

ООО «Гепард» · GGCO · курьерская служба

ПОЛИТИКА

в отношении обработки персональных данных

со справочными приложениями 1–8

Опубликована: <https://ggco.ru/privacy>

Обязательства Оператора устанавливает только раздел I. Раздел II носит справочный характер.

Содержание

Раздел I. Политика в отношении обработки персональных данных	3
1. Общие положения и сведения об операторе	4
2. Цели, субъекты, данные и правовые основания	4
3. Способы и действия по обработке	5
4. Где хранятся данные	5
5. Передача третьим лицам и трансграничная передача	5
6. Сроки обработки, хранения и уничтожение	6
7. Cookie, технические данные и аналитика	6
8. Права субъекта персональных данных	6
9. Порядок обращения и отзыв согласия	6
10. Меры защиты	7
11. Заключительные положения	7
Раздел II. Справочные приложения	8
Приложение 1. Термины и определения	9
Приложение 2. Принципы обработки персональных данных	24
Приложение 3. Права субъекта персональных данных: подробные разъяснения	32
Приложение 4. Как направить запрос или отзыв согласия	46
Приложение 5. Файлы cookie и похожие технологии: справочник	54
Приложение 6. Безопасность персональных данных: рекомендации пользователям	65
Приложение 7. Вопросы и ответы	78
Приложение 8. Обзор законодательства Российской Федерации о персональных данных	90

Раздел I. Политика в отношении обработки персональных данных

1. Общие положения и сведения об операторе

1.1. Настоящая Политика определяет порядок обработки персональных данных пользователей сайта ggco.ru (а также его зеркала ggco-delivery.ru) и разработана в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

1.2. Оператор: Общество с ограниченной ответственностью «Гепард» (ООО «Гепард»), ИНН 9724007014, КПП 236701001, ОГРН 1207700093325, адрес: 354364, Краснодарский край, г. Сочи, Адлерский р-н, ул. Ленина, д. 219/6Б, помещ. 46; e-mail: info@ggco.ru; телефон: +7 (495) 125-28-91.

1.3. Лицо, ответственное за организацию обработки персональных данных: генеральный директор ООО «Гепард» Горбунов Данил Александрович. Контакт для обращений по вопросам персональных данных: info@ggco.ru; почтовый адрес — адрес Оператора, указанный в п. 1.2.

2. Цели, субъекты, данные и правовые основания

2.1. Анкета кандидата (страница «Работа курьером»)

- Цель: рассмотрение кандидатуры для трудоустройства или заключения иного договора о выполнении работ/оказании услуг, связь с кандидатом по вопросу вакансии, проверка соответствия требованиям вакансии, организация собеседования, оформление и выход на работу.
- Субъекты: кандидаты (соискатели), заполнившие анкету.
- Данные: фамилия, имя, отчество; дата рождения; пол; гражданство; город работы; телефон; e-mail (по желанию); ник в Telegram; вид транспорта (по желанию); комментарий (по желанию); копии главной страницы паспорта, страницы паспорта с регистрацией и СНИЛС и содержащиеся в них сведения; IP-адрес, дата и время отправки, адрес страницы, технические сведения о браузере и устройстве (тип и версия браузера и ОС, модель устройства, параметры экрана, язык, часовой пояс, адрес страницы перехода).
- Правовое основание: согласие субъекта персональных данных (п. 1 ч. 1 ст. 6 Закона № 152-ФЗ), которое даётся отдельно — Согласие на обработку персональных данных. Без согласия анкета не отправляется. Факт согласия фиксируется вместе с анкетой: отметка о согласии, идентификатор редакции текста согласия, дата и время.

Специальные категории персональных данных (сведения о расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, интимной жизни) и биометрические персональные данные в анкете не запрашиваются и не обрабатываются. Фотографическое изображение в копии паспорта не используется для установления личности по биометрическим признакам.

2.2. Посетители сайта

- Цель: обеспечение работы и безопасности сайта, защита от злоупотреблений, диагностика неполадок.
- Данные: IP-адрес, сведения о браузере (User-Agent), адрес запрошенной страницы, дата и время запроса, адрес страницы перехода — в технических журналах веб-сервера; на служебной странице проверки соединения (/status) — IP-адрес, сведения о браузере и результаты проверки, если пользователь сам её запускает.

— Правовое основание: обработка необходима для обеспечения работы сайта, запрошенного пользователем (п. 7 ч. 1 ст. 6 Закона № 152-ФЗ — законный интерес Оператора, не нарушающий прав субъекта).

Сайт не ведёт рекламных и маркетинговых рассылок, не публикует и не распространяет персональные данные неопределённому кругу лиц.

3. Способы и действия по обработке

Обработка ведётся смешанным способом (с использованием средств автоматизации и без них) и включает сбор, запись, систематизацию, накопление, хранение, уточнение, извлечение, использование, передачу (предоставление, доступ), блокирование, удаление и уничтожение. Решения, порождающие юридические последствия для субъекта, исключительно на основании автоматизированной обработки не принимаются.

4. Где хранятся данные

— Анкеты и копии документов кандидатов сохраняются на сервере сайта (хостинг-провайдер ООО «ТАЙМВЭБ.КЛАУД» (Timeweb Cloud), ИНН 7810945525, ОГРН 1227800052215; центр обработки данных в г. Москве, Российская Федерация).

— Технические журналы веб-сервера хранятся на том же сервере.

— Запись, систематизация, накопление и хранение персональных данных граждан РФ ведутся с использованием баз данных, находящихся на территории РФ (ч. 5 ст. 18 Закона № 152-ФЗ).

5. Передача третьим лицам и трансграничная передача

5.1. Текст анкеты кандидата и копии документов после сохранения на сервере в РФ направляются в закрытый канал мессенджера Telegram, доступный только уполномоченным работникам Оператора, участвующим в подборе персонала. Серверы Telegram находятся за пределами Российской Федерации — это трансграничная передача персональных данных, которая осуществляется на основании согласия кандидата. Сервис Telegram предоставляет Telegram FZ-LLC (Объединённые Арабские Эмираты, Дубай), входящая в группу Telegram Group Inc. (Британские Виргинские острова); данные хранятся в центрах обработки данных Telegram в нескольких странах, в том числе за пределами Российской Федерации. Трансграничная передача осуществляется с соблюдением требований статьи 12 Закона № 152-ФЗ, в том числе после уведомления Роскомнадзора о намерении осуществлять трансграничную передачу.

5.2. Хостинг-провайдер предоставляет Оператору вычислительные ресурсы для размещения сайта и не использует размещённые данные в собственных целях.

5.3. На странице «Контакты» может быть показана интерактивная карта сервиса «Яндекс Карты» (ООО «Яндекс»). Карта загружается только после того, как пользователь включил функциональные cookie или сам нажал «Показать карту». При загрузке карты сервис Яндекса получает IP-адрес, сведения о браузере и может использовать собственные cookie.

5.4. На главной странице может быть показан виджет рейтинга курьерских служб «Курьерофф» (сайт kuroff.ru, администрируется его владельцем — физическим лицом, не связанным с Оператором). Виджет загружается только после того, как пользователь включил функциональные cookie; при

загрузке сайт kureroff.ru получает IP-адрес, сведения о браузере и устанавливает собственный cookie.

5.5. Иным третьим лицам персональные данные не передаются, кроме случаев, предусмотренных законодательством РФ (например, по запросам уполномоченных государственных органов).

6. Сроки обработки, хранения и уничтожение

- Анкеты и копии документов кандидатов: до достижения цели обработки, но не дольше 6 (шести) месяцев с даты отправки анкеты, либо до отзыва согласия. Сообщения с анкетами и копиями документов в канале Telegram удаляются уполномоченным работником Оператора в те же сроки.
- Если с кандидатом заключён договор, его данные далее обрабатываются на основании договора и в сроки, установленные законодательством (в том числе об архивном деле и бухгалтерском учёте).
- Технические журналы веб-сервера: 14 дней с последующим автоматическим удалением.
- Данные служебной страницы проверки соединения: не более 30 дней с даты проверки.

По достижении цели, истечении срока или отзыве согласия данные уничтожаются в течение 30 дней путём удаления с сервера и из канала Telegram, что подтверждается актом об уничтожении персональных данных, а при автоматизированной обработке — также выгрузкой из журнала регистрации событий, в соответствии с Требованиями к документальному оформлению факта уничтожения персональных данных, утверждёнными приказом Роскомнадзора от 28.10.2022 № 179.

7. Cookie, технические данные и аналитика

Сайт не использует сервисы веб-аналитики и рекламные пиксели. Сайт хранит в браузере пользователя только сведения о его выборе в отношении cookie (необходимые данные), а сторонние сервисы («Яндекс Карты», виджет рейтинга КурьероФФ) загружаются лишь с согласия пользователя. Подробнее — в Политике использования файлов cookie.

8. Права субъекта персональных данных

Субъект персональных данных вправе:

- получать сведения об обработке своих персональных данных (ч. 7 ст. 14 Закона № 152-ФЗ);
- требовать уточнения, блокирования или уничтожения данных, если они неполные, устаревшие, неточные, незаконно полученные или не являются необходимыми для заявленной цели;
- отозвать согласие на обработку персональных данных;
- обжаловать действия или бездействие Оператора в Роскомнадзоре или в суде.

9. Порядок обращения и отзыв согласия

Запросы и отзыв согласия направляются Оператору на e-mail info@ggco.ru или письмом по адресу, указанному в п. 1.2. Запрос должен содержать сведения, позволяющие идентифицировать субъекта (например, ФИО и телефон, указанные в анкете). Оператор отвечает на запрос в течение 10 рабочих дней с даты его получения; срок может быть продлён не более чем на 5 рабочих дней с уведомлением о причинах.

10. Меры защиты

- передача данных между браузером и сайтом — только по защищённому протоколу HTTPS;
- файлы анкет хранятся на сервере вне общедоступной части сайта и не выдаются по веб-адресам; доступ к серверу имеют только уполномоченные лица;
- служебные страницы сайта защищены паролем, действует ограничение числа попыток входа и частоты отправки форм;
- доступ к каналу Telegram с анкетами имеют только уполномоченные работники Оператора;
- назначение лица, ответственного за организацию обработки персональных данных (п. 1.3), и определение перечня работников, допущенных к персональным данным кандидатов;
- ознакомление работников, допущенных к обработке, с требованиями законодательства о персональных данных, настоящей Политикой и локальными актами Оператора;
- оценка вреда, который может быть причинён субъектам персональных данных, в соответствии с приказом Роскомнадзора от 27.10.2022 № 178;
- определение угроз безопасности и уровня защищённости персональных данных в информационной системе в соответствии с постановлением Правительства РФ от 01.11.2012 № 1119;
- внутренний контроль соответствия обработки персональных данных требованиям Закона № 152-ФЗ и настоящей Политики.

11. Заключительные положения

Политика публикуется в свободном доступе по адресу <https://ggco.ru/privacy>. Оператор вправе изменять Политику; новая редакция действует с момента её публикации на сайте и заменяет предыдущие.

Раздел II. Справочные приложения

Справочный материал. Не является частью Политики и не устанавливает обязательств Оператора. Сведения о том, какие данные обрабатывает Оператор, в каких целях и в какие сроки, содержатся только в Политике (раздел I).

Приложение 1. Термины и определения

Справочный материал. Не является частью Политики и не устанавливает обязательств Оператора. Сведения о том, какие данные обрабатывает Оператор, в каких целях и в какие сроки, содержатся только в Политике (раздел I).

Это приложение объясняет простыми словами понятия, которые встречаются в Политике обработки персональных данных, в законодательстве о персональных данных и в повседневной работе любого сайта или сервиса. Пояснения носят просветительский характер. Юридически значимые формулировки содержатся в Федеральном законе от 27 июля 2006 года № 152-ФЗ «О персональных данных» и в самой Политике; если толкование в этом приложении в чём-то расходится с законом или с Политикой, приоритет имеют они. Примеры подобраны из жизни курьерской службы: человек заказывает доставку, кандидат откликается на вакансию курьера, посетитель просто заходит на сайт, чтобы узнать условия работы.

Персональные данные

Персональные данные — это любая информация, которая прямо или косвенно относится к определённом или определяемому физическому лицу. Закон намеренно формулирует понятие широко: речь идёт не только о паспорте и фамилии, но о любых сведениях, по которым можно понять, о каком именно человеке идёт речь, или которые с этим человеком связаны.

На практике к персональным данным относятся фамилия, имя и отчество, номер телефона, адрес электронной почты, адрес доставки, дата рождения, фотография, сведения об опыте работы, ник в мессенджере в сочетании с перепиской. Например, когда кандидат на работу курьером пишет в анкете своё имя, город и телефон, всё это — его персональные данные. Важно понимать, что отдельная деталь сама по себе может и не указывать на человека, но в сочетании с другими сведениями она начинает его определять, и тогда эта деталь тоже становится персональными данными.

Субъект персональных данных

Субъект персональных данных — это физическое лицо, к которому относятся персональные данные. Проще говоря, это сам человек, о котором идёт речь. Субъектом может быть клиент, получатель посылки, кандидат на вакансию, сотрудник, посетитель сайта, человек, который написал в чат поддержки.

Закон наделяет субъекта рядом прав: узнавать, обрабатываются ли его данные, получать сведения об обработке, требовать уточнения неточных данных, их блокирования или уничтожения, отзываться согласие, обжаловать действия оператора. Например, человек, который однажды откликнулся на вакансию и передумал, остаётся субъектом в отношении тех данных, которые он успел оставить, и вправе спросить, что с ними происходит.

Оператор

Оператор — это государственный орган, муниципальный орган, юридическое или физическое лицо, которое самостоятельно или совместно с другими лицами организует и (или) осуществляет обработку персональных данных, а также определяет цели обработки, состав данных и действия с ними. Ключевое в этом определении — именно определение целей и средств: оператор решает, зачем и как обрабатываются сведения.

Оператор несёт основную ответственность перед субъектом. Даже если часть работы выполняет подрядчик, например хостинг-провайдер или сервис рассылок, перед человеком отвечает тот, кто организовал обработку. Кто является оператором в отношении данных, обрабатываемых на сайте и в

сервисах компании, указано в соответствующем разделе Политики.

Обработка персональных данных

Обработка — это любое действие или совокупность действий с персональными данными, совершаемых с использованием средств автоматизации или без них. Закон перечисляет такие действия: сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение.

Из этого перечня видно, что обработкой считается практически всё, что вообще можно сделать с информацией. Даже простое хранение анкеты в папке без какого-либо использования — уже обработка. Когда менеджер открывает карточку заказа, чтобы уточнить адрес, он извлекает и использует данные; когда исправляет опечатку в номере телефона — уточняет; когда удаляет старую заявку — уничтожает.

Автоматизированная обработка персональных данных

Автоматизированная обработка — это обработка персональных данных с помощью средств вычислительной техники. Сюда относится работа с данными в базах данных, в таблицах, в системах управления заказами, в почтовых сервисах, в чат-ботах, на сайте.

