



Политика обработки персональных данных: как правильно составить и где разместить

 Время на чтение: 13 минут

По статистике Роскомнадзора, самое распространённое нарушение среди бизнеса — отсутствие Политики обработки персональных данных на сайте. По правилам каждый, кто запрашивает личную информацию у пользователей, обязан разработать локальный нормативный акт по обработке персональных данных и разместить его в открытом доступе. Но многие забывают или не знают об этой обязанности, что приводит к штрафам до 60 000 рублей. Разбираемся, кому нужна Политика обработки персональных данных, как ее создать и опубликовать. А также рассказываем, какие еще документы стоит разместить на сайте или просто иметь готовыми на рабочем столе.

→ Основные понятия

→ Законодательные требования по персональным данным

к коммерческим сайтам

→ Как составить Политику обработки персональных данных

→ Место Политики на сайте

→ Ответственность за нарушения в Политике

→ Рекомендации по работе с Политикой персональных данных сайта

→ Дополнительно. Другие правовые документы, которые регулируют работу с персональными данными

Основные понятия

Персональные данные (персданные) — это информация, которая может быть использована для того, чтобы идентифицировать конкретного человека. Обычно к персональным данным относят:

- Ф. И. О.;
- ИНН/СНИЛС;
- номер телефона;
- адрес прописки и места жительства;
- дата и место рождения.

К персданным относят и другую информацию. Например, если онлайн-магазин предлагает посетителям зарегистрироваться на своём сайте по номеру телефона или ФИО, логин или ник пользователя тоже будут считаться персональными данными.

Обработка персональных данных — это любые действия с личными данными пользователей: сбор, хранение, использование для собственного бизнеса или передача пользовательских данных другим лицам, удаление. Если вы запросили телефон или Ф. И. О. пользователя для регистрации, это тоже считается обработкой персональных данных.

Операторы персональных данных — все, кто обрабатывают персональные данные. Это касается любых данных:

- о клиентах;
- о работниках;
- об исполнителях по гражданско-правовым договорам.

Вы являетесь оператором персональных данных, если:

1. Нанимаете работников и запрашиваете у них личную информацию (Ф. И. О., семейное положение, сведения об образовании)
2. Ведёте клиентскую базу, выдаёте покупателям бонусные карты, регистрируете пользователей на сайте.

Важно! Операторами персональных данных могут быть как организации, так и предприниматели. Организационно-правовая форма бизнеса никак не влияет на обязанности операторов персданных.

Субъект персональных данных — это физлицо, сведения о котором обрабатывают операторы. Это может быть ваш работник, клиент, посетитель сайта. Каждый из них должен дать официальное (в письменном или электронном виде) согласие на обработку своих данных.

Способы обработки персональных данных:

1. **С использованием средств автоматизации.** Любая автоматическая обработка данных: через формы обратной связи на сайте, CRM-системы, информационные базы данных. Обратите внимание, что оператор обязан использовать для обработки только российские базы данных, в том числе, если собирает информацию через свой сайт. Например, Postgre, Digital Q.DataBase, Ред База Данных.
2. **Без использования средств автоматизации.** Обработка данных вручную, без помощи техники. К примеру, когда клиент заполняет бумажную анкету, а продавец собирает данные в специальную папку и также хранит всё на бумаге. Или же посетитель сообщает свои Ф. И. О. и номер телефона

Обязанности любого оператора персональных данных:

