D!AL
Digital Agency

Разъяснение 152-ФЗ «О защите персональных данных»

- 152-ФЗ был принят Государственной Думой 8 июля 2006 года.
- Одобрил его Совет Федерации 14 июля 2006 года.
- Последняя редакция закона произошла 22 февраля текущего года. Действовала она до 1 марта 2017.

D!AL
Digital Agency

Что такое персональные данные?

Любые данные о человеке, по которым его можно опознать. Точного перечисления в законе нет, но, например, если логин пользователя нам ни о чем не говорит, то электронная почта — это уже персональные данные.

Определение из закона 152-ФЗ «О персональных данных»:

Персональные данные — любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

D!AL
Digital Agency

Часто используемые персональные данные

Неважно, используете ли вы эту информацию по отдельности или в сочетании — если вы как-то получаете ее от пользователей, вы — оператор персональных данных.

- Email
- Телефон
- Имя, фамилия, отчество (и по отдельности)
- Адрес
- Дата рождения
- Фотография
- Ссылка на персональный сайт и профиль в соцсетях

Если на вашем сайте есть любая форма сбора данных — обратной связи, подписки на рассылку, регистрации или личный кабинет, это считается обработкой персональных данных.

D!AL
Digital Agency

Про жизнь

!!!

Исходя из позиции судов и Роскомнадзора даже cookie, данные об IP-адресе, местоположении без указания фамилии и имени являются персональными данными. В деле LinkedIn (который заблокировали за использование cookie, сведений о поведении пользователя на странице и сведений о местонахождении) и провайдера Скартел позиция судов и Роскомнадзора подтверждается.

Операторов персональных данных.

Оператор — любая организация, ИП и физическое лицо, которые обрабатывают персональные данные, например, собирает электронные адреса для рассылки.

Определение из закона 152-ФЗ «О персональных данных»:

Оператор персональных данных — государственный орган, муниципальный орган, 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.

D!AL
Digital Agency

Я не обрабатываю персональные данные, а только собираю

Хранение и сбор тоже попадают под определение обработки. Даже если вы собираете данные и через пару минут удаляете, это будет считаться обработкой персональных данных.

Определение из закона 152-ФЗ «О персональных данных»:

Обработка персональных данных — любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

D!AL
Digital Agency

Что делать с сайтом

Вам нужно сделать так, чтобы сайт соответствовал требованиям 152-ФЗ.

Эти требования применимы для всех — физических лиц и компаний.

Убедитесь, что вы соблюдаете следующие условия:

1. Хостинг и база данных с персональными данными должна располагаться на территории России. Об этом прямо говорят данные проверок Роскомнадзора (снова LinkedIn) и закона №242-ФЗ , который обязывает записывать, хранить, обновлять и извлекать персональные данные граждан РФ с использованием баз данных на территории России с 1 сентября 2015 года.

Это касается иностранных компаний с юрлицом в России и без него, а также российских компаний, которые пользуются иностранными хостинг-провайдерами, дата-центрами и облачными платформами. Все осложняется тем, что требования Роскомнадзора до конца не ясны, приходится догадываться самим. Подробнее о локализации данных рассказывается http://blog.b-152.ru/blog/как-хранить-персональные-данные-с-1-сен/

Если вы не понимаете, где хранить данные и что делать, обратитесь с запросом в Роскомнадзор или Минкомсвязи. И возможно у вашего хостинг-провайдера есть готовые решения на такой случай.

2. Под каждой формой сбора данных, включая сбор email, разместить текст «Нажимая на кнопку, вы даете согласие на обработку своих персональных данных». В тексте должна быть ссылка на документ — Пользовательское соглашение, договор или согласие на обработку персональных данных. Текст самого документа можно разместить на отдельной странице.

Какая информация должна быть в соглашении об обработке персональных данных

Согласно ч.4 ст. 9 закона 152-ФЗ «О персональных данных» в соглашении обязательно должна быть следующая информация:

- наименование или фамилия, имя, отчество и адрес оператора, получающего согласие субъекта персональных данных;
- цель обработки персональных данных;
- перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;
- наименование или фамилия, имя, отчество и адрес лица, осуществляющего обработкуперсональных данных по поручению оператора, если обработка будет поручена такому лицу;
- перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;
- срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;

D!AL Digital Agency

Также нужно указать информацию о том, как физическое лицо может отозвать свое согласие на обработку персональных данных (ч.2 ст. 9 152-ФЗ «О персональных данных»).

3. Разместить на сайте в общем доступе (например, в подвале сайта) ссылку на документ — политику организации в отношении обработки персональных данных на сайте.

4. Показывать всем новым пользователям сайта предупреждение с текстом о том, что вы собираете метаданные пользователя (cookie, данные об IP-адресе и местоположении) для функционирования сайта и, если он не хочет, чтобы эти его данные обрабатывались, то должен покинуть сайт.

D!AL
Digital Agency

Что нужно еще сделать компаниям кроме сайта.

1. Согласно закону РФ, руководитель компании должен утвердить порядок использования личных сведений. Необходимые нормы указываются в локальном документе организации о защите данных. Они должны соответствовать требованиям правовых актов РФ и 152-ФЗ.