Противоположность — неавтоматизированная обработка, например работа с бумажными анкетами. На деле в большинстве организаций обработка смешанная: человек заполняет форму на сайте (автоматизированно), а затем сотрудник может распечатать документ и подписать его (неавтоматизированно). Для каждого вида обработки закон и подзаконные акты предусматривают свои требования к защите.

Неавтоматизированная обработка

Неавтоматизированной обработка считается тогда, когда такие действия, как использование, уточнение, распространение и уничтожение данных в отношении каждого субъекта, осуществляются при непосредственном участии человека. Классический пример — бумажный журнал, папка с копиями документов, распечатанный список.

Такая обработка тоже требует защиты: бумажные документы нужно хранить так, чтобы к ним не получили доступ посторонние, а уничтожать — способом, исключающим восстановление. Типичная ошибка организаций — выбрасывать распечатки с персональными данными в обычную урну вместо того, чтобы пропускать их через шредер или иным образом надёжно уничтожать.

Распространение персональных данных

Распространение — это действия, направленные на раскрытие персональных данных неопределённому кругу лиц. Ключевое слово здесь — «неопределённому»: данные становятся доступны любому желающему, и оператор уже не контролирует, кто их увидит.

Примеры распространения — публикация списка лучших курьеров месяца с фамилиями на открытой странице сайта или размещение фотографии сотрудника в публичном канале. Для распространения закон требует отдельного согласия, оформленного по особым правилам, о чём подробнее рассказано в определении данных, разрешённых субъектом для распространения.

Предоставление персональных данных

Предоставление — это действия, направленные на раскрытие персональных данных определённому лицу или определённому кругу лиц. В отличие от распространения, здесь известно, кому именно передаются сведения.

Например, когда служба доставки передаёт курьеру имя и телефон получателя, чтобы тот смог связаться с человеком при доставке, это предоставление данных определённому лицу. Когда организация по закону направляет сведения в государственный орган, это тоже предоставление. Предоставление допускается при наличии законного основания и только в объёме, необходимом для цели.

Блокирование персональных данных

Блокирование — это временное прекращение обработки персональных данных, за исключением случаев, когда обработка необходима для уточнения данных. Данные при этом не удаляются, но ими нельзя пользоваться в обычном порядке.

Блокирование применяется, например, когда человек сообщил, что его данные неточны, и оператору нужно время на проверку. Пока идёт проверка, данные блокируются, чтобы неверные сведения не использовались. Также блокирование применяется, если выявлена неправомерная обработка, — до устранения нарушения.

Уничтожение персональных данных

Уничтожение — это действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе и (или) в результате которых уничтожаются материальные носители персональных данных.

Важно различать уничтожение и простое удаление в бытовом смысле. Если запись в базе только помечена как удалённая, но физически остаётся и может быть восстановлена, с точки зрения закона она не уничтожена. Уничтожение бумажного документа — это измельчение или сжигание, а не выбрасывание целиком. Закон также требует подтверждать факт уничтожения в установленном порядке.

Удаление персональных данных

Удаление в обиходе означает стирание записи из системы. В законе удаление стоит в перечне действий по обработке рядом с уничтожением. Практическое различие состоит в том, что удаление может быть обратимым: файл попадает в корзину, запись остаётся в резервной копии, сообщение остаётся у собеседника.

Поэтому, когда человек просит удалить свои данные, добросовестный оператор проверяет все места, где они могут храниться: основную базу, почтовые ящики сотрудников, выгрузки в таблицах, резервные копии. Порядок обращения с резервными копиями обычно описывается отдельно, поскольку из них данные удаляются по мере их естественной замены новыми копиями.

Обезличивание персональных данных

Обезличивание — это действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту. Например, вместо фамилии в отчёте ставится условный номер, а таблица соответствия номеров и фамилий хранится отдельно и под защитой.

Обезличивание полезно для аналитики: можно посчитать, сколько кандидатов откликнулось на вакансию в каждом городе, не видя их имён. Следует помнить, что обезличенные данные не всегда

перестают быть персональными: если таблица соответствия существует, личность можно восстановить. Поэтому обезличивание — это мера снижения риска, а не способ полностью вывести данные из-под действия закона.

Анонимизация

Анонимизация — термин, широко используемый в технической и зарубежной практике, обозначающий необратимое удаление связи между данными и человеком. В отличие от обезличивания, после анонимизации восстановить личность не может никто, включая самого оператора.

Достичь настоящей анонимизации сложнее, чем кажется. Если в наборе данных остались дата рождения, район проживания и место работы, то даже без имени человека нередко можно узнать. Именно поэтому при подготовке статистики опытные специалисты укрупняют данные: вместо точной даты рождения указывают возрастную группу, вместо адреса — город.

Информационная система персональных данных

Информационная система персональных данных — это совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств. Иными словами, это сами данные плюс программы и оборудование, с помощью которых с ними работают.

Информационной системой может быть сайт с формой заявки и базой, в которую заявки сохраняются; система учёта заказов; программа кадрового учёта. Для каждой информационной системы оператор определяет уровень защищённости и принимает соответствующие меры, установленные требованиями к защите персональных данных.

Трансграничная передача персональных данных

Трансграничная передача — это передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу. Важно, что значение имеет не только физическое пересечение границы, но и то, кому передаются сведения.

Трансграничная передача может происходить незаметно для обычного пользователя: например, если на сайте установлен виджет иностранного сервиса или если письма проходят через зарубежный почтовый сервис. Закон устанавливает особые условия такой передачи, включая предварительное уведомление уполномоченного органа и учёт того, обеспечивает ли иностранное государство адекватную защиту прав субъектов. Есть ли трансграничная передача в конкретном случае, указывается в Политике.

Специальные категории персональных данных

Специальные категории — это сведения, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, а также сведения о судимости, обработка которых регулируется отдельно. Обработка таких данных по общему правилу запрещена, кроме прямо перечисленных в законе случаев.

Для курьерской службы это означает, например, что в анкете кандидата не должно быть вопросов о религии или национальности, поскольку они не нужны для оценки пригодности к работе. Сведения о состоянии здоровья могут обрабатываться только в случаях, предусмотренных законодательством, например трудовым, и с соблюдением особых правил.

Биометрические персональные данные

Биометрические персональные данные — это сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность, и которые используются оператором для установления личности субъекта. Примеры — отпечатки пальцев, изображение радужной оболочки глаза, геометрия лица, используемая системой распознавания.

Важная деталь: обычная фотография в анкете сама по себе, как правило, не считается биометрическими данными, если оператор не использует её для установления личности, например не сравнивает её автоматически с другим изображением. Если же фото применяется для идентификации, требования к обработке становятся значительно строже, включая необходимость письменного согласия.

Персональные данные, разрешённые субъектом для распространения

Это персональные данные, доступ неограниченного круга лиц к которым предоставлен самим субъектом путём дачи отдельного согласия на обработку данных, разрешённых для распространения. Такое согласие оформляется отдельно от иных согласий и может содержать запреты и условия.

Например, если компания захочет разместить на сайте отзыв курьера с его именем и фотографией, ей понадобится именно такое отдельное согласие. Человек вправе указать, что разрешает публиковать только имя, но не фотографию, или только на сайте, но не в социальных сетях. Тот факт, что сведения о человеке где-то уже опубликованы, сам по себе не даёт другим операторам права их свободно использовать.

Общедоступные персональные данные

Общедоступными в обиходе называют сведения, которые человек сам сделал доступными всем, например указал в открытом профиле. Однако закон с определённого момента делает акцент не на «общедоступности» как таковой, а на наличии согласия субъекта на распространение.

На практике это значит, что нельзя рассуждать так: «Телефон человека есть в интернете, значит, мы можем внести его в базу и звонить с предложениями». Для обработки всё равно нужно законное основание, а цели обработки должны быть совместимы с тем, ради чего человек разместил сведения.

Согласие на обработку персональных данных

Согласие — одно из оснований обработки. Закон требует, чтобы согласие было конкретным, предметным, информированным, сознательным и однозначным. Это значит, что человек должен понимать, кто будет обрабатывать его данные, какие именно, зачем и как долго, и выразить своё согласие явно.

Галочка, которая заранее проставлена в форме, или фраза «продолжая пользоваться сайтом, вы соглашаетесь со всем» вызывают серьёзные сомнения с точки зрения однозначности. Хорошая практика — отдельный чекбокс, который человек ставит сам, со ссылкой на текст согласия и на Политику. Например, кандидат, заполняющий анкету курьера, видит, какие данные у него просят, и отдельно отмечает согласие на их обработку.

Письменное согласие

В ряде случаев закон требует согласия в письменной форме — например, при обработке специальных категорий данных, биометрических данных, при некоторых видах трансграничной передачи. Письменная форма означает документ с собственноручной подписью субъекта; равнозначным ему

признаётся согласие в форме электронного документа, подписанного электронной подписью в соответствии с законодательством.

Письменное согласие должно содержать определённый законом набор сведений: данные субъекта и оператора, цель обработки, перечень данных, перечень действий, срок действия согласия и способ его отзыва. Если какого-то обязательного элемента нет, согласие может быть признано ненадлежащим.

Отзыв согласия

Отзыв согласия — это заявление субъекта о том, что он больше не согласен на обработку своих данных. Отзыв по общему правилу возможен в любой момент, и оператор не вправе ставить его в зависимость от каких-либо условий.

После получения отзыва оператор обязан прекратить обработку и уничтожить данные, если сохранение не требуется по иным основаниям, например по закону или по договору. Например, если кандидат на вакансию отозвал согласие, анкету следует уничтожить; но если человек уже стал сотрудником, некоторые кадровые документы оператор обязан хранить по требованиям законодательства независимо от отзыва. Способы направления отзыва указываются в Политике.

Законное основание обработки

Законное основание — это обстоятельство, которое делает обработку правомерной. Согласие — лишь одно из них. Закон также допускает обработку, если она необходима для исполнения договора, стороной которого является субъект, для выполнения обязанностей, возложенных на оператора законом, для защиты жизни и здоровья, для осуществления прав и законных интересов оператора при условии, что не нарушаются права субъекта, и в ряде других случаев.

Например, чтобы доставить посылку, службе нужен адрес и телефон получателя: эта обработка необходима для исполнения договора. Отдельного согласия на неё, как правило, не требуется, но человек всё равно имеет право знать, как используются его данные.

Лицо, осуществляющее обработку по поручению оператора

Оператор вправе поручить обработку персональных данных другому лицу. Такое лицо часто называют обработчиком. Поручение оформляется договором или иным актом, в котором должны быть указаны перечень действий, цели обработки, обязанность соблюдать конфиденциальность и обеспечивать безопасность данных, а также требования к защите.

Типичные обработчики — хостинг-провайдер, на серверах которого работает сайт; сервис, который отправляет SMS; бухгалтерская фирма. Обработчик не вправе использовать данные в собственных целях. При этом ответственность перед субъектом несёт оператор, а обработчик отвечает перед оператором.

Третье лицо

Третьим лицом в контексте персональных данных обычно называют любое лицо, кроме самого субъекта, оператора и обработчика. Передача данных третьим лицам возможна только при наличии законного основания.

Например, если получатель посылки попросил передать её соседу, то сосед становится третьим лицом, и сообщать ему данные получателя сверх необходимого нельзя. Аналогично звонок от человека, который представился родственником кандидата и просит рассказать о результатах собеседования, — запрос третьего лица, и без законного основания сведения ему не сообщаются.

Конфиденциальность персональных данных

Конфиденциальность — это обязанность операторов и иных лиц, получивших доступ к персональным данным, не раскрывать их третьим лицам и не распространять без согласия субъекта, если иное не предусмотрено законом.

Эта обязанность распространяется на каждого сотрудника, работающего с данными. Курьер, который знает адрес и телефон клиента, не вправе обсуждать их с посторонними или использовать для личного общения. Менеджер, видевший анкету кандидата, не вправе пересылать её знакомым. Нарушение конфиденциальности может повлечь ответственность.

Уполномоченный орган по защите прав субъектов персональных данных

В России функции уполномоченного органа выполняет Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор). Он ведёт реестр операторов, проводит контрольные мероприятия, рассматривает жалобы граждан.

Если человек считает, что его права нарушены, он может обратиться к оператору, а также в уполномоченный орган или в суд. Обращение к оператору не является обязательным предварительным шагом, но часто позволяет решить вопрос быстрее.

Уведомление об обработке

Уведомление об обработке — это сообщение, которое оператор по общему правилу направляет в уполномоченный орган до начала обработки персональных данных. В нём указываются сведения об операторе, цели обработки, категории данных и субъектов, правовые основания, меры защиты и иные сведения.

На основании уведомлений формируется публичный реестр операторов. Любой человек может проверить, зарегистрирован ли оператор в реестре. При изменении сведений, указанных в уведомлении, оператор обязан сообщить об изменениях.

Ответственный за организацию обработки персональных данных

Оператор, являющийся юридическим лицом, назначает лицо, ответственное за организацию обработки персональных данных. Это сотрудник, который следит за соблюдением законодательства внутри организации, доводит до работников требования, организует приём обращений субъектов.

Наличие такого ответственного важно и для человека: именно через него или через указанный в Политике канал обычно удобнее всего направлять вопросы и требования. Контакты для обращений по вопросам персональных данных приведены в соответствующем разделе Политики.

Утечка персональных данных

Утечка — это неправомерная или случайная передача, предоставление, распространение персональных данных или доступ к ним, в результате которых нарушены права субъектов. Утечка может произойти из-за взлома, ошибки сотрудника, потери ноутбука, неправильной настройки сервера.

Пример ошибки: сотрудник по невнимательности отправил таблицу со списком кандидатов в общий чат вместо личного сообщения коллеге. Это тоже утечка, даже если злого умысла не было. При выявлении таких случаев закон обязывает оператора уведомить уполномоченный орган в сжатые сроки: о самом факте инцидента — в течение суток, о результатах внутреннего расследования — в течение трёх суток.

Инцидент информационной безопасности

Инцидент — это событие, которое нарушает или может нарушить безопасность информации: попытка взлома, заражение компьютера вредоносной программой, подозрительный вход в учётную запись, несанкционированный доступ к базе.

Не каждый инцидент приводит к утечке, но каждый требует реакции: выяснить, что произошло, ограничить ущерб, устранить причину, при необходимости уведомить пострадавших и регулятор. Зрелые организации ведут учёт инцидентов и анализируют их, чтобы ошибки не повторялись.

Угрозы безопасности персональных данных

Угрозы — это совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать их уничтожение, изменение, блокирование, копирование, предоставление, распространение.

Угрозы бывают внешние (хакеры, мошенники) и внутренние (небрежные или недобросовестные сотрудники), технические (сбой оборудования) и организационные (отсутствие правил доступа). Определение актуальных угроз — первый шаг при выборе мер защиты: невозможно защищаться от всего сразу, поэтому оператор оценивает, какие угрозы для его систем наиболее вероятны и опасны.