1. **Определить состав персданных.** То есть объем личной информации, который вам нужно собрать (например, Ф. И. О. и номера телефонов клиентов).
- Совет.** Старайтесь минимизировать набор обрабатываемых данных — это упростит вам защиту личной информации клиентов.
2. **Определить цель обработки.** К примеру, для регистрации на сайте или ведения клиентской базы.
3. **Разработать локальные нормативные акты по персданным.** К обязательным относятся: Политика обработки персональных данных (она же Политика конфиденциальности) и сведения о мерах защиты полученной информации, приказ о назначении ответственного за работу с данными.
4. **Опубликовать Политику по персданным** в открытом доступе. Политика должна быть опубликована на официальном сайте компании. Остальные документы публиковать не обязательно, но оператор должен иметь их на случай проверки.
5. **Уведомить Роскомнадзор об обработке персональных данных.** Уведомление нужно отправить до начала обработки по унифицированной [форме](#). После этого РКН внесет вас в [реестр операторов](#) персданных. Если планируете обрабатывать данные только вручную, без средств автоматизации, уведомлять Роскомнадзор не надо.
6. **Получить согласие на обработку персональных данных.** Это обязательное требование. Если хотите использовать личную информацию о клиентах, сотрудниках или других лицах, нужно получить их официальное согласие. Согласие на обработку персданных должно быть конкретным, предметным, информированным и однозначным. Письменное согласие пользователей получать не надо, достаточно разместить на сайте форму с возможностью заполнения чек-бокса.
7. **Обрабатывать и хранить персональные данные в соответствии с законом.** Федеральный закон № 152-ФЗ от 27.07.2006 строго закрепляет порядок работы с личными данными. Оператор должен обеспечить безопасность информации при ее использовании и удалить/уничтожить данные после окончания обработки. Безопасность электронных данных обеспечивают за счет технических мер, используя специальные сервисы и ПО по защите от внешних цифровых угроз — например, Solar Aura или «152 онлайн». Также нужно зарегистрироваться в [РосСОПКЕ](#) — системе обнаружения, предупреждения и ликвидации последствий кибератак. Через нее бизнес сообщает об утечках данных и взломах сайтов.

Законодательные требования по персональным данным к коммерческим сайтам

Если обрабатываете персональные данные посетителей сайта, вы автоматически становитесь оператором ([п. 2 ст. 3 152-ФЗ](#)). В таком случае владельцу коммерческого сайта нужно:

1. Разработать и опубликовать Политику в отношении обработки и Сведения о реализуемых требованиях к защите персональных данных.
2. Обеспечить неограниченный доступ к этой информации.
3. Получать согласие на обработку персональных данных.

Далее объясняем, как малому бизнесу правильно соблюдать каждый пункт.

Как составить Политику обработки персональных данных

Роскомнадзор подготовил [рекомендации](#) по разработке Политики персональных данных. В локальном акте нужно указать ([п. 2 ч. 1 ст. 18.1 152-ФЗ](#)):

- информацию об операторе;
- общие положения;
- цели и правовые основания обработки;
- категории и перечень обрабатываемых данных;
- категории субъектов персданных;
- способы и сроки обработки и хранения;
- порядок уничтожения;
- меры, которые принимает оператор, чтобы выполнить обязанности по 152-ФЗ;
- способы связи с оператором.

Важно! Дословно копировать и размещать на своем сайте Политику другого оператора нельзя. Роскомнадзор может признать такую обработку персданных нецелевой и оштрафовать оператора по статье [13.11 КоАП РФ](#). Кроме того, имя оператора персданных, указанное в Политике, должно совпадать с именем администратора доменного имени.

Информация об операторе. Укажите полное название, юридический и фактический адрес, а также контакты владельца сайта.

Общие положения. Опишите назначение вашей Политики. К примеру, сбор и обработка персональных данных в рамках продажи товаров, работ, услуг. Также приведите базовую терминологию — укажите, что такое (в конкретно вашем случае):

- обработка данных;
- оператор;
- субъект;
- конфиденциальность данных.

Обязательно укажите, что Политика конфиденциальности применяется только для конкретного сайта и не распространяется на другие онлайн-ресурсы.

- законными;
- заранее определёнными;
- конкретными.

Для коммерческого сайта целью может быть сбор данных о пользователях сайта для формирования клиентской базы или рекламной email-рассылки.

Обработка персданных должна быть целевой. Поэтому оператор обязан строго следить за содержанием и объёмом данных и их соответствию целям обработки. Например, если на сайте салона красоты запрашивают информацию об имущественном положении или образовании клиентов, это избыточные данные, которые нельзя обрабатывать

Категории субъектов персональных данных. Нужно перечислить все категории физлиц, о которых вы собираете данные. Это могут быть:

- клиенты и контрагенты — физлица, пользователи/посетители сайта;
- представители/работники клиентов и контрагентов — юрлица.

