Ракета®

юридический сервис
для бизнеса

Руководство

по сбору и использованию персональных данных клиентов

Содержание

Какие данные считаются персональными

Персональные данные (ПДн) — это любая информация, которая позволяет прямо или косвенно идентифицировать человека.

Что может быть персональными данными:

- Ф.И.О.,
- номер телефона,
- электронная почта,
- адрес места жительства,
- IP-адрес устройства или иные данные,
- ID пользователя,
- файлы cookie,
- данные систем интернет-аналитики.

Обратите внимание!

Не все данные о человеке сами по себе являются персональными. Важно, чтобы сочетание данных позволяло установить личность человека.

Пример № 1:

Просто указание ФИО — это ещё не ПДн, так как совпадений могут быть тысячи. А вот ФИО + адрес — уже персональные данные. Фотография на аватарке в соцсети + имя + фамилия — тоже ПДн.

Пример № 2:

Электронная почта liza2007@mail.ru — не ПДн, так как установить по таким данным личность человека невозможно. Зато адрес roman.petrov080760@raketa.one — ПДн, так как в нем содержатся имя, фамилия, дата, месяц и год рождения человека, название компании, где он работает.

Бизнес как оператор персональных данных

Если компания собирает и обрабатывает ПДн клиентов, то она является оператором персональных данных.

Например:

- когда пользователь сайта регистрируется в личном кабинете,
- когда пользователь заполняет форму сбора контактных данных (оставляет заявку на услугу, подписывается на рассылку, заполняет форму регистрации на сайте)

Признаки оператора персональных данных:

- ☐ Обрабатывает данные — собирает, хранит, систематизирует, обновляет, использует, передает, удаляет и прочее;
- ☐ Определяет цели обработки ПДн;
- ☐ Устанавливает перечень ПДн, необходимых для достижения целей.

Регистрация в качестве оператора ПДн

Оператору ПДн нужно зарегистрироваться в специальном реестре Роскомнадзора. Для этого необходимо заполнить и отправить форму уведомления в бумажном или электронном виде на сайте Роскомнадзора.

Важно!

Уведомление необходимо направить до того как вы начнете собирать и обрабатывать ПДн.

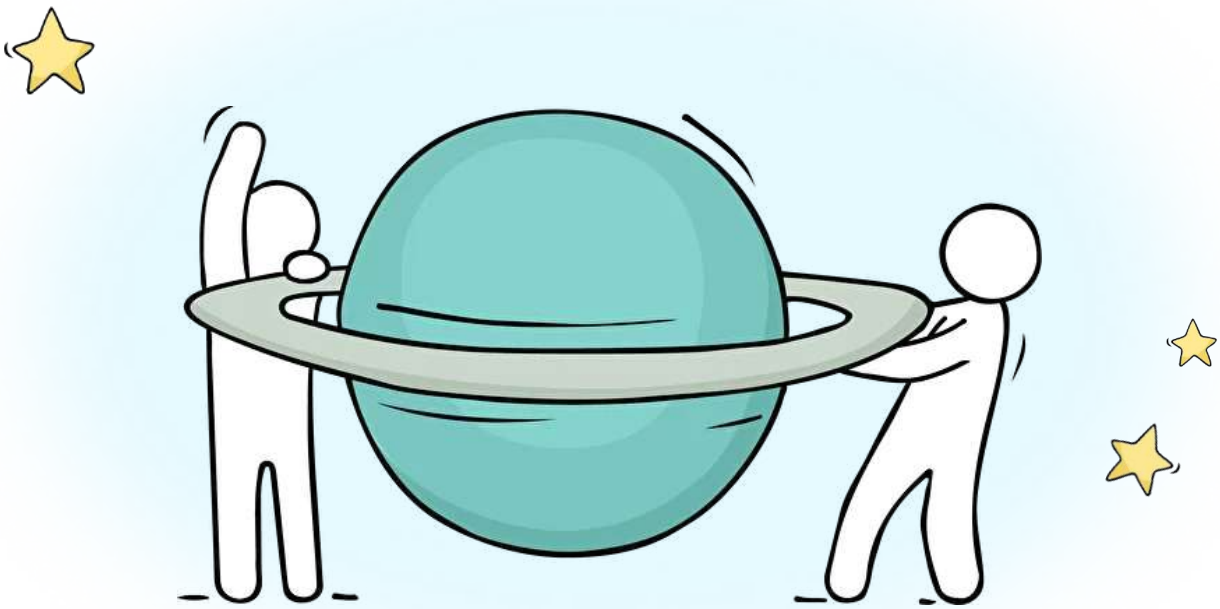
В каких случаях можно не подавать уведомление:

- ☐ Вы обрабатываете только данные сотрудников компании и только для целей исполнения требований трудового законодательства, при этом не передаете данные третьим лицам, например, в банки для оформления зарплатных карт;
- ☐ Вы обрабатываете данные индивидуально с каждым работником или клиентом, заключая договор без передачи данных третьим лицам;

Иные исключения, когда можно не подавать уведомление в Роскомнадзор содержатся в п. 2 ст. 22 152 - ФЗ.

Важно!

Даже если ваша компания не отправит уведомление в Роскомнадзор о регистрации в качестве оператора ПДн, на неё будет распространяться законодательство о персональных данных и обязанности по его соблюдению.



Необходимые документы для работы с персональными данными

Политика обработки персональных данных

Разработайте политику в отношении обработки персональных данных (далее – Политика) с учетом требований закона о персональных данных.

Зачем нужна политика обработки персональных данных?

При передаче вам своих персональных данных, пользователь вправе знать:

- для чего вы их собираете,
- как будет осуществляться обработка данных,
- в течение какого срока данные будут храниться,
- как будет обеспечиваться их безопасность.

Многие бизнесы просто скачивают шаблоны политик из интернета. Однако, это влечет риск того, что этот документ не будет учитывать особенности вашего бизнеса и не будет в полной мере соответствовать требованиям законодательства.

Для составления политики рекомендуется обращаться к юристам, которые помогут учесть все индивидуальные особенности бизнеса и корректно составить политику, чтобы избежать проблем с Роскомнадзором.