Уровень защищённости

Уровень защищённости — это комплексный показатель, который характеризует требования к защите информационной системы с учётом категорий обрабатываемых данных, их объёма и актуальных угроз. Правительство Российской Федерации установило несколько уровней защищённости, от наиболее строгого к наименее строгому.

Для каждого уровня определён набор организационных и технических мер. Например, система, где хранятся сведения о здоровье большого числа людей, требует более серьёзной защиты, чем система, в которой хранятся только имена и телефоны небольшого числа клиентов.

IP-адрес

IP-адрес — это числовой адрес устройства в сети, по которому сервер понимает, куда отправить ответ. Когда человек открывает сайт, его устройство сообщает серверу свой IP-адрес; без этого страница просто не смогла бы загрузиться.

Сам по себе IP-адрес часто указывает не на конкретного человека, а на точку подключения: домашний роутер, мобильного оператора, офисную сеть. Однако в сочетании с другими сведениями, например с временем входа и данными учётной записи, он может помочь определить человека, поэтому многие операторы осторожно относятся к IP-адресам как к сведениям, которые могут быть персональными данными.

User-Agent

User-Agent — это строка, которую браузер передаёт серверу при каждом запросе. В ней указываются тип и версия браузера, операционная система, иногда модель устройства. Например, из неё можно понять, что посетитель зашёл на страницу вакансии с телефона под управлением Android через определённую версию браузера.

Эти сведения нужны, чтобы правильно показать страницу: мобильную версию для телефона, полную — для компьютера. Они также попадают в журналы веб-сервера и используются для диагностики ошибок. Сами по себе они редко указывают на конкретного человека, но в совокупности с другими

признаками участвуют в формировании отпечатка браузера.

Cookie

Cookie (куки) — это небольшие текстовые файлы, которые сайт сохраняет в браузере посетителя. При следующем обращении браузер отправляет их обратно, и сайт «узнаёт» устройство. Благодаря cookie сайт помнит, что посетитель уже выбрал город, вошёл в личный кабинет или закрыл всплывающее окно.

Cookie бывают необходимыми для работы сайта (без них невозможно, например, сохранить вход), функциональными (запоминают настройки), аналитическими (помогают понять, какие страницы популярны) и рекламными. Пользователь может посмотреть и удалить cookie в настройках браузера, а также запретить их сохранение, хотя при этом часть функций сайта может перестать работать.

Сессионные cookie

Сессионные cookie живут только до закрытия браузера. Как только человек закрывает окно, они удаляются. Их назначение — поддерживать работу сайта в течение одного визита: например, помнить, что посетитель заполнил первую страницу анкеты и перешёл ко второй.

Такие cookie обычно считаются наименее чувствительными с точки зрения приватности, поскольку они не позволяют отслеживать человека от визита к визиту. Без них многие формы и личные кабинеты просто не смогли бы работать.

Постоянные cookie

Постоянные cookie сохраняются в браузере на определённый срок, который задаёт сайт, — от нескольких часов до нескольких лет, — или до тех пор, пока пользователь сам их не удалит. Они позволяют сайту узнать посетителя при повторном визите.

Например, постоянная cookie может помнить выбранный язык или то, что посетитель уже согласился с уведомлением о cookie. Аналитические сервисы с помощью постоянных cookie отличают новых посетителей от вернувшихся. Чем дольше срок жизни такой cookie и чем больше сайтов её читает, тем выше потенциальное влияние на приватность.

Собственные и сторонние cookie

Собственные (first-party) cookie устанавливает тот сайт, который человек открыл в адресной строке. Сторонние (third-party) cookie устанавливают другие домены, чьи элементы встроены в страницу: счётчики аналитики, рекламные сети, кнопки социальных сетей, встроенные карты.

Сторонние cookie позволяют внешним сервисам видеть посетителя на разных сайтах, где установлены их элементы, и строить представление о его интересах. Поэтому многие браузеры по умолчанию ограничивают или блокируют сторонние cookie. Какие внешние сервисы используются на сайте компании, описывается в Политике и, при наличии, в отдельном уведомлении о cookie.

Локальное хранилище браузера (localStorage)

localStorage — это механизм браузера, позволяющий сайту сохранять данные на устройстве посетителя в большем объёме, чем cookie, и без автоматической отправки на сервер при каждом запросе. Данные хранятся до тех пор, пока их не удалит сайт или сам пользователь.

Сайты используют localStorage, например, чтобы запомнить черновик заполняемой анкеты, если человек случайно закрыл страницу, или чтобы хранить настройки интерфейса. С точки зрения

приватности localStorage сходен с постоянными cookie: очистить его можно через настройки браузера, удалив данные сайта.

Сессионное хранилище (sessionStorage)

sessionStorage — родственный localStorage механизм, но данные в нём живут только в пределах одной вкладки и удаляются при её закрытии. Это удобно для временных сведений, которые не нужны после окончания визита.

Например, сайт может хранить в sessionStorage номер шага многоэтапной формы. Если человек откроет сайт в новой вкладке, там этих сведений уже не будет. Такой механизм практически не влияет на возможность долговременного отслеживания.

Сессия

Сессией называют период непрерывного взаимодействия пользователя с сайтом или приложением. В техническом смысле сессия — это способ сервера связать между собой последовательные запросы одного и того же посетителя, обычно с помощью уникального идентификатора, хранящегося в cookie.

Например, после входа в личный кабинет сервер выдаёт идентификатор сессии, и пока он действителен, пользователю не нужно вводить пароль заново. Если злоумышленник похитит этот идентификатор, он может выдать себя за пользователя, поэтому идентификаторы сессий защищают, ограничивают срок их действия и аннулируют при выходе.

HTTPS

HTTPS — это защищённая версия протокола, по которому браузер обменивается данными с сайтом. Буква S означает secure, то есть «защищённый». При использовании HTTPS всё, что передаётся между устройством и сервером, шифруется.

На практике признак HTTPS — адрес, начинающийся с https://, и значок замка в адресной строке. Если человек заполняет анкету на сайте без HTTPS, его данные могут быть перехвачены, например, в общественной сети Wi-Fi в кафе. Поэтому вводить персональные данные стоит только на страницах, работающих по HTTPS.

TLS

TLS (Transport Layer Security) — это криптографический протокол, на котором основан HTTPS и многие другие защищённые соединения, например между почтовыми серверами. Он обеспечивает три вещи: шифрование передаваемых данных, проверку подлинности сервера и защиту от незаметного изменения данных в пути.

Подлинность сервера подтверждается сертификатом, выданным удостоверяющим центром. Если сертификат недействителен или принадлежит другому сайту, браузер выдаёт предупреждение. Такое предупреждение нельзя игнорировать: оно может означать, что соединение перехватывается.

Шифрование

Шифрование — это преобразование информации в вид, непонятный без специального ключа. Различают шифрование при передаче (данные защищены, пока идут по сети) и шифрование при хранении (данные защищены, пока лежат на диске или в базе).

Шифрование не делает данные недоступными для оператора, у которого есть ключ, но существенно снижает последствия кражи носителя или перехвата трафика. Например, если зашифрованный ноутбук потерян, найти на нём анкеты кандидатов без ключа практически невозможно.

Хеширование

Хеширование — это одностороннее преобразование данных в строку фиксированной длины, из которой нельзя восстановить исходное значение. В отличие от шифрования, у хеширования нет ключа для обратного преобразования.

Хеширование применяют прежде всего для хранения паролей: система хранит не сам пароль, а его хеш, и при входе сравнивает хеш введённого пароля с сохранённым. Если база будет похищена, злоумышленник не получит пароли в открытом виде. Добросовестные сервисы используют для этого специальные медленные алгоритмы с добавлением случайной «соли».

Пароль

Пароль — это секретная последовательность символов, подтверждающая, что в учётную запись входит её владелец. Надёжность пароля зависит прежде всего от его длины и непредсказуемости.

Хорошая практика для пользователя — не использовать один и тот же пароль на разных сайтах, применять менеджер паролей и не сообщать пароль никому, включая людей, которые представляются сотрудниками поддержки. Добросовестная организация никогда не просит назвать пароль по телефону или в мессенджере.

Двухфакторная аутентификация

Двухфакторная аутентификация — это способ входа, при котором кроме пароля нужен второй, независимый признак: одноразовый код из SMS или приложения-генератора, аппаратный ключ, подтверждение на другом устройстве.

Смысл в том, что для взлома злоумышленнику мало узнать пароль — нужно ещё получить доступ ко второму фактору. Для сотрудников, имеющих доступ к базам с персональными данными, двухфакторная аутентификация считается одной из наиболее эффективных и недорогих мер защиты.

Аутентификация и авторизация

Аутентификация — это проверка того, что пользователь действительно тот, за кого себя выдаёт, например по паролю. Авторизация — это определение того, что этому пользователю разрешено делать после входа.

В курьерской службе разные сотрудники обычно должны иметь разный доступ: курьер видит только адреса своих текущих заказов, менеджер по подбору — анкеты кандидатов, бухгалтер — сведения для расчётов. Разграничение прав доступа — одна из базовых мер защиты, вытекающая из принципа минимально необходимого доступа.

Журнал веб-сервера

Журнал (лог) веб-сервера — это файл, в который сервер автоматически записывает сведения о каждом запросе: время, IP-адрес, запрошенную страницу, код ответа, User-Agent, иногда адрес страницы, с которой пришёл посетитель.

Журналы нужны для диагностики ошибок, отражения атак и обеспечения безопасности. Например, по журналу можно понять, что кто-то тысячи раз подряд пытается подобрать пароль к панели управления.

Поскольку журналы содержат IP-адреса, их хранение тоже должно быть ограничено разумным сроком и защищено.

Хостинг

Хостинг — это услуга по размещению сайта или приложения на сервере, подключённом к интернету. Хостинг-провайдер предоставляет оборудование, сетевое подключение и, как правило, базовую защиту инфраструктуры.

С точки зрения персональных данных хостинг-провайдер обычно выступает лицом, которое обеспечивает техническую инфраструктуру, а иногда и обработчиком по поручению оператора. Важно, в какой стране находятся серверы: российское законодательство требует, чтобы при сборе персональных данных граждан Российской Федерации запись, систематизация, накопление, хранение, уточнение и извлечение осуществлялись с использованием баз данных, находящихся на территории России.

Центр обработки данных (ЦОД)

Центр обработки данных — это специально оборудованное здание или помещение, где размещаются серверы. В ЦОД обеспечиваются бесперебойное электропитание, охлаждение, физическая охрана, пожаротушение и резервные каналы связи.

Для человека, чьи данные хранятся в ЦОД, важно, что физический доступ к серверам ограничен и контролируется. Профессиональные ЦОД нередко проходят независимую проверку соответствия стандартам безопасности, что снижает риск физической кражи или повреждения оборудования.

Резервная копия

Резервная копия — это копия данных, сделанная для восстановления на случай сбоя, ошибки или атаки. Например, если из-за неисправности диска потеряна база заказов, её можно восстановить из вчерашней копии.

Резервные копии — важная мера обеспечения доступности и целостности данных, но они сами содержат персональные данные и должны защищаться так же, как основная база. Кроме того, при уничтожении данных по запросу субъекта нужно учитывать, что сведения могут сохраниться в старых копиях до момента их плановой замены; добросовестный оператор не восстанавливает из копий данные, подлежащие уничтожению.

Фишинг

Фишинг — это вид мошенничества, при котором злоумышленник выдаёт себя за известную организацию, чтобы выманить пароли, данные банковских карт или иные сведения. Чаще всего фишинг приходит в виде письма, SMS или сообщения в мессенджере со ссылкой на поддельный сайт.

Курьерские службы — частая мишень для подделок: человеку приходит сообщение «ваша посылка задержана, оплатите доставку по ссылке». Признаки фишинга — срочность, угрозы, ссылка на адрес, похожий на настоящий, но с незаметными отличиями, просьба ввести данные карты или код из SMS. При сомнениях лучше самостоятельно открыть официальный сайт или позвонить по известному номеру, а не переходить по ссылке.

Социальная инженерия

Социальная инженерия — это методы, при которых злоумышленник получает доступ к информации, обманывая людей, а не взламывая технику. Он может позвонить сотруднику, представиться руководителем или работником банка и под благовидным предлогом попросить продиктовать данные.

Например, менеджеру по подбору звонит человек, который представляется сотрудником полиции и просит срочно назвать адрес одного из кандидатов. Правильная реакция — не сообщать сведения по телефону, а действовать по установленной процедуре: запросы государственных органов направляются официальным путём и проверяются.

Мессенджер

Мессенджер — это приложение для обмена сообщениями, например Telegram, WhatsApp, VK Мессенджер, МАХ и другие. Многие организации используют мессенджеры для связи с клиентами, кандидатами и сотрудниками, поскольку это быстро и удобно.

При общении через мессенджер часть данных обрабатывает сам сервис-мессенджер по своим правилам: имя профиля, номер телефона, содержимое переписки, время активности. Человеку полезно понимать, что, отправляя фотографию документа в мессенджер, он передаёт её не только организации, но и через инфраструктуру этого сервиса. Где это возможно, документы лучше передавать через защищённые формы, предусмотренные оператором.

Бот

Бот — это программа, которая автоматически отвечает на сообщения, задаёт вопросы, принимает заявки. В мессенджерах боты часто используются для первичного общения с кандидатами, приёма заказов, отправки уведомлений о статусе доставки.

Когда человек общается с ботом, его сообщения обрабатываются автоматически, а затем могут быть переданы сотрудникам. Добросовестная практика — сообщать человеку, что он общается с автоматической системой, и давать возможность связаться с живым сотрудником. Если бот использует внешние сервисы, например для распознавания текста, это должно учитываться при описании обработки.

Канал

Каналом в мессенджере называют страницу, где автор публикует сообщения для подписчиков; подписчики обычно могут только читать. Каналы бывают открытыми, доступными любому, и закрытыми, доступными по приглашению.

С точки зрения персональных данных важно, что публикация в открытом канале — это распространение, то есть раскрытие сведений неопределённому кругу лиц. Поэтому размещать в каналах сведения о конкретных людях, например фото курьера или его имя, можно только при наличии соответствующего согласия. Закрытый канал снижает круг лиц, но не превращает публикацию в безопасную автоматически.

Сеть доставки контента (CDN)

CDN (Content Delivery Network) — это распределённая сеть серверов, которая хранит копии файлов сайта, например картинок, стилей и скриптов, ближе к посетителям и тем самым ускоряет загрузку страниц.

Когда браузер загружает файл через CDN, сервер этой сети получает IP-адрес и User-Agent посетителя, как при любом сетевом запросе. Если CDN расположена за рубежом или принадлежит иностранной

компании, это может иметь значение с точки зрения трансграничной передачи. Поэтому выбор CDN — не только технический, но и юридический вопрос.