Оператор должен перечислить в Политике объём обрабатываемых данных по каждой из категорий субъектов и по каждой цели обработки. К примеру, по клиентам-физлицам для ведения клиентской базы данных: Ф.И.О., дата рождения, адрес. А по контрагентам-юрлицам для учёта заказов: ИНН, КПП, юрадрес, организационно-правовая форма, налоговый режим.

Порядок и условия обработки персональных данных. В этом разделе нужно подробно описать:

- 1. Порядок получения персональных данных.** Укажите, требуется ли согласие пользователей на обработку, и как вы будете его запрашивать.
- 2. Порядок обработки персональных данных.** Нужно перечислить все действия, которые вы планируете проводить с персданными: сбор, обработка, хранение, передача, удаление и проч. Если вы будете передавать данные третьим лицам, укажите основания для такой передачи. К примеру, по запросу ведомственных органов или в целях безопасности субъекта персданных.
- 3. Порядок хранения и защиты персональных данных.** Опишите, как будете сохранять конфиденциальность и защищать полученную информацию. Какие организационные, технические меры и ИТ-решения будете использовать для защиты от нераспространения и случайного доступа. Что будете делать при утрате или разглашении пользовательских данных.

Отдельно опишите процедуру завершения обработки. В Политике нужно закрепить, что обработка заканчивается в момент достижения цели. После этого оператор должен удалить данные. Определите порядок актуализации, исправления, удаления и уничтожения персданных, а также ответов на запросы субъектов на доступ к личной информации. К примеру, если цель — регулярная email-рассылка, укажите, сколько лет планируете её проводить. Иначе придётся удалять все полученные сведения после первой же рассылки.

Обязательства сторон. Укажите, что посетитель вправе предоставить личную информацию для сайта с его согласия, а оператор обязан организовать целевую обработку и обеспечить конфиденциальность полученных данных. Также в обязанности оператора входит блокировка данных по запросу пользователя.

Способы связи с оператором. Укажите все доступные контакты для связи с оператором: адрес электронной почты, почтовый адрес, многоканальный телефон и рабочий номер ответственного за обработку персданных. Также можно подготовить и разместить на сайте форму запроса жалобы оператору.