Какие сведения должна содержать политика

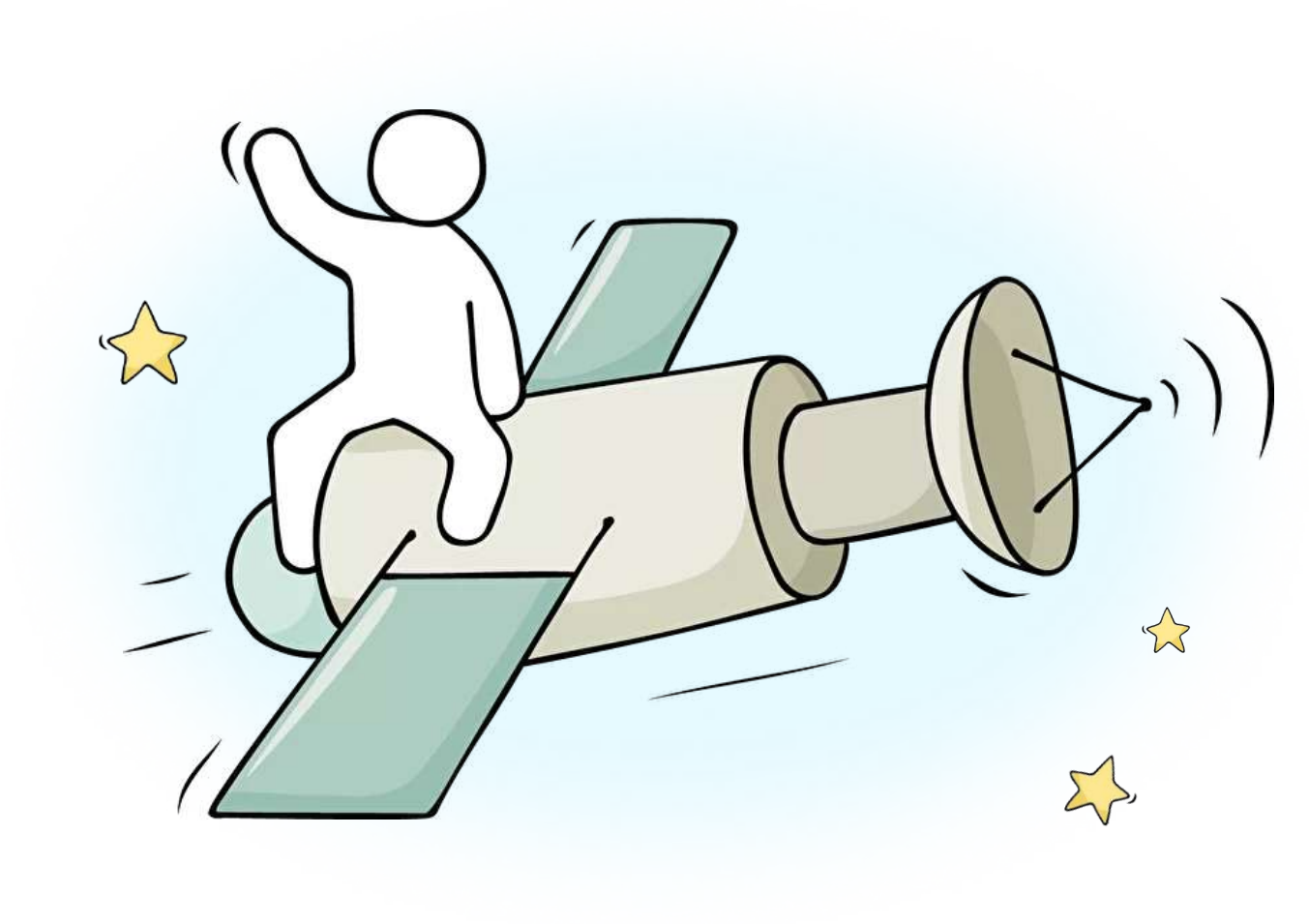
- Определение основных терминов – документ должен быть понятен обычным пользователям.
- Информацию об операторе (наименование компании, ОГРН, ИНН, юридический адрес), а также контакты, куда пользователь сможет обратиться с вопросом или с просьбой прекратить обработку его персональных данных.
- Порядок взаимодействия оператора ПДн и пользователя – сроки реагирования на обращения, адреса, иные контакты.
- Цели сбора, объем и категории собираемых персональных данных.

- Категории субъектов персональных данных – работники, бывшие работники, клиенты и т.п.
- Сведения о том, как обеспечивается безопасность данных
- Иные положения в зависимости от особенностей вашего бизнеса.

Где необходимо разместить политику?

Политика должна быть размещена на сайте компании.

Также будьте готовы предъявить клиенту полный текст политики — в бумажном виде, если вы оказываете услуги или продаете товары оффлайн. Распечатанную политику можно хранить на ресепшен или повесить на информационный стенд.



Согласия на обработку ПДн

Помимо политики обработки персональных данных компания в обязательном порядке должна разработать формы согласий на обработку ПДн (далее — Согласие). Требования к составлению согласия на обработку персональных данных содержатся в законе о персональных данных.

В отличие от политики, где определяются общие правила работы с ПДн, согласие на обработку персональных данных — это конкретный документ, отвечающий на три главных вопроса:

- какие данные вы собираете у данного пользователя?
- для чего вы собираете его данные?
- что вы намерены с ними делать?