Виджет

Виджет — это готовый элемент стороннего сервиса, встроенный в страницу сайта: онлайн-чат, карта, кнопка «поделиться», форма обратного звонка, видеоплеер. Виджет, как правило, загружается с серверов своего разработчика.

Даже если посетитель не нажимает на виджет, сам факт загрузки страницы может передать разработчику виджета сведения о визите. Например, встроенная карта с офисом компании может сообщить сервису карт IP-адрес посетителя и адрес страницы. Поэтому на сайтах, заботящихся о приватности, количество виджетов ограничивают, а их использование описывают в Политике.

iframe

iframe — это технический способ встроить в страницу другую веб-страницу, как окно в окне. Через iframe часто встраивают видео, карты, платёжные формы, формы сторонних сервисов.

Содержимое iframe работает по правилам своего сервиса: оно может устанавливать собственные cookie и собирать данные о посетителе. С другой стороны, iframe иногда используется и для защиты: например, платёжная форма банка во фрейме означает, что данные карты вводятся напрямую на стороне банка и не проходят через сервер магазина или службы доставки.

Веб-аналитика

Веб-аналитика — это сбор и анализ сведений о том, как посетители пользуются сайтом: какие страницы смотрят, сколько времени проводят, откуда пришли, на каком шаге бросают заполнение формы. Для этого используются счётчики, например Яндекс Метрика или аналогичные сервисы.

Аналитика помогает делать сайт удобнее: если большинство кандидатов уходят со страницы анкеты на вопросе о стаже, возможно, вопрос сформулирован непонятно. Вместе с тем аналитические сервисы обрабатывают идентификаторы устройств и сведения о поведении, поэтому их использование должно быть описано в Политике, а объём собираемых сведений — разумным. Особенно чувствительна функция записи сеансов, при которой фиксируются движения мыши и нажатия на странице.

Отпечаток браузера

Отпечаток браузера (fingerprint) — это совокупность технических характеристик устройства и браузера: разрешение экрана, установленные шрифты, часовой пояс, язык, версия браузера, особенности графической подсистемы. Вместе эти признаки нередко образуют уникальную комбинацию, позволяющую узнать устройство без всяких cookie.

Отпечаток трудно увидеть и трудно удалить, поэтому он считается одним из наиболее инвазивных способов отслеживания. Некоторые браузеры специально усложняют его снятие. Для обычного сайта сервисной компании необходимости снимать отпечатки, как правило, нет; если же такая технология используется, например, для защиты от мошенничества, это следует честно описывать.

Идентификатор устройства

Идентификатор устройства — это уникальная метка, по которой приложение или сервис отличает одно устройство от другого. Это может быть рекламный идентификатор мобильной операционной системы, идентификатор установки приложения, токен для push-уведомлений.

Например, приложение курьера может использовать идентификатор, чтобы отправлять уведомления о новых заказах именно на его телефон. Такие идентификаторы обычно считаются сведениями, которые в сочетании с учётной записью относятся к конкретному человеку. Пользователь, как правило, может сбросить рекламный идентификатор в настройках телефона.

Геолокация

Геолокация — это определение местоположения устройства с помощью спутниковой навигации, сотовых вышек, сетей Wi-Fi или по IP-адресу. Точность варьируется от нескольких метров до уровня города.

В курьерской деятельности геолокация может использоваться, например, для построения маршрута или отображения статуса доставки. Сведения о местоположении особенно чувствительны: они раскрывают, где человек живёт, работает, бывает. Поэтому браузеры и телефоны спрашивают разрешение на доступ к точной геолокации, а добросовестные сервисы запрашивают её только тогда, когда это действительно нужно, и не собирают в фоне без необходимости.

Профилирование

Профилированием называют автоматизированную обработку данных для оценки личных качеств человека, анализа или прогнозирования его поведения, предпочтений, надёжности. Например, система может автоматически оценивать кандидатов по ответам в анкете.

Российский закон устанавливает, что решения, порождающие юридические последствия для человека или иным образом затрагивающие его права, по общему правилу нельзя принимать исключительно на основании автоматизированной обработки, кроме случаев, прямо предусмотренных законом, или при наличии письменного согласия. Человеку должна быть разъяснена процедура и предоставлена возможность возразить против такого решения.

Персональные данные о соискателе

Персональные данные соискателя — это сведения, которые человек сообщает работодателю при поиске работы: резюме, анкета, контакты, сведения об опыте, ответы на вопросы. Это отдельная категория субъектов, обработка данных которых обычно описывается в Политике как отдельная цель.

Типичная ситуация: человек увидел объявление о вакансии курьера, оставил отклик через сайт с вакансиями или через форму на сайте компании. Его данные обрабатываются в целях рассмотрения кандидатуры. Если трудоустройство не состоялось, сохранение анкеты на будущее, например для включения в резерв, требует отдельного основания, как правило согласия.

Получатель отправления

Получатель — человек, которому доставляется посылка или документ. Часто его данные передаёт в службу доставки не он сам, а отправитель: интернет-магазин, компания-партнёр, знакомый.

Для получателя это означает, что служба доставки обрабатывает его имя, телефон и адрес, хотя он мог и не обращаться в неё напрямую. Обработка в этом случае опирается на договор с отправителем и на необходимость доставить отправление, а объём данных должен ограничиваться необходимым для доставки. Получатель вправе обратиться к оператору с вопросами о своих данных так же, как любой другой субъект.

Приложение 2. Принципы обработки персональных данных

Справочный материал. Не является частью Политики и не устанавливает обязательств Оператора. Сведения о том, какие данные обрабатывает Оператор, в каких целях и в какие сроки, содержатся только в Политике (раздел I).

Статья 5 Федерального закона № 152-ФЗ «О персональных данных» закрепляет принципы, на которых должна основываться любая обработка персональных данных. Эти принципы — не декларация, а рабочий инструмент: с ними сверяют каждое решение о том, какие сведения собирать, как их использовать и когда удалять. Ниже каждый принцип разобран отдельно: что он означает, почему он важен, как выглядит его соблюдение на практике, какие ошибки встречаются чаще всего и что принцип даёт самому человеку. Изложение носит общий характер и не описывает конкретные процессы Оператора; о них говорится в соответствующих разделах Политики.

Законность и справедливость обработки

Первый принцип гласит, что обработка персональных данных должна осуществляться на законной и справедливой основе. Законность означает, что для каждой операции с данными есть основание, предусмотренное законом: согласие человека, договор с ним, обязанность, возложенная на оператора законодательством, или иное прямо указанное в законе обстоятельство. Справедливость — понятие более широкое: обработка не должна быть скрытой, вводящей в заблуждение или неожиданной для человека.

Почему это важно. Персональные данные дают власть над человеком: зная его телефон, адрес, место работы и привычки, можно ему навредить, начиная от навязчивых звонков и заканчивая мошенничеством. Требование законности ограничивает эту власть рамками, которые общество через закон признало допустимыми. Требование справедливости защищает от ситуаций, когда формально основание есть, но человека фактически обманули, например спрятали важное условие в мелком шрифте.

На практике соблюдение этого принципа начинается с вопроса: на каком основании мы это делаем? Если организация не может на него ответить, обработка, скорее всего, незаконна. Добросовестный оператор заранее определяет основания для каждой цели и фиксирует их в Политике. Человеку сообщают, кто обрабатывает его данные и зачем, до того, как данные собраны, а не задним числом. Тексты согласий формулируются понятным языком, без расплывчатых оборотов вроде «и в иных целях».

Справедливость проявляется и в мелочах. Если кандидат на вакансию курьера заполняет анкету, он вправе ожидать, что его телефон используют для связи по поводу этой вакансии, а не передадут партнёрам для рекламы кредитов. Если посетитель сайта читает условия доставки, он не ожидает, что сайт тайно записывает каждое движение его мыши. Обработка, которая противоречит разумным ожиданиям человека, даже при наличии формальной галочки, вызывает вопросы с точки зрения справедливости.

Типичные ошибки организаций: ссылка на согласие там, где оно не было получено или получено в ненадлежащей форме; согласие, которое «вшито» в пользовательское соглашение и не может быть отклонено без отказа от услуги, хотя сама услуга этих данных не требует; использование чужих баз контактов, купленных или найденных в интернете, для холодного обзвона; отсутствие какой-либо информации об обработке на сайте. Ещё одна распространённая ошибка — считать, что если данные человека где-то опубликованы, ими можно свободно пользоваться.

Отдельно стоит сказать о скрытых методах сбора. Тайная запись телефонных разговоров без

предупреждения, скрытое снятие отпечатка браузера, сбор сведений о человеке из социальных сетей без его ведома — всё это плохо сочетается с принципом справедливости, даже если оператор считает, что действует в своих законных интересах. Открытость — лучшая защита и для человека, и для самой организации: честно описанная обработка редко становится предметом жалоб.

Для человека этот принцип означает право задать оператору простой вопрос: на каком основании вы обрабатываете мои данные? И получить на него конкретный ответ. Если ответа нет или он сводится к общим словам, это повод воспользоваться правами, которые закон предоставляет субъекту: потребовать прекращения обработки, обратиться в уполномоченный орган или в суд.

Ограничение обработки достижением конкретных, заранее определённых и законных целей

Второй принцип требует, чтобы обработка персональных данных ограничивалась достижением конкретных, заранее определённых и законных целей. Закон прямо запрещает обработку, несовместимую с целями сбора. Здесь сразу три требования: цель должна быть конкретной, определённой заранее и законной.

Конкретность означает, что цель описывается так, чтобы было понятно, какая именно деятельность за ней стоит. «Улучшение качества обслуживания» или «осуществление деятельности компании» — формулировки слишком размытые: под них можно подвести почти что угодно. «Рассмотрение кандидатуры соискателя на вакансию курьера», «доставка отправления получателю», «ответ на обращение, направленное через форму обратной связи» — примеры конкретных целей.

Заранее определённая цель — это цель, известная до начала сбора. Нельзя сначала собрать как можно больше сведений «на всякий случай», а потом придумать, для чего они пригодятся. Такой подход переворачивает логику закона: не данные порождают цели, а цели определяют, какие данные нужны. Если у организации появилась новая цель, для неё нужно отдельно проверить наличие основания, а при необходимости — получить новое согласие и проинформировать человека.

Почему это важно. Цель — это граница, за которую обработка не должна выходить. Человек, давая свои данные, соглашается на определённое использование и рассчитывает, что этим всё ограничится. Когда цели расплывчаты, человек фактически теряет контроль над тем, что с его сведениями происходит. Кроме того, именно от цели зависят все остальные параметры: какой объём данных допустим, кто может иметь к ним доступ, как долго их можно хранить.

На практике оператор составляет перечень целей обработки, и для каждой цели определяет категории субъектов, состав данных, основания, сроки и способы обработки. Такой перечень обычно включается в Политику. Сотрудники, работающие с данными, знают, для чего им даны те или иные сведения, и не используют их иначе. Например, телефон получателя, переданный курьеру для доставки, используется для связи по этой доставке и ни для чего больше.

Совместимость целей — тонкий вопрос. Иногда новая цель тесно связана с исходной и разумно ожидаема человеком: скажем, служба доставки сообщает получателю, что курьер задерживается. Это укладывается в цель доставки. Но если та же служба начинает рассылать получателю рекламу своих услуг, это уже другая цель, которая требует собственного основания. Критерий простой: удивился бы человек такому использованию его данных или нет.

Типичные ошибки: одна цель «для всех случаев» в Политике; использование контактов кандидатов, которым отказали, для последующих рекламных рассылок; использование данных, собранных для обеспечения безопасности, например видеозаписей, для контроля личной жизни сотрудников; передача

клиентской базы аффилированным компаниям «для информирования о продуктах» без согласия. Ещё одна ошибка — несогласованность между Политикой, текстом согласия и реальной практикой: в документах написано одно, а в работе происходит другое.

Для человека принцип означает, что он вправе знать, для каких именно целей обрабатываются его данные, и вправе возражать против использования, выходящего за их рамки. Если кандидат на работу вдруг начал получать рекламные сообщения, он может потребовать прекратить такую обработку, а оператор обязан проверить, на каком основании она ведётся.

Недопустимость объединения баз данных с несовместимыми целями

Третий принцип запрещает объединять базы данных, содержащие персональные данные, обработка которых осуществляется в целях, несовместимых между собой. Этот принцип продолжает предыдущий: если цели отдельных наборов данных не совместимы, нельзя сводить их в одну базу, чтобы использовать сообща.

Смысл запрета в том, что объединение баз создаёт новое качество информации. По отдельности сведения могут быть безобидными: в одной базе — телефоны получателей посылок, в другой — анкеты кандидатов, в третьей — сведения о сотрудниках. Но если всё это слить в одну систему, появляется возможность строить подробные профили людей, которые никогда на это не соглашались, и использовать данные для целей, которые не были заявлены ни в одном из исходных случаев.

Почему это важно. Объединённые базы опаснее и в случае утечки: злоумышленник получает не разрозненные фрагменты, а целостную картину. Кроме того, объединение размывает границы ответственности и доступа: сотрудник, которому нужны только адреса доставок, вдруг получает возможность видеть и анкеты кандидатов. Наконец, объединённые базы труднее чистить: когда человек просит удалить его данные, приходится разбираться, какие записи к какой цели относятся.

На практике соблюдение этого принципа выражается в разделении систем и наборов данных по целям. Анкеты соискателей хранятся отдельно от клиентских заказов, кадровые сведения — отдельно от маркетинговых. Даже если технически данные лежат в одной программе, в ней настраивается разграничение: разные разделы, разные права доступа, разные сроки хранения. Важно, что запрет касается именно несовместимых целей: объединение данных для совместимых целей само по себе не запрещено.

Пример из жизни. Человек однажды получил посылку через курьерскую службу, а через год откликнулся на её вакансию курьера. Если служба сопоставит эти две записи и при собеседовании начнёт обсуждать, что и когда он заказывал, это будет использованием данных о получателе для цели подбора персонала, с которой они несовместимы. Добросовестный оператор такого сопоставления не делает, даже если технически это возможно.

Типичные ошибки организаций: одна общая таблица «все контакты», куда сваливаются клиенты, кандидаты, партнёры и случайные собеседники; выгрузка разных баз в одну систему рассылки; использование базы сотрудников для маркетинговых целей; построение «единого профиля клиента» без анализа совместимости целей и без информирования людей. Часто это происходит не из злого умысла, а из соображений удобства, но последствия для людей от этого не меньше.

Для человека принцип означает защиту от того, чтобы сведения, оставленные им в одной ситуации, неожиданно всплыли в совсем другой. Если человек подозревает, что его данные были перенесены из одного контекста в другой без основания, он вправе запросить у оператора сведения об обработке и потребовать прекращения неправомерного использования.