Место Политики на сайте

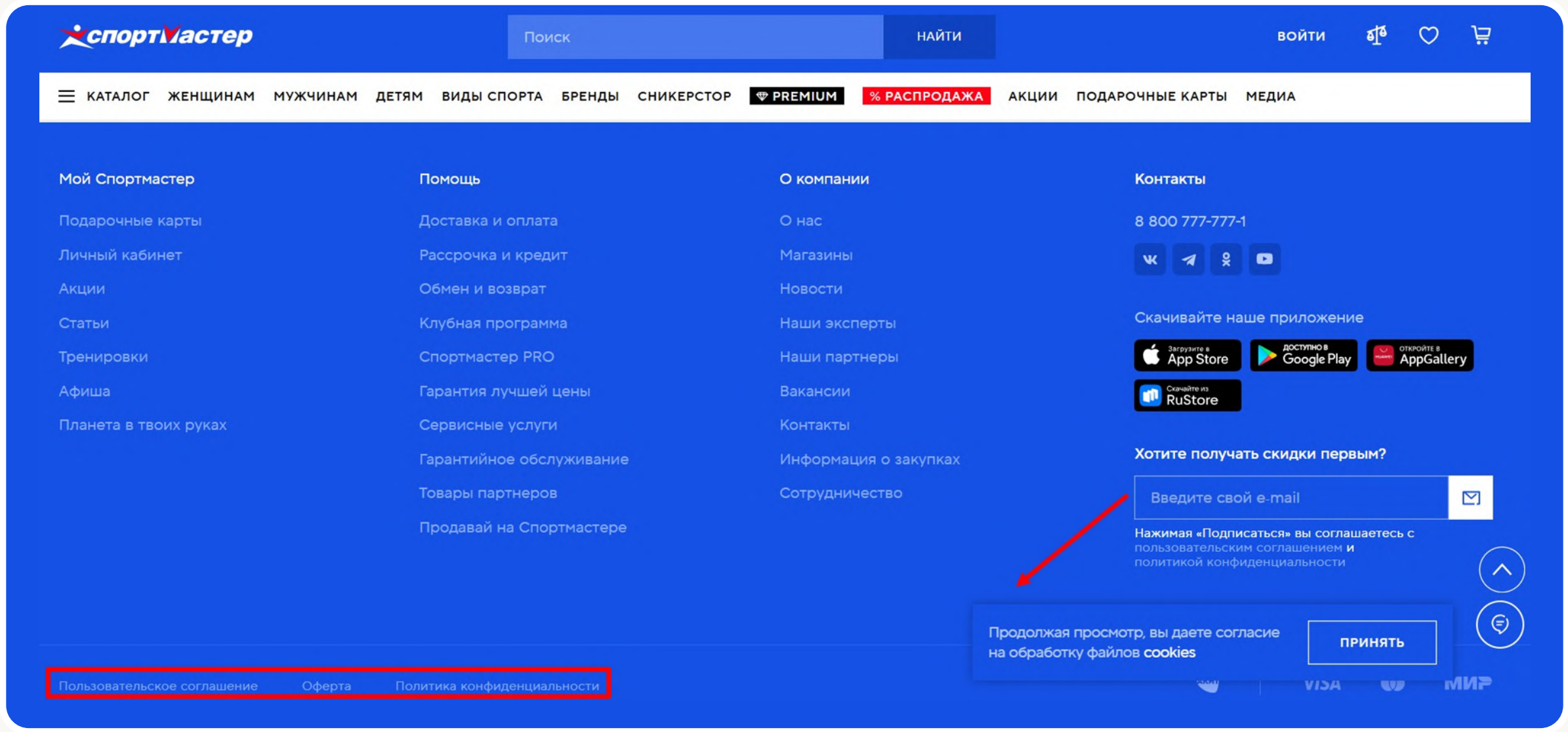
Разместите Политику на главной странице в нижнем блоке (футере или подвале) сайта — так, чтобы пользователь сразу её нашёл. Расположение документа Политики должно быть интуитивно понятным для каждого посетителя. Кроме того, нужно поставить ссылку на Политику на всех страницах сайта — если там собираются персональные данные. У каждого посетителя должен быть неограниченный доступ к Политике обработки персданных и к сведениям о реализуемых требованиях по их защите.

Размещение Политики конфиденциальности не означает автоматическое согласие пользователей на обработку персданных. Оператор обязан предоставить посетителям возможность выразить согласие на обработку непосредственно на сайте. Например, разместить на странице чек-бокс, в котором пользователь поставит галочку для подтверждения согласия.