Список необходимых документов, которых прошел огонь , воду и проверки Роскомнадзора:

1.Приказ о назначении комиссии по приведению в соответствие с требованиями законодательства в области персональных данных

2. Положение о комиссии по приведению в соответствие с требованиями законодательства в области персональных данных

3. План мероприятий по приведению в соответствие с требованиями законодательства в области персональных данных

4. Перечень должностей и третьих лиц, допущенных к обработке персональных данных

5. Форма Обязательства о неразглашении персональных данных

6. Форма Соглашения об обеспечении безопасности персональных данных, переданных на обработку

7. Перечень обрабатываемых персональных данных

8. Форма Согласия на обработку персональных данных

9. Перечень помещений для обработки персональных данных

10. Перечень информационных систем персональных данных

D!AL
Digital Agency

11. Перечень применяемых средств защиты информации
12. Технический паспорт информационных систем персональных данных
13. Приказ о назначении лиц, ответственных за обработку и защиту персональных данных
14. Инструкция администратора информационной безопасности
15. Инструкция ответственного за обработку персональных данных
16. Положение по обработке персональных данных (внутренний документ)
17. Политика компании в отношении обработки персональных данных (для публичного доступа)
18. Положение об обеспечении безопасности персональных данных
19. Уведомление об обработке персональных данных
20. Регламент по определению уровней защищенности персональных данных в информационных системах .
21. Модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных .
22. Протокол определения ущерба.
23. Акты определения уровней защищенности персональных данных.
24. Техническое задание на систему защиты персональных данных .
25. Приказ об утверждении Инструкции пользователя информационных систем персональных данных .
26. Инструкция пользователя информационных систем персональных данных .
27. Регламент по учёту, хранению и уничтожению носителей персональных данных .
28. Регламент по допуску сотрудников и третьих лиц к обработке персональных данных .
29. Регламент по реагированию на запросы субъектов персональных данных .
30. Регламент по взаимодействию с органами государственной власти в области персональных данных 31. Регламент по резервному копированию персональных данных .
32. Регламент по проведению контрольных мероприятий и реагированию на инциденты информационной безопасности.
33. Регламент по обезличиванию персональных данных.

2. Подать уведомление, чтобы внести организацию в реестр операторов персональных данных Роскомнадзора.

Подать уведомление, чтобы внести организацию в реестр операторов персональных данных Роскомнадзора — можно сделать через сайт

http://pd.rkn.gov.ru/operators-registry/operators-list/)/

Уведомление можно не подавать, если вы:

- обрабатываете только данные работников и только для исполнения требований трудового законодательства (без передачи данных в банки, например, оформления зарплатного проекта)
- обрабатываете данные, заключая договор с каждым клиентом и работником, и не передаете данные третьим лицам
- обрабатываете персональные данные только на бумажных носителях.

Другие исключения, когда уведомление в Роскомнадзор можно не подавать, содержатся во втором пункте статьи 22 закона 152-ФЗ.

D!AL
Digital Agency

3.Правильно отрегулировать взаимодействие с физическими лицами, государственными органами и контрагентами. Это значит, вам нужно:

- Подписать с сотрудниками обязательства о неразглашении персональных данных, согласие на обработку персональных данных и под роспись ознакомить их с внутренними документами по персональным данным.

- Со всеми другими физическими лицами подписывать согласие на обработку персональных данных или добавлять пункты об обработке персональных данных в договоры, которые вы заключаете.

- Заключать поручения на обработку персональных данных, если вы передаете кому-то данные физических лиц (например, рекламным агентствам).
- Отвечать на запросы физических лиц по поводу обработки их персональных данных — не игнорировать, как часто делают.

D!AL
Digital Agency

4. Защитить персональные данные техническими и организационными мерами — антивирусными системами, средствами межсетевого экранирования, разграничить права доступа. Все это прописано в приказе ФСТЭК № 21.

В зависимости от требований проверять компанию могут разные инстанции:

Роскомнадзор, ФСТЭК и ФСБ России.

Самые редкие случаи проверки для частных организаций — проверка технической защиты персональных данных, это делает ФСБ в малом количестве.

D!AL
Digital Agency

Какие штрафы ждут за невыполнение закона.

Если раньше сумма штрафов для юридических лиц не превышала 10 000 рублей, то с 1 июля она спокойно может доходить до 300 000 рублей. Если нарушений несколько, штрафов тоже будет несколько.

Например, если вам напишет пользователь и попросит уточнить или удалить его персональные данные с вашего сайта, а вы не предоставите эту информацию, то штраф для физических лиц будет до 2000 рублей, для ИП — до 20 000 рублей, для компаний — до 45 000 рублей.

Все штрафы можно посмотреть в поправках к закону https://rg.ru/2017/02/10/administrpravo-dok.html.

Как правило, вначале Роскомнадзор присылает «письмо счастья», в котором указывает выявленные нарушения на сайте, связанные с неправомерной обработкой персональных данных.

Хотя в случае с астраханскими сайтами http://astravolga.ru/v-astraxani-nachaki-shtrafovat-organizacii-u-kotorih-est-sobstvenniy-sait/ , которых оштрафовали за форму обратной связи на сайте, проверку просто начали по алфавиту.

D!AL
Digital Agency