Обработка только тех персональных данных, которые отвечают целям обработки

Четвёртый принцип устанавливает, что обработке подлежат только персональные данные, которые отвечают целям их обработки. Это требование связывает набор собираемых сведений с заявленной целью: если данные не нужны для достижения цели, их не следует обрабатывать.

Смысл принципа — дисциплина в отношении каждого отдельного поля, каждого вопроса анкеты, каждой собираемой характеристики. Для каждого элемента данных должен существовать ответ на вопрос: как именно он помогает достичь цели? Если ответ звучит как «может пригодиться» или «так принято», значит, это поле, скорее всего, лишнее.

Почему это важно. Каждый лишний элемент данных — это дополнительный риск без дополнительной пользы. Его могут похитить, по ошибке раскрыть, неправильно использовать. Кроме того, запрос лишних сведений подрывает доверие: человек, которого при отклике на вакансию курьера просят указать семейное положение, вероисповедание или доход супруга, вполне обоснованно задаётся вопросом, зачем это нужно и куда это пойдёт.

На практике соблюдение принципа выглядит как регулярный пересмотр форм и процессов. Анкета соискателя должна содержать то, что действительно нужно для оценки кандидата и связи с ним: например, имя, контакт, город, опыт, готовность к определённому графику. Форма заказа доставки — то, что нужно для доставки: адрес, контакт получателя, сведения об отправлении. Если какое-то поле оставлено «на будущее», его стоит убрать или сделать необязательным с понятным объяснением, зачем оно.

Важно учитывать и технические данные. Сайт, как правило, неизбежно получает IP-адрес и сведения о браузере — без этого невозможно показать страницу. Но вопрос о том, нужно ли эти сведения сохранять, передавать в аналитические сервисы, связывать с заявками, решается исходя из целей. Если цель — обеспечить работу и безопасность сайта, хранение журналов в течение разумного срока оправдано; если же цели нет, данные лучше не накапливать.

Типичные ошибки: формы с десятками обязательных полей, большинство из которых нигде не используются; запрос копий документов на этапе, когда они ещё не нужны, например просьба прислать фото паспорта ещё до собеседования; сбор сведений о родственниках без необходимости; установка на сайт множества аналитических и рекламных счётчиков «по умолчанию», без анализа, нужны ли они. Нередко лишние сведения собираются просто потому, что шаблон формы был взят у другой организации с другими задачами.

Для человека принцип означает право не сообщать сведения, которые не нужны для цели, и право спросить, зачем у него просят те или иные данные. Если ответ неубедителен, это сигнал насторожиться. Отдельно полезно помнить: если необязательное поле можно оставить пустым, это не должно влиять на рассмотрение заявки или оказание услуги.

Соответствие содержания и объёма данных заявленным целям, недопустимость избыточности

Пятый принцип тесно связан с предыдущим и уточняет его: содержание и объём обрабатываемых персональных данных должны соответствовать заявленным целям обработки, а обрабатываемые данные не должны быть избыточными по отношению к заявленным целям. Если предыдущий принцип отвечает на вопрос «какие данные», то этот — ещё и на вопрос «сколько» и «насколько подробно».

Соответствие по содержанию означает, что характер сведений совпадает с целью. Соответствие по

объёму означает, что их количество и степень детализации не превышают необходимого. Например, для связи с кандидатом нужен один рабочий контакт, а не все его телефоны, адреса почты и страницы в социальных сетях. Для понимания, удобно ли кандидату добираться до места работы, может быть достаточно района или ближайшей станции метро, а не точного адреса с номером квартиры.

Почему это важно. Избыточность — одна из самых распространённых проблем в обработке персональных данных, и одна из самых незаметных. Организации склонны собирать больше, чем нужно, потому что это кажется безвредным и удобным. Но избыточные данные увеличивают последствия любой утечки, усложняют выполнение запросов субъектов и требуют больше ресурсов на защиту. Принцип минимизации, по сути, — самый дешёвый способ защиты: то, чего у организации нет, невозможно потерять.

На практике соблюдение этого принципа выражается в нескольких привычках. Сведения запрашиваются поэтапно: на первом шаге — минимум для начала общения, на последующих — по мере реальной необходимости. Например, при первичном отклике на вакансию достаточно имени и контакта, а документы, необходимые для оформления, запрашиваются, когда дело действительно дошло до оформления, и по каналу, подходящему для таких документов. Доступ сотрудников тоже ограничивается объёмом, нужным для их задачи.

Ещё одна сторона принципа — степень детализации технических данных. Аналитика сайта часто может работать с укрупнёнными показателями: сколько посетителей, из какого города, с каких устройств. Для этого не нужно хранить полные IP-адреса или записывать каждое действие посетителя. Многие аналитические инструменты позволяют отключить избыточные функции, такие как запись сеансов или сбор полных адресов страниц с параметрами, в которых могут оказаться персональные данные.

Типичные ошибки: сканирование всего паспорта целиком, когда нужны только отдельные реквизиты; хранение переписки целиком, когда для цели достаточно итогового результата; запрос фотографии там, где она не нужна; сбор точной геолокации, когда достаточно города; дублирование одних и тех же сведений в нескольких системах. Отдельная ошибка — просить человека прислать документы в мессенджер «для удобства», после чего копии месяцами лежат в переписке у нескольких сотрудников.

Для человека этот принцип означает, что он вправе ожидать сдержанности. Разумная организация попросит ровно столько, сколько нужно, и объяснит, зачем. Если при отклике на вакансию сразу просят прислать фото всех страниц паспорта, СНИЛС, ИНН и банковские реквизиты, это повод уточнить, действительно ли всё это нужно на данном этапе, и выяснить, каким образом документы будут защищены. Такая осторожность полезна ещё и потому, что под видом работодателей нередко действуют мошенники, собирающие документы для своих целей.

Точность, достаточность и актуальность персональных данных

Шестой принцип требует, чтобы при обработке персональных данных обеспечивались их точность, достаточность, а в необходимых случаях и актуальность по отношению к целям обработки. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.

Точность означает, что сведения верны: правильно записаны имя, номер телефона, адрес. Достаточность означает, что данных хватает для достижения цели: нельзя доставить посылку, если в адресе не указан номер дома. Актуальность означает, что сведения не устарели: если человек сменил номер телефона, старый номер уже не позволит с ним связаться, а звонки по нему будут беспокоить

совсем другого человека.

Почему это важно. Неточные данные могут навредить человеку напрямую. Письмо доставят не по адресу, и её получит посторонний. Сообщение с личной информацией уйдёт на чужой номер. Кандидату откажут из-за ошибки в записи о его опыте. Неточность в данных — это не только неудобство для организации, но и риск нарушения прав субъекта, в том числе раскрытия его сведений третьим лицам.

На практике соблюдение принципа начинается с аккуратного сбора: проверка формата номера телефона и адреса почты в формах, подтверждение контакта кодом, возможность для человека самому проверить введённые данные перед отправкой. Далее — удобный способ сообщить об изменениях: если получатель сменил адрес, он должен иметь возможность это указать. Наконец — реакция на обращения: если человек сообщил о неточности, оператор проверяет и исправляет сведения, а на время проверки при необходимости блокирует их.

Закон даёт субъекту право требовать уточнения своих персональных данных, если они неполные, устаревшие или неточные. Оператор обязан в установленный законом срок внести изменения или уничтожить такие данные, если они являются незаконно полученными или не являются необходимыми для заявленной цели, и уведомить человека о принятых мерах. Если данные ранее передавались третьим лицам, разумно сообщить им об уточнении, чтобы ошибка не продолжала жить в других системах.

Достаточность — обратная сторона минимизации. Принцип не требует собирать как можно меньше любой ценой; он требует собирать столько, сколько нужно. Если для доставки нужен подъезд и этаж, их отсутствие в заявке делает данные недостаточными. Здесь важен баланс: достаточно для цели, но не больше.

Типичные ошибки организаций: отсутствие механизма для исправления данных пользователем; игнорирование сообщений «это не мой номер, перестаньте мне звонить»; хранение нескольких противоречивых версий одних и тех же сведений в разных системах; ручной перенос данных из одного места в другое с опечатками. Особенно неприятная ситуация — когда звонки и сообщения, предназначенные одному человеку, годами получает другой, потому что номер в базе никто не исправил.

Для человека этот принцип означает право требовать исправления. Если человек обнаружил, что о нём записаны неверные сведения, или что его данные используются по ошибке вместо данных другого лица, он вправе обратиться к оператору. Полезно в обращении указать, какие именно сведения неверны и какими они должны быть, — это ускоряет исправление.

Хранение не дольше, чем этого требуют цели, и уничтожение по достижении целей

Седьмой принцип состоит из двух связанных частей. Первая: хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта, не дольше, чем этого требуют цели обработки, если срок хранения не установлен федеральным законом или договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект. Вторая: обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено законом.

Смысл принципа в том, что у каждой обработки есть конец. Данные собирают для цели, и когда цель достигнута или стала неактуальной, основания хранить их в форме, позволяющей узнать человека, больше нет. Письмо доставлено, вопросы по ней закрыты — сведения о получателе, которые нужны

были только для доставки, по истечении разумного срока не должны лежать бесконечно. Кандидату отказано и он не дал согласия на включение в резерв — его анкету следует уничтожить.

Почему это важно. Бессрочное хранение — накопленный риск. Чем дольше и больше организация хранит, тем больше людей пострадает при утечке, тем сложнее поддерживать данные в актуальном состоянии, тем больше соблазн использовать их для новых, не заявленных целей. Многие крупные утечки затрагивали сведения людей, которые много лет назад перестали быть клиентами и давно забыли о существовании организации.

На практике оператор устанавливает сроки хранения для каждой цели обработки и предусматривает порядок уничтожения. Сроки могут определяться законом (например, для бухгалтерских и кадровых документов действуют обязательные сроки хранения), договором или самой целью. Конкретные сроки, применяемые Оператором, указываются в Политике; в этом справочном приложении они не приводятся. Важно, что по истечении срока данные не просто «лежат без дела», а действительно уничтожаются или обезличиваются, и это подтверждается в установленном порядке.

Обезличивание названо в законе как альтернатива уничтожению. Это позволяет сохранять полезную статистику, например сколько заказов было выполнено в определённом районе, без сведений, позволяющих узнать конкретных людей. Но, как отмечалось в Приложении 1, обезличивание должно быть настоящим: если таблица соответствия сохраняется и личность легко восстановить, цель принципа не достигнута.

Отдельные ситуации прямо предусмотрены законом. При отзыве согласия оператор прекращает обработку и уничтожает данные, если не вправе продолжать её на ином законном основании. При выявлении неправомерной обработки, которую невозможно сделать правомерной, данные уничтожаются. Закон устанавливает сроки для таких действий; как правило, они исчисляются днями, а не месяцами, и об уничтожении оператор уведомляет субъекта, если тот обращался.

Типичные ошибки организаций: отсутствие каких-либо сроков хранения («храним всё, вдруг пригодится»); удаление из основной системы при сохранении данных в выгрузках, почтовых ящиках и личных файлах сотрудников; забытые архивы на старых компьютерах и флешках; переписка с кандидатами в мессенджерах, которая сохраняется годами; резервные копии, хранящиеся бесконечно. Ещё одна ошибка — уничтожение без фиксации: если человек спросит, удалены ли его данные, организация не сможет это подтвердить.

Для человека этот принцип означает, что его сведения не должны храниться вечно. Он вправе спросить, как долго хранятся его данные и на каком основании, а когда цель обработки исчерпана — требовать их уничтожения. Например, человек, который однажды откликнулся на вакансию курьера, но так и не стал сотрудником, вправе ожидать, что его анкета не будет храниться годами без его согласия.

Как принципы работают вместе

Перечисленные принципы не существуют по отдельности: они образуют единую логику. Всё начинается с законного основания и честного информирования человека. Затем определяется конкретная цель. Цель задаёт границы: какие данные нужны, в каком объёме, кто должен иметь к ним доступ, с какими другими базами их можно или нельзя связывать. Пока цель достигается, данные поддерживаются точными и актуальными. Когда цель достигнута, данные уничтожаются или обезличиваются.

Удобно представить жизненный цикл данных на примере анкеты кандидата. Человек видит на сайте описание того, кто и зачем будет обрабатывать его сведения, — законность и справедливость. Анкета

служит рассмотрению кандидатуры на конкретную вакансию — конкретная цель. Анкета хранится отдельно от клиентских заказов — запрет объединения несовместимых баз. В ней только вопросы, нужные для оценки и связи, — соответствие целям и отсутствие избыточности. Если кандидат сообщил новый номер, его обновляют — точность и актуальность. Когда решение принято и иное основание хранения отсутствует, анкету уничтожают — ограничение срока хранения.

Помимо принципов статьи 5, закон устанавливает обязанности оператора по обеспечению безопасности персональных данных, по ответам на запросы субъектов, по взаимодействию с уполномоченным органом. Принципы задают направление, а обязанности — конкретные действия. Для понимания того, как Оператор применяет эти принципы в своей деятельности, следует обращаться к соответствующим разделам Политики: о целях обработки, о категориях данных, об основаниях, о сроках, о мерах защиты и о порядке рассмотрения обращений.

Что полезно помнить человеку

Знание принципов обработки персональных данных помогает человеку уверенно вести себя в повседневных ситуациях. Перед тем как заполнить форму, стоит посмотреть, есть ли ссылка на Политику и понятно ли, зачем нужны сведения. Если просят слишком много, разумно уточнить, зачем. Если данные оказались неверными, следует попросить исправить. Если отношения с организацией закончились, можно поинтересоваться, хранятся ли ещё данные и на каком основании.

Важно также различать добросовестного оператора и мошенника. Добросовестная организация не торопит, объясняет назначение каждого запроса, не просит пароли и коды из SMS, предлагает защищённые способы передачи документов и даёт понятный канал для обращений. Мошенник, наоборот, давит срочностью, просит всё и сразу, предлагает переслать документы в личные сообщения незнакомому аккаунту и не может толком объяснить, кто он такой. Принципы закона — удобный ориентир, чтобы отличить одно от другого.

Наконец, если человек считает, что его права нарушены, у него есть несколько путей: обратиться к оператору по контактам, указанным в Политике; обратиться в уполномоченный орган по защите прав субъектов персональных данных; обратиться в суд, в том числе с требованием о возмещении убытков и компенсации морального вреда. Выбор пути зависит от ситуации, но знание своих прав и принципов, на которых должна строиться обработка, делает любой из этих шагов более уверенным и результативным.

Приложение 3. Права субъекта персональных данных: подробные разъяснения

Справочный материал. Не является частью Политики и не устанавливает обязательств Оператора. Сведения о том, какие данные обрабатывает Оператор, в каких целях и в какие сроки, содержатся только в Политике (раздел I).