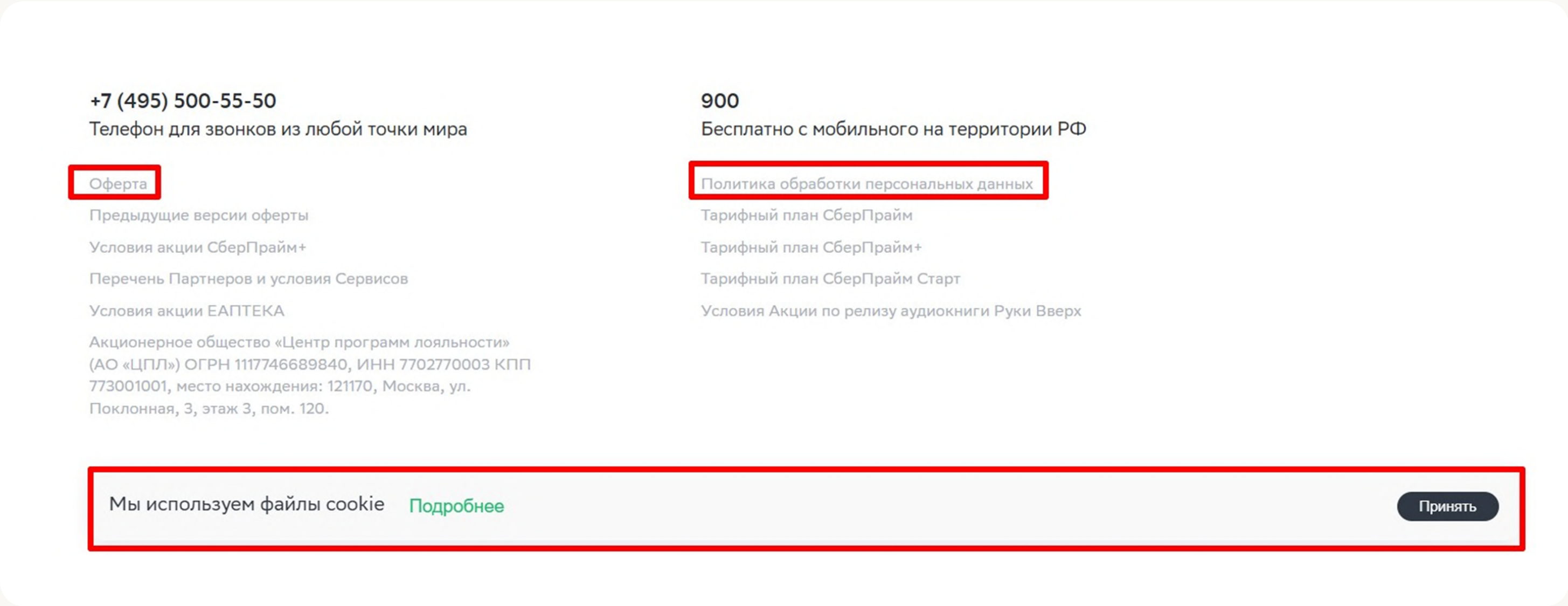
Коммерческие сайты собирают cookie-файлы посетителей. Поскольку в cookie хранятся не только личные данные для авторизации (имя, email, логин, пароль), но и настройки рекламных и потребительских предпочтений, это персданные. И посетитель должен дать согласие на их использование.

Чаще всего это делают в виде всплывающего баннера, который пользователь замечает сразу же при посещении сайта и сможет принять или отклонить сбор cookie-файлов. Обратите внимание: cookie-баннер — это обязательный элемент сайта. А вот публиковать отдельную Политику использования файлов cookie на сайте не обязательно. Достаточно сделать раздел в Политике конфиденциальности и указать, для каких целей собираются cookie-файлы, и как человек может прекратить их обработку в браузере.