Согласия собираются в письменном виде — их нельзя получать в устной форме или по телефону. Согласия собираются через интернет (сайт компании) или с помощью заполнения клиентом бумажных анкет (например в оффлайн магазине). При этом согласие, полученное через форму на сайте считается полученным в письменной форме.

Что должно содержаться в согласии

- ☐ Сведения об операторе (наименование компании, ОГРН, ИНН, юридический адрес)
- ☐ Перечень ПДн и цель их обработки
- ☐ Сроки и способы обработки ПДн

Обратите внимание!

Разместить на сайте политику обработки персональных данных недостаточно. Если вы оператор ПДн, то вы обязаны иметь согласия на обработку данных, в которых указана цель сбора данных и срок их хранения. Составлять универсальные или так называемые «бесшовные» согласия — неверно. Под каждую цель — своё согласие.

Пример:

На сайте компании есть форма подписки на рекламную рассылку. В согласии к этой форме вы должны указать конкретный список ПДн (имя, фамилия, адрес электронной почты) и цель сбора — отправка электронных писем рекламного характера один раз в неделю. Такое согласие уже не подойдёт для формы обратной связи, где клиент вводит другой набор данных, например, Ф. И. О., адрес и телефон, и вы собираете их для другой цели — чтобы ответить на вопросы о доставке или покупке товара.

Важно!

Закон разрешает собирать только те персональные данные, которые нужны, чтобы выполнить цель сбора.

Если клиент заполняет форму для доставки товара на дом, имеет смысл запросить у него Ф. И. О. и адрес доставки, а просить иные сведения, скажем ИНН — уже незаконно.

Что делать, если клиент не хочет подписывать согласие?

Если подобные данные необходимы, вы можете отказаться от предоставления услуги.

Пример:
невозможно оформить билет на самолет без предоставления паспортных данных.

Однако имейте в виду, что для осуществления, например, рекламных рассылок, клиент не обязан подписывать согласие, если не хочет их получать.

Нужно ли собирать согласия в оффлайн?

В ряде случаев сбор персональных данных может осуществляться на бумажных носителях с помощью заполнения анкет, если вы предоставляете услуги или продаёте товары в оффлайн.

Например, оффлайн-магазин может запрашивать согласие клиента, если планирует использовать его данные иным образом, чем для продажи товаров.

При этом продуктовый супермаркет, как правило, не запрашивает персональные данные покупателей. Однако, персональные данные могут запрашиваться для того, чтобы открыть дисконтную карту. В этом случае вы обязаны запросить согласие клиента на сбор ПДн и попросить его заполнить соответствующую анкету.

В бумажные согласия добавьте графы, куда субъект ПДн (или его представитель) должен будет внести данные документа, удостоверяющего личность, адрес и проставить подпись. Галочку в электронном чекбоксе и подпись субъекта ПДн на бумажном носителе можно считать равнозначными.

Можно ли заранее предустанавливать в чекбоксах согласий галочки, подразумевающие согласие клиента на сбор и обработку ПДн?

Это будет считаться нарушением. Галочка в чекбоксе не должна стоять «по умолчанию». Рядом с чекбоксом должны быть кликабельные ссылки на текст согласия и политику, а не общая фраза «я согласен на обработку (неких не конкретных) данных…».

Иными словами, пользователь должен сам принять решение о предоставлении вам своих персональных данных и поставить галочку, ознакомившись предварительно с условиями их сбора и обработки.

При этом лог-файлы на сайте, которые могут быть доказательством того, что пользователь подписал согласие, нужно сохранять.

Может ли субъект отозвать согласие на обработку персональных данных?

Да, такое право у клиента есть. Для этого гражданин должен написать заявление об отзыве согласия с указанием:

- Ф. И. О.;
- контактов (номер телефона, адрес электронной почты или почтовый адрес);
- переченя персональных данных, обработка которых должна быть прекращена.