Это приложение носит справочный и просветительский характер. Оно не является частью Политики обработки персональных данных, не изменяет и не дополняет её положений и не устанавливает для Оператора или для граждан каких-либо новых обязанностей. Его задача скромнее и практичнее: простым языком рассказать человеку, чьи сведения обрабатываются, какие права даёт ему российское законодательство о персональных данных, как этими правами пользоваться и чего разумно ожидать в ответ. Основным источником здесь служит Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных» в действующей редакции, а также общие нормы гражданского и процессуального права.

Чтобы текст не оставался абстрактным, в нём используются бытовые примеры. Чаще всего это два собирательных персонажа. Первый — кандидат на работу курьером: он увидел объявление, оставил отклик, переписывался с рекрутером, заполнял анкету, возможно, присылал фото документов. Второй — посетитель сайта: он заходил на страницы службы доставки, оформлял заявку или отслеживал заказ, оставлял телефон для обратного звонка, а его браузер при этом передавал технические сведения. Примеры условные и не описывают реальные процедуры конкретной компании; они нужны лишь для того, чтобы показать, как общие нормы закона работают в обычной жизни.

Важная оговорка: законодательство меняется, а правоприменительная практика уточняет смысл норм. Если речь идёт о серьёзном споре, о крупных суммах или о чувствительных сведениях, разумно свериться с актуальным текстом закона и при необходимости получить консультацию юриста. Настоящее приложение не заменяет юридическую помощь в конкретной ситуации.

Кто такой субъект персональных данных и почему у него есть права

Персональные данные — это любая информация, которая прямо или косвенно относится к определённом или определяемому физическому лицу. Само это лицо закон называет субъектом персональных данных. Фамилия и имя, номер телефона, адрес электронной почты, дата рождения, сведения о прежних местах работы, фотография, номер паспорта, а в ряде случаев и сочетание технических данных, по которому можно вычислить конкретного человека, — всё это может быть персональными данными.

Оператором называется тот, кто организует и (или) осуществляет обработку персональных данных и определяет её цели, состав данных и действия с ними. Когда кандидат откликается на вакансию курьера, оператор — это работодатель или компания, которая ведёт набор. Когда посетитель оставляет заявку на сайте, оператор — владелец сайта, который решает, зачем ему эти сведения и что с ними делать.

Отношения между субъектом и оператором неравны по информации: оператор знает, что он хранит, где и зачем, а человек часто не знает даже того, что его данные куда-то попали. Права субъекта, закреплённые законом, призваны выровнять эту асимметрию. Они позволяют узнать, что происходит с данными, исправить ошибки, прекратить обработку, которая больше не нужна или незаконна, и, в крайнем случае, защититься через государственный орган или суд.

Права субъекта не зависят от того, является ли человек клиентом, работником, кандидатом или

случайным посетителем сайта. Не нужно быть стороной договора, чтобы спросить оператора, какие сведения о вас у него есть. Достаточно того, что оператор, по мнению человека, обрабатывает его персональные данные.

Закон исходит из принципа добросовестности обработки. Оператор должен обрабатывать только те данные, которые соответствуют заявленным целям, не собирать лишнего, хранить сведения не дольше, чем нужно, и обеспечивать их точность. Права субъекта во многом служат инструментом контроля за соблюдением этих принципов: человек как бы получает возможность самостоятельно проверить, соблюдаются ли они в отношении именно его сведений.

Право на доступ к сведениям об обработке

Первое и, пожалуй, базовое право — право знать. Закон предоставляет субъекту право на получение сведений, касающихся обработки его персональных данных. Без этой информации невозможно воспользоваться остальными правами: нельзя потребовать исправить то, о чём не знаешь, и нельзя оценить законность обработки, если неизвестны её цели и основания.

Согласно статье 14 Закона о персональных данных, по запросу субъекта оператор обязан сообщить, в частности, следующие сведения:

- подтверждение факта обработки персональных данных оператором;
- правовые основания и цели обработки персональных данных;
- цели и применяемые оператором способы обработки персональных данных;
- наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;
- обрабатываемые персональные данные, относящиеся к соответствующему субъекту, и источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- сроки обработки персональных данных, в том числе сроки их хранения;
- порядок осуществления субъектом прав, предусмотренных законом;
- информацию об осуществлённой или о предполагаемой трансграничной передаче данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;
- информацию о способах исполнения оператором обязанностей по обеспечению безопасности и законности обработки, установленных законом;
- иные сведения, предусмотренные Законом о персональных данных или другими федеральными законами.

Рассмотрим, как это выглядит на практике. Кандидат на должность курьера несколько недель назад откликнулся на объявление, пообщался в чате, а потом передумал. Через месяц ему звонят с другого номера и предлагают «вернуться к оформлению». Он вправе спросить оператора: какие именно сведения о нём хранятся, откуда они получены (из отклика, из резюме на сайте объявлений, от знакомого), с какой целью и на каком основании они обрабатываются, сколько их собираются хранить и кому они передавались. Ответ на эти вопросы позволит ему понять, нужно ли что-то исправить или прекратить.

Посетитель сайта находится в похожем положении. Он оставил номер телефона в форме обратного

звонка и хочет понять, используется ли этот номер только для ответа на заявку или также для рассылок, передаётся ли он сервисам аналитики, хранится ли после выполнения заявки. Право на доступ даёт ему законный способ получить эти ответы, а не гадать.

Сведения должны быть предоставлены в доступной форме. Закон прямо указывает, что в них не должны содержаться персональные данные, относящиеся к другим субъектам, за исключением случаев, когда имеются законные основания для их раскрытия. Например, если в переписке с кандидатом упоминались сведения о другом человеке, оператор не обязан и не вправе раскрывать их в ответе на запрос, но должен сообщить всё, что касается самого заявителя.

Субъект вправе обратиться за сведениями повторно. По общему правилу закона повторный запрос о тех же сведениях можно направить не ранее чем через тридцать дней после первоначального обращения, если более короткий срок не установлен федеральным законом, нормативным правовым актом или договором. Однако если в ответ на первый запрос сведения были предоставлены не в полном объёме, человек может обратиться повторно и раньше, обосновав причину повторного обращения. Оператор вправе отказать в выполнении повторного запроса, не соответствующего этим условиям, но такой отказ должен быть мотивированным, а обязанность доказать его обоснованность лежит на операторе.

Сведения можно получить как лично, так и через представителя, а также в ответ на письменный запрос или запрос в форме электронного документа. Подробнее о том, как составить запрос, рассказано в Приложении 4.

Важно понимать, чем право на доступ не является. Оно не обязывает оператора передавать человеку внутренние документы, не связанные с его данными, раскрывать коммерческую тайну или описывать технические меры защиты в такой детализации, которая сама по себе создаёт угрозу безопасности. Речь идёт о сведениях, касающихся обработки данных конкретного человека. Вместе с тем общие сведения о мерах защиты и о способах исполнения обязанностей оператора закон относит к информации, которую субъект вправе получить.

Право на доступ полезно использовать не только при подозрении на нарушение. Это нормальный инструмент «гигиены»: раз в какое-то время можно поинтересоваться у организаций, с которыми вы взаимодействовали, что у них о вас осталось. Часто такой запрос сам по себе побуждает оператора навести порядок и удалить то, что хранить уже не нужно.

Право на уточнение, блокирование и уничтожение

Получив сведения, человек может обнаружить, что они неточны, устарели, неполны или вообще не должны обрабатываться. На этот случай закон даёт право требовать от оператора уточнения персональных данных, их блокирования или уничтожения, если данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

Уточнение — это исправление или дополнение данных. Простой пример: в анкете кандидата допущена опечатка в номере телефона, и все сообщения уходят чужому человеку. Или кандидат сменил фамилию после вступления в брак. Или в форме на сайте был указан старый адрес доставки. Во всех этих случаях человек вправе потребовать, чтобы оператор привёл сведения в соответствие с действительностью. По действующей редакции закона, если субъект представил сведения, подтверждающие неполноту, неточность или неактуальность данных, оператор обязан внести необходимые изменения в течение семи рабочих дней со дня представления таких сведений.

Блокирование — это временное прекращение обработки, за исключением случаев, когда обработка необходима для уточнения данных. Его смысл в том, чтобы «заморозить» сведения на время проверки. Например, человек сообщает, что его данные обрабатываются без законного основания, или что они неточны, а оператору нужно время, чтобы разобраться. На этот период данные не должны использоваться: по ним не звонят, их не передают, не принимают на их основе решений. Закон обязывает оператора блокировать данные с момента обращения субъекта или его представителя в случаях выявления неправомерной обработки или неточных данных, если это не нарушает прав и законных интересов субъекта или третьих лиц.

Уничтожение — это действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе и (или) в результате которых уничтожаются материальные носители данных. Важно отличать уничтожение от простого «скрытия» записи в интерфейсе или перемещения файла в корзину. Закон говорит именно о невозможности восстановления содержания.

Когда возникает обязанность уничтожить данные? Если сведения получены незаконно или не являются необходимыми для заявленной цели обработки, оператор при подтверждении этого обязан их уничтожить; закон связывает с такими ситуациями сроки в несколько рабочих дней. Если выявлена неправомерная обработка и обеспечить её правомерность невозможно, оператор должен уничтожить данные или обеспечить их уничтожение в течение десяти рабочих дней с даты выявления. При достижении целей обработки, а также при отзыве согласия по общему правилу данные подлежат уничтожению в течение тридцати дней, если иное не предусмотрено договором, иным соглашением или федеральным законом. Об уничтожении и о других принятых мерах оператор должен уведомить субъекта.

Пример с кандидатом. Человек откликнулся на вакансию курьера, прошёл собеседование, но решил не выходить на работу. Через полгода он узнаёт, что копия его паспорта по-прежнему хранится у оператора, хотя никаких отношений не возникло. Если цель обработки (рассмотрение кандидатуры) достигнута, а иных законных оснований хранить копию нет, кандидат вправе потребовать уничтожения. При этом стоит учитывать, что отдельные документы оператор может быть обязан хранить по требованию закона, например, если отношения всё-таки возникли и действуют правила о хранении кадровых или бухгалтерских документов. В таком случае оператор должен объяснить основание и срок хранения.

Пример с посетителем сайта. Человек когда-то подписался на уведомления или оставил контакты для акции, а теперь не хочет, чтобы его номер хранился. Если номер больше не нужен для исполнения заказа и не требуется хранить его по закону, посетитель вправе требовать прекращения обработки и уничтожения.

Стоит различать ситуации, когда человек просит удалить данные, и когда оператор продолжает их обрабатывать на ином законном основании. Закон о персональных данных знает несколько оснований обработки помимо согласия: исполнение договора, стороной которого является субъект; исполнение обязанностей, возложенных законом на оператора; защита жизни и здоровья; осуществление прав и законных интересов оператора или третьих лиц при условии, что не нарушаются права субъекта, и другие. Если такое основание действительно есть, требование уничтожения может быть удовлетворено не полностью — но оператор должен это обосновать, а не просто проигнорировать просьбу.

Удобно формулировать требование конкретно: какие именно сведения, по вашему мнению, неточны и каковы верные; какие сведения, по вашему мнению, не нужны для целей обработки; какие действия вы

просите совершить. Чем точнее запрос, тем меньше пространства для формального ответа и тем быстрее можно добиться результата.

Право на отзыв согласия и его последствия

Согласие на обработку персональных данных — одно из оснований обработки, но не единственное. Закон требует, чтобы согласие было конкретным, предметным, информированным, сознательным и однозначным. Человек даёт его свободно, своей волей и в своём интересе. Логичное продолжение этой свободы — право в любой момент отозвать согласие.

Отзыв согласия не требует объяснения причин. Кандидат может просто написать, что больше не желает, чтобы его данные обрабатывались в целях подбора персонала. Посетитель сайта может отозвать согласие на получение рекламных сообщений или на обработку данных для аналитики, если такая обработка основана на согласии.

Что происходит после отзыва? По общему правилу оператор обязан прекратить обработку персональных данных или обеспечить её прекращение, если обработку ведёт другое лицо по поручению оператора. Если сохранение данных больше не требуется для целей обработки, оператор обязан уничтожить их или обеспечить уничтожение в срок, не превышающий тридцати дней с даты поступления отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект, иным соглашением между оператором и субъектом либо если оператор не вправе осуществлять обработку без согласия на основаниях, предусмотренных законом.

Здесь кроется важная тонкость, о которой часто не знают. Закон прямо допускает, что в случае отзыва согласия оператор вправе продолжить обработку без согласия при наличии иных оснований, указанных в законе. Например, если между кандидатом и компанией уже заключён договор, данные, необходимые для его исполнения, будут обрабатываться на основании договора, а не согласия. Если закон обязывает хранить определённые документы, их хранение продолжится. Отзыв согласия в этом случае прекратит лишь ту часть обработки, которая держалась исключительно на согласии.

Пример. Курьер работал по договору, затем отношения прекратились, и он отзывает согласие. Сведения, которые обрабатывались только ради, скажем, приглашений на новые вакансии или рассылок, должны быть прекращены к использованию. А вот документы, которые обязательно хранить по налоговому, бухгалтерскому или трудовому законодательству (если такие отношения были), оператор сохранит до истечения установленного срока, но не будет использовать их в иных целях.

Последствия отзыва согласия могут затронуть и самого человека. Если обработка данных была необходима для оказания услуги или для рассмотрения кандидатуры, после отзыва оператор, скорее всего, не сможет продолжить это взаимодействие. Кандидат, отозвавший согласие на обработку анкеты, фактически выходит из процесса отбора. Посетитель, отозвавший согласие на обработку телефона, больше не получит обратного звонка. Это не наказание, а естественное следствие: без данных невозможно выполнить действия, для которых они нужны.

Отзыв согласия не имеет обратной силы. Обработка, которая велась до отзыва на законном основании, не становится незаконной задним числом. Отзыв действует на будущее.

Отозвать согласие можно в той же форме, в которой оно давалось, либо в письменной форме или в форме электронного документа. Практически полезно сделать это так, чтобы у вас осталось подтверждение отправки: копия письма с отметкой о получении, квитанция почтового отправления, сохранённое электронное письмо или скриншот обращения через официальный канал. Если оператор

предоставил специальный механизм отзыва, например ссылку «отписаться» в рассылке, им тоже можно воспользоваться, но для серьёзных случаев лучше дополнительно направить полноценное письменное заявление.

Отдельно стоит упомянуть ситуацию, когда человек требует не отзыва согласия как такового, а прекращения обработки. В действующей редакции закона предусмотрено, что по требованию субъекта о прекращении обработки оператор обязан прекратить её в срок, не превышающий десяти рабочих дней с даты получения требования, с возможностью продления на пять рабочих дней при направлении субъекту мотивированного уведомления — за исключением случаев, прямо указанных в законе. На практике эти два инструмента часто используют вместе: «отзываю согласие и требую прекратить обработку».

Права при обработке в целях продвижения товаров, работ, услуг

Отдельные правила закон устанавливает для обработки персональных данных в целях продвижения товаров, работ, услуг на рынке путём осуществления прямых контактов с потенциальным потребителем с помощью средств связи, а также в целях политической агитации. Речь о звонках, сообщениях, письмах, рассылках, через которые человеку что-либо предлагают.