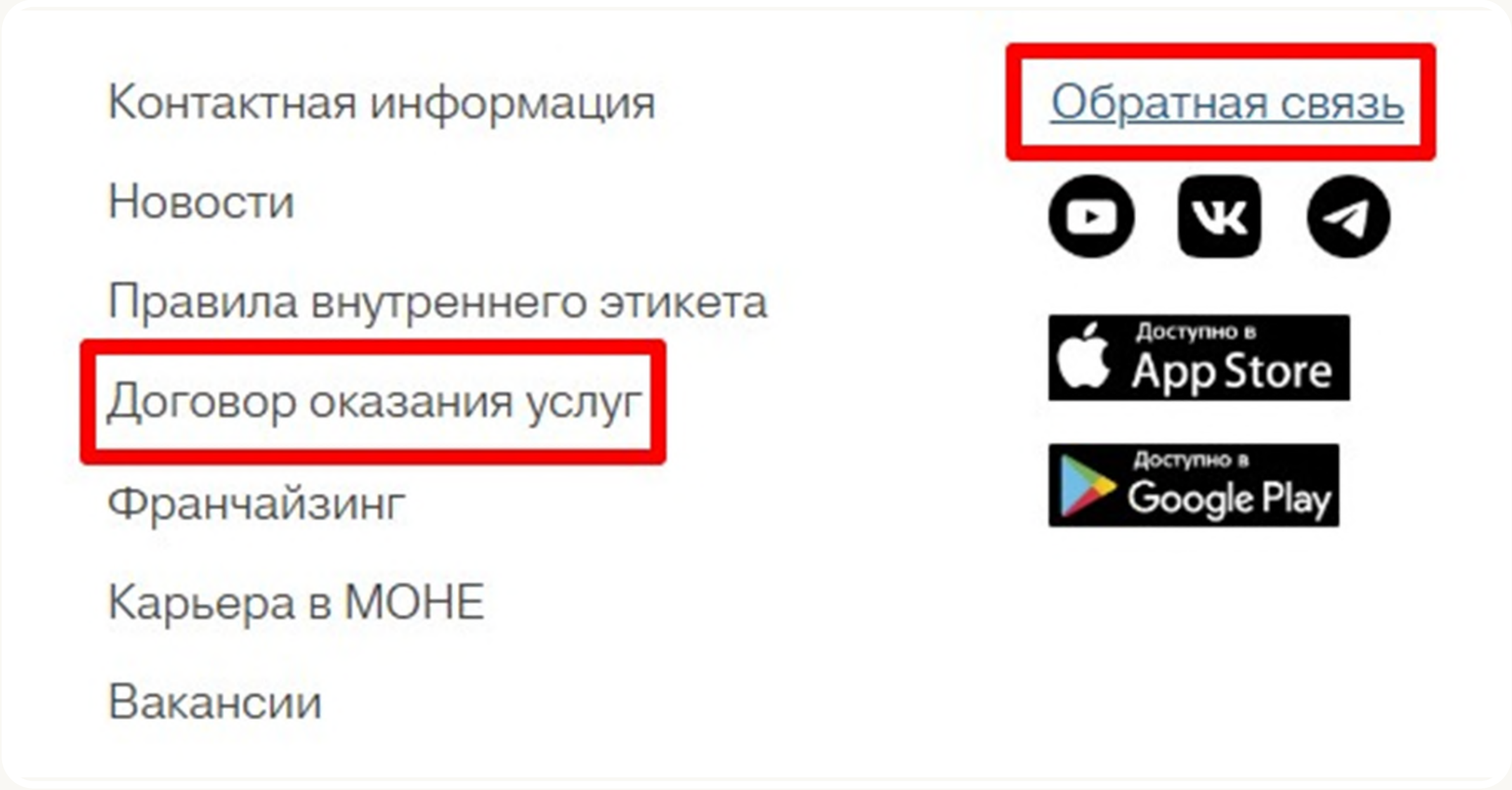
Вот несколько примеров размещения Политики конфиденциальности и согласия на сбор cookie-файлов на сайте:



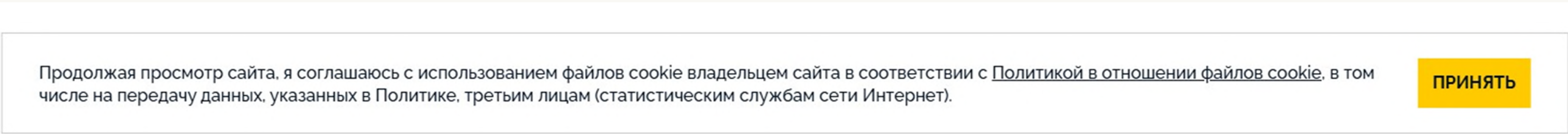
На главной странице сайта спортивного магазина можно найти и оферту, и политику конфиденциальности, и согласие на обработку cookie



На главной странице банка также собрали для пользователей всю информацию об обработке персданных



На сайте салона красоты есть форма обратной связи. Здесь нет уведомления ни о файлах cookie, ни о политике конфиденциальности, но есть публичная оферта



Пример cookie-файлов в онлайн-магазине косметики

Важно! Если вы также ведете бизнес офлайн, то распечатайте утвержденную Политику обработки персональных данных и разместите на информационном стенде вашей точки продаж

Ответственность за нарушения в Политике

Роскомнадзор проверяет как наличие локальных актов операторов в отношении персональных данных, так и их соблюдение. Вы обязаны предоставить по запросу РКН все локальные нормативные акты (ЛНА) — Политику, приказы, положения, требования к защите и другие документы ([ч. 4 ст. 18.1 152-ФЗ](#)).