Оператор персональных данных обязан прекратить распространение ПДн в течение трех рабочих дней с момента получения заявления. В противном случае субъект персональных данных вправе обратиться в суд с этим же требованием (п. 14 ст. 10.1 Закона № 152-ФЗ).

Уведомления об использовании Cookies на сайте

Файлы Cookies также считаются персональными данными.

Поэтому закон обязывает вас 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.

Как правильно хранить персональные данные и обеспечивать их безопасность

1. Базы с персональными данными должны храниться на российских серверах

Хостинг и база данных с персональными данными должна располагаться на территории России. Об этом прямо говорят данные проверок Роскомнадзора и закон № 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.

Если Роскомнадзор обнаружит нарушение, то сайт заблокируют, а вам выпишут большой штраф — до 6 млн рублей для юрлиц или до 200 тысяч рублей для ИП.

Если вам все же необходимо передавать данные за границу или хранить их в иностранных базах данных, первичный сбор и хранение ПДн все равно нужно организовать на российских серверах.

2. Назначьте сотрудника, ответственного за организацию обработки ПДн

Такой человек назначается приказом по организации. По закону это обязательное требование для юрлиц, но если вы ИП — необходимо возложить эту функцию на себя через соответствующий приказ. Ответственный будет иметь доступ к базам ПДн и следить за тем, чтобы они обрабатывались правильно.

3. Укажите в политике и согласиях сведения о передаче ПДн третьим лицам

Если вам необходимо передавать ПДн третьим лицам (например, ваша компания состоит в холдинге и обработку данных осуществляет другая компания холдинга), то это нужно указать в политике и согласии, кому вы будут передавать данные и с какой целью. Неважно, обрабатываете вы ПДн сами или передаёте их ещё кому-то для обработки — ответственность за утечку будете нести вы.

Краткая пошаговая инструкция по работе с персональными данными:

1. В большинстве случае, если вы собираете персональные данные, вам нужно сообщить об этом в Роскомнадзор и зарегистрироваться в специальном реестре операторов ПДн.
2. Разработайте политику обработки персональных данных, необходимые формы согласий на обработку ПДн с учётом требования 152-ФЗ.
3. Проведите аудит вашего сайта. Проверьте, размещена ли там политика, в каждой ли форме сбора данных есть ссылка на согласие, не стоят ли предустановленные галочки в чекбоксах согласий. Если вы собираете данные в оффлайне — разработайте согласия на бумажном носителе и будьте готовы предъявить клиенту политику в распечатанном виде.
4. Проверьте, что у каждой формы сбора ПДн есть конкретная цель, и вы не собираете избыточные данные. Например, для рекламных рассылок вы указываете цель — отправка электронных писем рекламного характера. Для других целей указанное согласие уже не подойдёт.
5. Организуйте правильную работу с документами в отношении ПДн внутри компании: назначьте ответственного сотрудника, который будет следить за безопасностью данных, их учётом и хранением. Не передавайте кому-либо ПДн в том числе вашим партнёрам, если вы не получили об этом отдельное согласие пользователя.
6. Подпишите с сотрудниками обязательства о неразглашении персональных данных, согласие на обработку их персональных данных и под подпись ознакомьте их с внутренними документами и политиками компании по использованию и защите персональных данных.

7. Отвечайте на запросы физических лиц по поводу обработки их персональных данных — не игнорируйте, как часто делают.

В процессе сбора персональных данных есть много тонкостей. Чтобы гарантированно избежать проблем с проверяющими органами, обращайтесь к профессиональным юристам.

Провести аудит и разработать весь комплект документов в отношении персональных данных компании вы можете в рамках стандартной подписки на юридический сервис Ракета.

Спецпредложение для наших подписчиков

30% скидка на 1-й месяц юридического сопровождения бизнеса по подписке.

Чтобы воспользоваться спецпредложением оставьте заявку на сайте и не забудьте сказать консультанту кодовое слово «Деловая среда».