Статья 15 Закона о персональных данных устанавливает, что такая обработка допускается только при условии предварительного согласия субъекта. При этом обработка считается осуществляемой без предварительного согласия, если оператор не докажет, что такое согласие было получено. Иными словами, бремя доказывания лежит на том, кто рассылает, а не на том, кто получает.

Оператор обязан немедленно прекратить по требованию субъекта обработку его данных в этих целях. Слово «немедленно» здесь существенно: в отличие от других случаев, закон не даёт оператору нескольких рабочих дней на раздумья.

Пример с посетителем сайта. Человек однажды заказал доставку и оставил номер. Теперь ему регулярно приходят сообщения с предложениями услуг. Если он не давал согласия на получение рекламы, такая рассылка не основана на законе. Если давал, но больше не хочет её получать, он может потребовать прекратить рассылку, и оператор должен это сделать сразу.

Пример с кандидатом. Человек откликнулся на вакансию, но не стал работать. Затем он начинает получать предложения о других вакансиях, акции, приглашения на мероприятия. Здесь важно разобраться, какую цель преследуют сообщения. Если это продвижение услуг или иных предложений, на них распространяются правила о предварительном согласии. Кандидат вправе потребовать прекратить такие контакты.

Помимо Закона о персональных данных, рекламные рассылки регулируются законодательством о рекламе. Оно также требует предварительного согласия абонента на получение рекламы по сетям электросвязи и обязывает рекламораспространителя прекратить рассылку по требованию. Нарушения могут проверяться антимонопольным органом. Таким образом, у человека есть два параллельных пути защиты: по линии персональных данных и по линии рекламы.

Практический совет: при требовании прекратить рекламные контакты укажите, с какого номера или адреса приходят сообщения, примерные даты и содержание, а также ваш номер или адрес, на который они поступают. Это облегчит оператору поиск записей и снизит риск того, что ваша просьба «потеряется». Если рассылка продолжается после требования, сохраните доказательства: скриншоты с датами, записи звонков (с соблюдением закона), детализацию.

Стоит различать рекламу и служебные сообщения. Уведомления о статусе заказа, подтверждение записи на собеседование, напоминание о встрече, которую человек сам назначил, обычно не являются продвижением товаров и услуг и связаны с исполнением договора или с запросом самого человека. Однако если в служебное сообщение «подмешивается» реклама, к этой части применимы правила о согласии.

Права при принятии решений на основании исключительно автоматизированной обработки

Всё больше решений принимается с участием алгоритмов: автоматически сортируются отклики, ранжируются резюме, оценивается вероятность того, что кандидат подойдёт, программы ведут первичную переписку. Закон о персональных данных содержит специальную норму на этот случай — статью 16.

Общее правило таково: запрещается принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта или иным образом затрагивающих его права и законные интересы. Исключения — случаи, когда имеется согласие в письменной форме субъекта или когда это предусмотрено федеральными законами, устанавливающими также меры по обеспечению соблюдения прав и законных интересов субъекта.

Ключевое слово здесь — «исключительно». Если алгоритм лишь помогает человеку, например подготавливает черновик ответа, сортирует обращения или подсвечивает информацию, а окончательное решение принимает сотрудник, это не решение «на основании исключительно автоматизированной обработки». Если же программа сама, без участия человека, отклоняет кандидатуру, блокирует доступ или отказывает в услуге, такое решение подпадает под ограничения закона.

Если решение всё-таки принимается автоматически на законном основании, оператор обязан разъяснить субъекту порядок принятия такого решения и возможные юридические последствия, предоставить возможность заявить возражение против такого решения, а также разъяснить порядок защиты субъектом своих прав и законных интересов. Возражение оператор обязан рассмотреть в установленный законом срок и уведомить человека о результатах.

Пример с кандидатом. Человек заполнил анкету и через минуту получил автоматический отказ «по результатам анализа». Он вправе спросить, принималось ли решение исключительно автоматически, на каком основании, по какой логике, и заявить возражение. Если окажется, что отказ стал следствием ошибки в данных, например неправильно распознанной даты рождения или неверно указанного города, кандидат может одновременно потребовать уточнения сведений.

Пример с посетителем. Сайт автоматически отказывает в оформлении заявки на основании технических признаков, скажем, из-за адреса или из-за «подозрительного» поведения. Если такой отказ затрагивает права человека, он может поинтересоваться, как принято решение, и потребовать рассмотрения его ситуации человеком.

Следует понимать, что закон не запрещает автоматизацию как таковую. Он защищает от ситуации, когда значимое для человека решение принимает «чёрный ящик» без возможности объясниться и быть услышанным. Поэтому правильный вопрос к оператору звучит не «почему вы используете программы», а «участвовал ли в принятии решения человек, как я могу оспорить решение и кто его пересмотрит».

Право на возражение против автоматизированного решения не означает автоматической отмены решения. Оператор рассматривает возражение по существу. Но человек вправе ожидать, что его доводы будут изучены, а не отклонены очередным шаблонным ответом.

Право на обжалование в Роскомнадзор и в суд

Если оператор не отвечает на запрос, отвечает формально, отказывает без оснований или продолжает обработку, которую человек считает незаконной, закон даёт два основных пути защиты: обращение в уполномоченный орган по защите прав субъектов персональных данных и обращение в суд. Статья 17 Закона о персональных данных прямо закрепляет: если субъект считает, что оператор осуществляет обработку его данных с нарушением требований закона или иным образом нарушает его права и свободы, он вправе обжаловать действия или бездействие оператора в уполномоченный орган или в судебном порядке.

Уполномоченным органом в России является Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций — Роскомнадзор, включая его территориальные управления. Он рассматривает обращения субъектов, проверяет содержащиеся в них сведения и принимает меры в пределах своей компетенции: может потребовать от оператора уточнить, заблокировать или уничтожить недостоверные или незаконно полученные данные, принять меры по приостановлению или прекращению обработки, а также привлечь виновных к ответственности в установленном порядке или направить материалы для этого.

Как правило, обращения граждан рассматриваются по общим правилам, установленным для обращений в государственные органы; общий срок рассмотрения письменного обращения составляет тридцать дней со дня регистрации, с возможностью продления в исключительных случаях. Обращение можно подать письменно или в электронной форме через официальные каналы ведомства. В нём стоит описать суть нарушения, указать оператора, приложить копии своих запросов к оператору и полученных ответов (или доказательства того, что ответа не было).

Нужно ли сначала обращаться к оператору? Закон не делает это строго обязательным условием для обращения в надзорный орган, однако на практике предварительное обращение к оператору очень полезно. Во-первых, многие проблемы решаются уже на этом этапе. Во-вторых, наличие запроса и отсутствие ответа или неудовлетворительный ответ — это наглядное доказательство нарушения, которое облегчит работу надзорного органа.

Судебная защита — второй путь. В суд можно обратиться с требованием признать действия оператора незаконными, обязать его совершить определённые действия (предоставить сведения, уточнить, уничтожить данные, прекратить обработку), а также взыскать убытки и компенсацию морального вреда. Споры между гражданином и организацией рассматриваются судами общей юрисдикции по правилам гражданского судопроизводства. Процессуальное законодательство допускает предъявление исков о защите прав субъекта персональных данных, в том числе о возмещении убытков и компенсации морального вреда, также по месту жительства истца; конкретную подсудность в своей ситуации лучше уточнить по актуальному тексту закона.

Два пути не исключают друг друга. Человек может одновременно обратиться в Роскомнадзор и в суд либо последовательно: сначала в надзорный орган, а затем, получив результат проверки, в суд, используя материалы проверки как доказательства. Административная ответственность оператора (например, по статье 13.11 Кодекса об административных правонарушениях, посвящённой нарушениям законодательства о персональных данных) — это публичная мера, которая не заменяет гражданско-

правовой компенсации самому пострадавшему. Денежная компенсация человеку присуждается судом.

Пример. Кандидат дважды направлял запрос о том, какие его данные хранятся, и не получил ответа в установленный срок. Он собрал копии запросов и доказательства их отправки, приложил их к обращению в территориальное управление Роскомнадзора. Параллельно, если бездействие причинило ему ощутимые неудобства или ущерб, он вправе обратиться в суд.

Совет по доказательствам: храните всё. Копии запросов, почтовые квитанции и уведомления о вручении, электронные письма с заголовками, скриншоты страниц сайта с датой, тексты согласий, которые вы давали, записи о звонках и сообщениях. В спорах о персональных данных выигрывает тот, кто может показать хронологию событий документально.

Право на возмещение убытков и компенсацию морального вреда

Закон о персональных данных прямо устанавливает, что субъект имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке. Кроме того, статья 24 закона уточняет, что моральный вред, причинённый субъекту вследствие нарушения его прав, нарушения правил обработки персональных данных, а также требований к защите данных, подлежит возмещению в соответствии с законодательством. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесённых субъектом убытков.

Убытки — это имущественные потери. Гражданское законодательство понимает под ними реальный ущерб (расходы, которые лицо произвело или должно будет произвести для восстановления нарушенного права, утрата или повреждение имущества) и упущенную выгоду (неполученные доходы, которые лицо получило бы при обычных условиях оборота, если бы право не было нарушено). Например, если из-за утечки данных мошенники оформили на человека заём, а он понёс расходы на юриста и восстановление документов, это может стать предметом требования о возмещении убытков, если удастся доказать связь с действиями оператора.

Моральный вред — это физические или нравственные страдания. Нарушение неприкосновенности частной жизни, тревога из-за того, что паспортные данные оказались в чужих руках, неприятные звонки и навязчивые контакты, раскрытие сведений перед знакомыми или коллегами — всё это может причинять нравственные страдания. Размер компенсации определяет суд с учётом характера страданий, степени вины нарушителя, требований разумности и справедливости.

Что нужно доказать? По общим правилам: факт нарушения (незаконная обработка, утечка, игнорирование требований), наличие вреда (для убытков — его размер; для морального вреда — характер страданий), причинную связь между нарушением и вредом. В части вины действуют общие правила гражданского законодательства. Для компенсации морального вреда по делам о персональных данных суды обычно исходят из того, что сам факт нарушения прав субъекта уже свидетельствует о причинении нравственных переживаний, однако размер компенсации зависит от обстоятельств.

Пример с кандидатом. Человек направил копию паспорта для оформления, а затем обнаружил, что фото документа было переслано в посторонний чат без его ведома. Он испытывает тревогу, вынужден менять номер телефона, тратит время на проверку кредитной истории. Здесь можно говорить и о моральном вреде, и, при наличии подтверждённых расходов, об убытках.

Пример с посетителем. Номер телефона, оставленный в форме на сайте, оказался в рекламных базах, и на человека обрушился поток звонков. Если удастся связать это с действиями конкретного оператора, требование компенсации морального вреда будет вполне обоснованным.

Важно трезво оценивать перспективы. Суды в России, как правило, присуждают по таким делам умеренные суммы компенсации морального вреда, и размер сильно зависит от обстоятельств. Тем не менее судебное решение важно не только деньгами: оно фиксирует факт нарушения и побуждает оператора пересмотреть свои процессы.

Перед подачей иска полезно направить оператору претензию с изложением требований и предложением урегулировать спор добровольно. Это не всегда обязательно, но часто помогает и демонстрирует суду добросовестность заявителя.

Ограничения права доступа, предусмотренные законом

Право на доступ к своим данным не абсолютно. Закон допускает его ограничение в ряде случаев, чтобы защитить важные публичные интересы или права других людей. Знать об этих ограничениях полезно, чтобы правильно оценивать ответ оператора и понимать, когда отказ может быть законным, а когда — нет.

Закон о персональных данных предусматривает, что право субъекта на доступ может быть ограничено в соответствии с федеральными законами, в частности, если обработка данных осуществляется в целях обороны страны, безопасности государства и охраны правопорядка; если обработка осуществляется органами, задержавшими лицо по подозрению в совершении преступления или предъявившими обвинение, за исключением случаев, предусмотренных уголовно-процессуальным законодательством; если обработка ведётся в соответствии с законодательством о противодействии легализации преступных доходов и финансированию терроризма; если доступ нарушает права и законные интересы третьих лиц; если обработка осуществляется в случаях, предусмотренных законодательством о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса.

Для обычной курьерской службы и её сайта большинство этих оснований вряд ли актуальны в повседневной жизни: компания доставки — не правоохранительный орган и не спецслужба. Наиболее практически значимое ограничение — защита прав и законных интересов третьих лиц. Если в данных, которые хранит оператор, содержатся сведения о других людях, оператор должен предоставить заявителю его сведения, но не раскрывать чужие.

Пример. Кандидат запрашивает переписку с рекрутёром, в которой есть упоминания других кандидатов, их имена и телефоны. Оператор вправе и обязан скрыть или исключить сведения о третьих лицах, но не вправе на этом основании отказать в раскрытии сведений о самом кандидате.

Ещё один пример. Посетитель сайта запрашивает данные о заказе, который оформлял другой человек на его адрес. Если сведения касаются заказчика, а не посетителя, оператор не обязан их раскрывать, поскольку это затронет права заказчика.

Любое ограничение права доступа должно быть основано на законе, а не на удобстве оператора. Ответ «это внутренняя информация» или «мы не раскрываем такие сведения» без ссылки на конкретное законное основание не является надлежащим. Если оператор отказывает в предоставлении сведений, он должен дать мотивированный ответ со ссылкой на положение закона, являющееся основанием для отказа, в установленный законом срок.

Если человек не согласен с отказом, он может оспорить его в надзорном органе или в суде. При этом бремя доказывания законности отказа, как правило, лежит на операторе.

Наконец, ограничения доступа не отменяют других прав субъекта. Даже если какие-то сведения не

могут быть раскрыты, человек сохраняет право на защиту от незаконной обработки, право требовать уточнения недостоверных данных в пределах, допускаемых законом, право обжалования и право на компенсацию вреда.

Права при трансграничной передаче персональных данных

Трансграничная передача — это передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу. В повседневной жизни она может происходить незаметно: при использовании зарубежных облачных сервисов, почтовых сервисов, систем аналитики, платформ искусственного интеллекта, сервисов рассылок, хостинга, расположенного за рубежом.

Российское законодательство в последние годы существенно ужесточило правила такой передачи. Оператор, прежде чем начать трансграничную передачу, по общему правилу обязан уведомить об этом Роскомнадзор, а также до подачи уведомления получить от иностранных получателей определённые сведения о мерах защиты данных и об условиях прекращения обработки. Роскомнадзор вправе запретить или ограничить передачу. Кроме того, действует требование о локализации: при сборе персональных данных граждан России, в том числе через интернет, запись, систематизация, накопление, хранение, уточнение и извлечение должны осуществляться с использованием баз данных, находящихся на территории России, за исключением отдельных случаев, предусмотренных законом.