На практике РКН штрафует бизнес, если:

- Политика отсутствует или размещена не на всех страницах сайта, на которых собирают персданные;
- размещена ссылка на другой документ, который не имеет отношения к Политике;
- размещена чужая Политика, документ с упоминанием другой организации или же одна Политика на несколько компаний;
- в Политике отсутствуют обязательные сведения из [п. 2 ч. 1 ст. 18.1 152-ФЗ](#) или указаны сведения, которые не соответствуют фактической деятельности компании или ИП;
- Политика полностью дублирует положения [152-ФЗ](#).

За нарушения, связанные с Политикой персданных, оштрафуют по [ч. 3 ст. 13.11 КоАП РФ](#). Директор организации заплатит от 6 000 до 12 000 рублей, ИП — от 10 000 до 20 000 рублей, организация — от 30 000 до 60 000 рублей.

Рекомендации по работе с Политикой персональных данных сайта

1. Не устанавливайте pre-checked box, где галочки с согласием на обработку уже проставлены. Такое согласие не считается добровольным. Для каждой страницы или формы нужно сделать индивидуальное окошко.
Если предлагаете ознакомиться с пользовательским соглашением, дать согласие на обработку и изучить политику конфиденциальности, сделайте три отдельных чек-бокса.
2. Используйте для обработки только российские серверы и базы данных.
И обязательно проверьте, не заблокирован ли ресурс на территории РФ.
Иначе вам грозит штраф до 6 млн рублей ([ч. 8 ст. 13.11 КоАП РФ](#)).
3. Удаляйте данные после достижения цели или истечения срока обработки.
Можно установить автоудаление данных после определённого срока — это снижает риск утечек.
4. Назначьте ответственного за обработку персданных. Многие предприниматели пропускают этот шаг и занимаются обработкой сами, из-за большой нагрузки часто допускают ошибки и платят крупные штрафы.
Ответственным может быть любой ваш сотрудник, который будет работать с полученной информацией. Например, если собираете данные для рекламных рассылок, можно сделать ответственным маркетолога.
А вот внештатника к работе с персданными лучше не привлекать.
С ним придётся подписывать соглашение о неразглашении конфиденциальной информации и постоянно контролировать его работу.
5. Регулярно проводите обучение сотрудников, работающих с персданными.
Так ответственные сотрудники будут проинформированы обо всех законодательных изменениях и смогут применить новые правила в работе.
6. Периодически оценивайте угрозы безопасности информации. Если появился риск утечки, обновите требования к локальной защите данных.
7. Актуализируйте Политику, технические и организационные меры безопасности данных при изменении законодательства. Также актуализация понадобится, если изменились цели обработки данных или технические условия оператора.

Дополнительно.
Другие правовые
документы,
которые
регулируют
работу
с персональными
данными

Политика — это ключевой документ, регламентирующий обработку персданных конкретного оператора, и именно его необходимо публиковать на сайте. Вместе с тем, операторам персданных нужно разработать и утвердить несколько внутренних документов по списку:

- 1. **Положение о персональных данных.** В этом документе описывают все действия оператора, связанные с обработкой персданных — хранение, использование данных и проч. В положении определяются категории и перечень персональных данных, способы, сроки их обработки и хранения — для каждой цели обработки. К примеру, предприниматель отдельно описывает порядок обработки данных сотрудников и клиентов.
- 2. **Приказ о назначении ответственных за обработку персональных данных.** Руководитель назначает ответственного за персданные отдельным распоряжением — этот специалист должен под подпись ознакомиться со своими обязанностями.
- 3. **Другие локальные документы.** Например, журналы учета персональных данных, их выдачи и передачи другим лицам, представителям сторонних организаций и государственным органам. Кроме того, можно разработать собственную форму согласия на обработку персональных данных.

Важно! Политика оператора в отношении обработки персональных данных и положения об обработке персональных данных — это два разных документа. И каждый из них должен обязательно быть у оператора. Вот в чём их основные отличия:

- Политика — это внешний документ для клиентов, контрагентов и других лиц, положение — для внутреннего пользования;
- требования к содержанию Политики о персональных данных регулируются [п. 2 ч. 1 ст. 18.1 152-ФЗ](#), а вот требований для внутреннего положения нет: каждый оператор сам решает, что включить в этот документ. Например, правила обработки данных для ответственных сотрудников;
- Политику утверждает руководитель компании/ИП, положение — руководитель плус профсоюз работников, поскольку оно касается внутренней работы с персданными.

