рублей на юридических лиц	специальных персональных данных (сведения о здоровье, о вероисповедании, политических взглядах и т.д.) на сайте без явного согласия на обработку таких данных. 2. Проведение онлайн-скоринга данных пользователя (включая IP, cookie и сведения из аккаунтов в соц.сетях) без явного согласия на обработку персональных данных в целях скоринга. 3. Отсутствие в согласии или оферте списка третьих лиц, кому могут передаваться персональные данные. 4. Неисполнение требований к форме согласия на обработку персональных данных, описанных в ч.4 ст.9 152-ФЗ.
ч.3 ст.13.11. Невыполнение оператором предусмотренной законодательством Российской Федерации в области персональных данных обязанности по опубликованию или обеспечению иным образом неограниченного доступа к документу, определяющему политику оператора в отношении обработки персональных данных, или сведениям о реализуемых требованиях к защите персональных данных	От 15 000 рублей до 30 000 рублей на юридических лиц	1. Отсутствие на сайте общедоступной ссылки на Политику организации в отношении обработки персональных данных.
ч.4 ст.13.11. Невыполнение оператором предусмотренной законодательством Российской Федерации в области персональных данных обязанности по предоставлению субъекту персональных данных информации, касающейся обработки его персональных данных	От 20 000 рублей до 40 000 рублей на юридических лиц	1. Игнорирование запросов физических лиц по поводу обработки и защиты их персональных данных. 2. Ответ на запрос в сроки, превышающие установленные законом. 3. Предоставление ложной информации.
ч.5 ст.13.11. Невыполнение оператором в сроки, установленные законодательством Российской Федерации в области персональных данных, требования субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных об уточнении персональных данных, их блокировании или уничтожении в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки	От 25 000 рублей до 45 000 рублей на юридических лиц	1. Игнорирование запросов физических лиц и Роскомнадзора по поводу прекращения обработки персональных данных и их уничтожении 2. Нарушение сроков предоставления ответов на поступившие запросы
ч.6 ст.13.11. Невыполнение оператором при обработке персональных данных без использования средств автоматизации обязанности по соблюдению условий,	От 25 000 рублей до 50 000 рублей на юридических лиц	1. Отсутствие списка лиц, допущенных к обработке персональных данных

обеспечивающих в соответствии с законодательством Российской Федерации в области персональных данных сохранность персональных данных при хранении материальных носителей персональных данных и исключающих несанкционированный к ним доступ, если это повлекло неправомерный или случайный доступ к персональным данным, их уничтожение, изменение, блокирование, копирование, предоставление, распространение либо иные неправомерные действия в отношении персональных данных, при отсутствии признаков уголовно наказуемого деяния		2. Отсутствие раздельного хранения данных
--	--	--

С 1 июля 2017 г. возбуждают дела об административных правонарушениях органы Роскомнадзора, а не прокуратура.. Уже сейчас понятно, что данные дела будут возбуждаться проще и быстрее, так как это будет делать сам орган, выявивший правонарушение.

В настоящее время за нарушение закона №152 ФЗ «О защите персональных данных» (сколько бы таких нарушений за 1 раз не было выявлено) можно привлечь только 1 раз. Начиная с 1 июля 2017 г. Роскомнадзор за один «визит» может составить сколько угодно протоколов об административном правонарушении по каждому нарушению.

Расположение хостинга сайта

В соответствии с ч. 5 ст. 18 ФЗ № 152, все интернет-ресурсы, на которых хранятся и обрабатываются персональные данные, должны быть расположены на территории Российской Федерации. С учётом того, что контролирующие органы считают персональными данными также и данные о поведении пользователя на сайте, то это касается практически любого интернет-ресурса. За нарушение этого требования Роскомнадзор их блокирует.

Под расположением хостинга подразумевается физическое местонахождение ЦОДа – Центр обработки данных, на котором размещен ваш сайт. То есть, если хостинг-провайдер зарегистрирован в России, а его ЦОДы расположены, к примеру, в Эстонии, вы нарушаете закон и попадаете под блокировку сайта.

Что нужно сделать на сайте, чтобы избежать штрафов

Мы составили список работ, которые стоит сделать на своём сайте прямо сейчас. Это тот необходимый минимум, который позволит вам избежать проблем в случае проверок Роскомнадзора.

1. Добавить текст согласия на обработку персональных данных

Под каждой формой ввода данных на сайте (регистрация, заявки на услугу, обратный звонок) разместить текст «Нажимая на кнопку «Название кнопки», я даю согласие на обработку персональных данных», где текст «согласие на обработку персональных данных» является ссылкой на документ. Примеры документов вы можете посмотреть на федеральных сайтах, например, ozon.ru и tinkoff.ru.

Вместо согласия можно использовать единую публичную оферту, но в ней будет нужно прописать, в каких целях, какие данные обрабатываются, то есть указать всё, [согласно ч.4 ст.9 152-ФЗ](#). В этом случае обязательно хранить логи, чтобы, в случае чего, доказать Роскомнадзору, что тот или иной пользователь действительно заходил на сайт и оставлял там свои персональные данные.

2. Составить документ "Политика в отношении обработки персональных данных"

Этот документ нужно разместить на сайте в свободном доступе. В данном документе должны быть описаны процедуры сбора, обработки и хранения персональных данных пользователей сайта. Хорошо проработанный документ о политике в отношении обработки персональных данных есть на ikea.com, bmw.ru. При этом с данным документом регистрирующийся не должен соглашаться при заполнении формы.

3. Узнать, где находится хостинг сайта

Узнать у хостинг-провайдера или с помощью общедоступных сервисов, где физически находится ЦОД, в котором расположен ваш сайт и, в случае, если он расположен не на территории РФ, перенести сайт на другой хостинг. Сделать это вы можете, отправив запрос в техническую поддержку сайта.

4. Указать email для обращений пользователей по персональным данным

Укажите email, куда физическое лицо может обратиться за тем, чтобы его персональные данные были удалены, заблокированы и вообще, куда

он может задать вопрос по персональным данным. Email можно указать в документах, описанных выше.

Важно, чтобы указанный email был рабочим, информация на нем регулярно проверялась, чтобы не пропустить запрос пользователя на удаление персональных данных с сайта.

5. Подать уведомление об обработке персональных данных в Роскомнадзор

Вам или агентству-разработчику сайта необходимо подать уведомление об обработке персональных данных в Роскомнадзор, а в случае подачи Уведомления ранее (до сентября 2015 года) необходимо направить Информационное письмо на внесение изменений с указанием местонахождения базы данных информации, содержащих персональные данные граждан РФ.

6. Заключить соглашение о безопасности персональных данных с разработчиком сайта

В случае если агентство-разработчик сайта имеет доступ к персональным данным из заявок или базы данных сайта (например, сайт находится на технической поддержке), вам необходимо заключить соглашение с агентством об обеспечении безопасности персональных данных. В соглашении должно быть указано, какие персональные данные агентство может обрабатывать, в каких целях и какие действия с ними выполнять. Также там должны быть требования по защите персональных данных.

7. Поставить на сайте дисклеймер

До 1 июля 2017 года поставить на сайте дисклеймер, который будет уведомлять посетителей сайта, что его персональные данные обрабатываются на сайте в целях его функционирования и, если он не согласен, то должен покинуть сайт. Примеры дисклеймеров вы можете посмотреть на сайтах www.rosbank.ru/ru/, marykay.ru и bmw.ru. В противном случае это будет являться согласием на обработку его персональных данных.