Документы (приказ, положение и др.) должны хранится непосредственно у оператора — их может в любой момент запросить РКН. С ними нужно обязательно ознакомить ответственных работников.

Рекомендации по подготовке документов по персданным можно найти на [сайте Роскомнадзора](#).

- 4. **Договор (оферта), на основании которого оператор собирает персональные данные пользователей.** Это может быть публичный договор, к которому посетитель сайта присоединяется для получения товаров и услуг. Обычно в оферте описывают порядок использования сайта: например, что, прочитав соглашение, посетитель ознакомился и согласился с форматом демонстрации товаров (ценами, условиями продажи).

Когда оферта не применяется, нужно использовать уведомление об обработке персданных, в котором необходимо кратко рассказать посетителям о целях сбора и их правах. Если пользователь согласен, он подтверждает это отметкой в чек-боксе. Важно помнить, что договор оферты не заменяет Политику обработки персданных оператора.

18 Публичная оферта

ПРОДАВЕЦ: ООО «Л'Окситан Рус», ИНН 7707591760 /КПП 770601001 ОГРН 1067746721239 .

ПОКУПАТЕЛЬ: Физическое лицо, осуществившее заказ Товара в Интернет - магазине Продавца [www.loccitane.ru](#). (Далее по тексту – «web-сайт»).

Покупатель настоящим подтверждает, что прочитал, понял и полностью согласен соблюдать настоящую Публичную Оферту. Администрация Интернет-магазина "Л'Окситан" оставляет за собой право изменять и дополнять настоящее соглашение без предварительного и последующего уведомления Покупателей. Все возможные изменения будут отражены в соглашении на данной странице.

Используя web-сайт, Покупатель заявляет, что он обладает необходимым оборудованием и программным обеспечением, позволяющим получить доступ к web-сайту, осуществлять просмотр его страниц (в том числе настоящего раздела), выполнять программные скрипты web-сайта, осуществлять телефонные звонки, прием и передачу смс-сообщений и сообщений электронной почты, а также просмотр контекстной рекламы.

Используя web-сайт Покупатель соглашается с утверждением, что оформление заказа с использованием web-сайта является сложной технической процедурой. Продавец не может гарантировать постоянную доступность web-сайта, отдельных его разделов, а также их стабильную работу на любом оборудовании Покупателя, в том числе работу отдельных программных скриптов, отвечающих за применение промо-кодов, выбор и помещение товара в «корзину», адаптацию web-страницы и отдельных баннеров на ней под конкретный дисплей и т.д.

Используя web-сайт Покупатель обязуется в случае невозможности оформить заказ на web-сайте вследствие любого технического сбоя, оформить желаемый заказ по телефону: 8 800 700 45 11.

Используя web-сайт Покупатель дает согласие на демонстрацию ему рекламных баннеров контекстной рекламы на сайте третьих лиц с использованием технологий «яндекс-директ» и «google ads», при этом Покупатель заявляет, что он ознакомлен и согласен с вышеуказанными технологиями, политикой конфиденциальности и условиями демонстрации рекламы.

Покупатель уведомлен и согласен с утверждением, что формат контекстной рекламы предполагает ограничение на размер рекламного баннера и количества символов на нем, при этом часть информации на баннере может отображаться некорректно в зависимости от типа оборудования Покупателя и сайта демонстрации.

Покупатель согласен с утверждением, что формат демонстрации контекстной рекламы продукции бренда L'Occitane предполагает получение полной информации о рекламируемом товаре на русском языке, а также сведений о Продавце (а равно – Организаторе стимулирующих мероприятий под брендом L'Occitane) путем нажатия на соответствующий рекламный баннер и перехода на сайт <https://www.loccitane.ru/>

Пример публичной оферты в онлайн-магазине косметики

Каждый оператор обязан соблюдать требования по обработке персональных данных, иначе ему грозит юридическая ответственность. Нужно заранее определить цель обработки данных и строго ее придерживаться, при необходимости получать согласие на обработку, уведомлять РКН и принимать меры для защиты данных.