Для субъекта это означает несколько практических прав. Во-первых, он вправе знать, осуществлялась ли или предполагается ли трансграничная передача его данных. Это прямо входит в перечень сведений, которые оператор обязан сообщить по запросу. Во-вторых, если передача осуществляется в государства, не обеспечивающие адекватной защиты прав субъектов, закон в ряде случаев требует письменного согласия субъекта; без него такая передача по этому основанию невозможна. В-третьих, человек может отозвать согласие, если передача основана на нём.

Пример с кандидатом. Анкета, заполненная кандидатом, обрабатывается с помощью сервиса, серверы которого находятся за рубежом, например для автоматического анализа текста. Кандидат вправе спросить оператора, передаются ли его данные за границу, в какие страны, кому и на каком основании.

Пример с посетителем сайта. На сайте установлены зарубежные счётчики посещаемости или чат-виджеты. Если через них передаются сведения, позволяющие идентифицировать посетителя, это тоже может быть трансграничной передачей. Посетитель вправе поинтересоваться этим и, если обработка основана на согласии, отозвать его.

Если человек считает, что его данные передаются за рубеж с нарушением закона, он может обратиться в Роскомнадзор с указанием известных ему обстоятельств. Надзорный орган располагает сведениями об уведомлениях операторов о трансграничной передаче и может проверить, соблюдены ли требования.

Стоит помнить, что за рубежом защита данных может регулироваться иначе, а возможности российского гражданина по защите своих прав там ограничены. Именно поэтому закон уделяет столько внимания контролю на этапе передачи. Задавая вопросы оператору заранее, человек защищает себя лучше, чем пытаясь восстановить права постфактум.

Права в отношении персональных данных, разрешённых субъектом для распространения

С 2021 года в Законе о персональных данных появилась отдельная статья 10.1 о персональных данных, разрешённых субъектом для распространения. Речь о ситуациях, когда человек сам соглашается, чтобы

его сведения стали доступны неограниченному кругу лиц: например, разрешает опубликовать фото и имя на сайте, в отзывах, на доске почёта, в рекламных материалах или в социальных сетях компании.

Главное правило: согласие на распространение оформляется отдельно от иных согласий на обработку персональных данных. Его нельзя «спрятать» в общий текст согласия мелким шрифтом. Оператор обязан обеспечить субъекту возможность определить перечень данных по каждой категории, которые тот разрешает распространять.

Субъект вправе установить запреты на передачу (кроме предоставления доступа) этих данных неограниченному кругу лиц, а также запреты на обработку или условия обработки (кроме получения доступа) неограниченным кругом лиц. Например, можно разрешить опубликовать имя и фотографию на сайте компании, но запретить их дальнейшее копирование и использование другими лицами. Отказ оператора установить такие запреты и условия не допускается.

Молчание или бездействие субъекта ни при каких обстоятельствах не может считаться согласием на распространение. Если из согласия не следует, что человек разрешил распространять сведения, или не определены категории и перечень данных, по общему правилу такие данные обрабатываются без права распространения.

Человек в любое время может потребовать прекратить передачу (распространение, предоставление, доступ) своих персональных данных, ранее разрешённых для распространения. Требование должно содержать фамилию, имя, отчество (при наличии), контактную информацию (номер телефона, адрес электронной почты или почтовый адрес) субъекта, а также перечень данных, обработка которых подлежит прекращению. Указанные в требовании данные могут обрабатываться только оператором, которому оно направлено. Действие согласия прекращается с момента поступления требования оператору, и передача данных должна быть прекращена в течение трёх рабочих дней с момента получения требования.

Пример. Курьер согласился, чтобы его фотография и имя были размещены на странице «Наша команда» или в материалах о работе в компании. Позже он перешёл на другую работу и хочет, чтобы фотографию убрали. Он вправе направить требование, и оператор обязан прекратить распространение в короткий установленный законом срок.

Если данные распространяются с нарушением закона, человек также вправе обратиться с требованием о прекращении передачи к любому лицу, обрабатывающему его данные, а при неисполнении — в суд. Например, если его фотографию разместил на своём ресурсе посторонний сайт, скопировав её с сайта компании, требование можно направить напрямую этому сайту.

Важно разграничивать данные, разрешённые для распространения, и данные, которые человек сам сделал общедоступными без какого-либо согласия, например разместил резюме на публичной площадке. Закон после поправок 2021 года отказался от упрощённого подхода, при котором любые «общедоступные» данные можно было свободно использовать. Сам факт того, что ваше резюме видно на сайте вакансий, не означает, что любой может копировать его и использовать в любых целях; правовое основание обработки должно быть у каждого, кто это делает.

Особенности для несовершеннолетних и представителей

Права субъекта персональных данных принадлежат каждому человеку, независимо от возраста. Но порядок их осуществления для несовершеннолетних и для недееспособных лиц имеет особенности, связанные с общими правилами гражданского законодательства о дееспособности.

Закон о персональных данных предусматривает, что в случае недееспособности субъекта согласие на обработку его данных даёт законный представитель. Для несовершеннолетних законными представителями являются родители, усыновители, опекуны или попечители. В ряде ситуаций от имени ребёнка действуют именно они, в том числе направляют запросы и требования оператору.

Вопрос о том, с какого возраста подросток может самостоятельно давать согласие на обработку своих данных, в законе о персональных данных прямо не решён единой цифрой и зависит от характера отношений. Гражданское законодательство предоставляет несовершеннолетним от четырнадцати до восемнадцати лет право самостоятельно совершать ряд действий, например распоряжаться своим заработком, а трудовое законодательство допускает заключение трудового договора с лицами, достигшими определённого возраста, с соблюдением ограничений. На практике для серьёзных юридически значимых действий операторы, как правило, ориентируются на совершеннолетие или требуют участия законного представителя.

Для курьерских служб вопрос о несовершеннолетних кандидатах обычно возникает в контексте возрастных требований к работе. Если подросток всё же оставил отклик или заполнил анкету, его права как субъекта данных сохраняются в полном объёме: он и его законный представитель вправе узнать, какие данные собраны, потребовать их уточнения или уничтожения, отозвать согласие. Если согласие подростка оказалось недостаточным с точки зрения закона, обработка его данных может быть признана незаконной, и законный представитель вправе потребовать её прекращения.

Пример. Пятнадцатилетний школьник увидел объявление о работе курьером и отправил анкету с фотографией и номером телефона. Родитель, узнав об этом, вправе обратиться к оператору с запросом о том, какие данные ребёнка собраны, и потребовать их уничтожения, приложив документы, подтверждающие свои полномочия, например копию свидетельства о рождении.

Помимо законных представителей, права субъекта может осуществлять представитель по доверенности. Совершеннолетний дееспособный человек вправе поручить другому лицу, например родственнику или юристу, направить запрос, получить сведения или подать жалобу от его имени. Полномочия представителя должны быть подтверждены доверенностью, оформленной в соответствии с гражданским законодательством. Для отдельных случаев может потребоваться нотариальное удостоверение; простая письменная доверенность также используется на практике, но оператор вправе проверить её подлинность и при обоснованных сомнениях запросить дополнительное подтверждение.

Представитель направляет запрос с указанием сведений о себе и о субъекте, прикладывает доверенность или иной документ, подтверждающий полномочия. Оператор не вправе отказать в рассмотрении запроса только потому, что его подал представитель, если полномочия подтверждены надлежащим образом. Но оператор обязан убедиться, что сведения о человеке не раскрываются постороннему: это защита самого субъекта.

Закон о персональных данных содержит также правило на случай смерти субъекта: согласие на обработку его данных дают наследники, если такое согласие не было дано субъектом при жизни. Это может быть актуально, например, если нужно решить вопрос о публикации материалов с изображением умершего сотрудника или о закрытии связанных с ним записей.

Отдельно стоит отметить: представитель не вправе действовать вопреки интересам субъекта. Если подросток уже вправе самостоятельно совершать определённые действия, а его законный представитель пытается получить чувствительную информацию с иной целью, оператор должен быть осторожен. Это скорее редкие ситуации, но они иллюстрируют, что право на защиту данных — это право конкретного человека, а не его окружения.

Как права соотносятся между собой: практический взгляд

Права субъекта лучше воспринимать не как набор разрозненных пунктов, а как последовательный инструментарий. Сначала человек узнаёт (право на доступ). Затем оценивает и исправляет (уточнение). Если обработка не нужна или незаконна — останавливает её (блокирование, отзыв согласия, требование прекратить обработку, требование прекратить распространение). Если что-то пошло не так — удаляет следы (уничтожение). И если оператор не реагирует — обращается к государству (Роскомнадзор, суд) и требует компенсации (убытки, моральный вред).

Пример полного цикла для кандидата. Человек откликнулся на вакансию курьера, потом получил несколько звонков с предложениями, которые его не интересуют. Он направляет запрос о предоставлении сведений и выясняет, что у оператора хранятся его телефон, анкета и фото паспорта. Он отзывает согласие на обработку анкеты и требует уничтожить копию паспорта, которая больше не нужна. Получив подтверждение уничтожения, он вопрос закрывает. Если бы подтверждения не пришло в разумный срок, следующим шагом стало бы обращение в Роскомнадзор.

Пример для посетителя сайта. Человек оставил заявку на звонок, и с тех пор ему регулярно приходят рекламные сообщения. Он требует немедленно прекратить обработку его номера в рекламных целях. Если сообщения продолжают приходить, он фиксирует это и обращается в надзорный орган и, возможно, в антимонопольный орган по линии законодательства о рекламе.

Разумная тактика — начинать с вежливого и конкретного обращения к оператору. Большинство добросовестных организаций заинтересованы в том, чтобы решить вопрос без споров: это дешевле и проще для всех. Обращение к государству и в суд — это не первая, а резервная мера, но человек всегда должен знать, что она у него есть.

Приложение 4. Как направить запрос или отзыв согласия

Справочный материал. Не является частью Политики и не устанавливает обязательств Оператора. Сведения о том, какие данные обрабатывает Оператор, в каких целях и в какие сроки, содержатся только в Политике (раздел I).

Это приложение — практическое пошаговое руководство для человека, который хочет воспользоваться своими правами: получить сведения об обработке своих данных, исправить их, потребовать уничтожения, отозвать согласие или пожаловаться. Как и Приложение 3, оно носит справочный характер и не является частью Политики обработки персональных данных. Сведения об Операторе, в том числе адреса для направления обращений, указываются в разделе 1 Политики; в этом приложении они намеренно не повторяются, а в образцах обозначены условной пометкой.

Шаг 1. Определите, чего вы хотите добиться

Прежде чем писать, сформулируйте для себя цель. От неё зависит содержание запроса. Возможные цели:

- узнать, обрабатываются ли ваши данные, какие именно, зачем, на каком основании, кому передавались и сколько будут храниться;
- исправить ошибку или дополнить устаревшие сведения;
- временно остановить обработку на время проверки;
- добиться уничтожения сведений, которые больше не нужны или получены незаконно;
- отозвать согласие, которое вы давали ранее;
- прекратить рекламные звонки и сообщения;
- прекратить распространение сведений, которые вы ранее разрешали публиковать;
- оспорить решение, принятое автоматически;
- зафиксировать нарушение и подготовиться к жалобе.

Можно совместить несколько целей в одном обращении, например одновременно запросить сведения и отозвать согласие. Но для ясности иногда лучше направить отдельные обращения: так проще отслеживать сроки ответа по каждому требованию.

Если вы не уверены, что оператор вообще обрабатывает ваши данные, начните с запроса о предоставлении сведений. Ответ покажет, есть ли смысл требовать уточнения или уничтожения.

Шаг 2. Соберите сведения, которые нужно указать в запросе

Закон требует, чтобы запрос позволял идентифицировать заявителя и связать его с обработкой у конкретного оператора. Это делается для защиты самого субъекта: оператор не должен выдавать сведения о человеке тому, кто лишь выдаёт себя за него.

Статья 14 Закона о персональных данных устанавливает, что запрос должен содержать:

- сведения о документе, удостоверяющем личность субъекта или его представителя (как правило, номер основного документа, сведения о дате выдачи и выдавшем органе), либо иные сведения, позволяющие идентифицировать заявителя, если это предусмотрено законом;
- сведения, подтверждающие участие субъекта в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки данных оператором;
- подпись субъекта или его представителя.

Как подтвердить «отношения с оператором», если договора не было? Для кандидата это может быть указание, что он откликнулся на вакансию курьера в определённое время, на определённой площадке, переписывался с конкретным контактом, заполнял анкету, присылал документы. Для посетителя сайта — дата оформления заявки, номер заявки или заказа, номер телефона или адрес электронной почты, указанный в форме. Чем больше конкретики, тем проще оператору найти ваши записи.

Указывайте контакт для ответа: почтовый адрес, адрес электронной почты или иной способ, которым вам удобно получить ответ. Учтите, что если вы просите выслать сведения о себе на электронную почту, оператор может уточнить, что адрес действительно принадлежит вам, чтобы не отправить данные постороннему.

Не нужно прикладывать к запросу больше документов, чем требуется. Копию паспорта целиком, как правило, присылать не обязательно: достаточно сведений о документе. Если оператор требует избыточных сведений, это само по себе может быть поводом для вопросов.

Если запрос подаёт представитель, дополнительно укажите сведения о представителе и приложите документ, подтверждающий его полномочия: доверенность, а для законного представителя несовершеннолетнего — документ, подтверждающий родство или опеку.

Шаг 3. Выберите способ направления

Закон допускает направление запроса в письменной форме на бумаге либо в форме электронного документа, подписанного электронной подписью в соответствии с законодательством Российской Федерации.

Бумажный запрос можно передать лично или направить почтой. Для почтового отправления лучше выбирать заказное письмо с уведомлением о вручении и описью вложения: у вас останутся квитанция, опись и уведомление, подтверждающие, что именно и когда было получено. При личной передаче попросите поставить на вашем экземпляре отметку о получении с датой и подписью принявшего лица.

Электронный документ должен быть подписан электронной подписью. Законодательство об электронной подписи различает простую, усиленную неквалифицированную и усиленную квалифицированную подписи. Какой вид подписи будет признан достаточным, зависит от закона и от соглашений между сторонами. Усиленная квалифицированная электронная подпись по общему правилу приравнивается к собственноручной. На практике многие операторы принимают также обращения через официальные электронные каналы, указанные в их Политике, например по электронной почте, но для юридически значимого требования надёжнее использовать способ, позволяющий однозначно подтвердить вашу личность и дату отправки.

Пользуйтесь каналами, которые оператор официально указал для обращений по вопросам персональных данных. Сообщение, отправленное случайному сотруднику в мессенджер, может не попасть к ответственному лицу, а вам будет сложнее доказать дату получения. Если официальный канал не указан или не работает, используйте почтовый адрес места нахождения организации.

Сохраняйте копию отправленного запроса и все подтверждения отправки и получения. Это ваша доказательная база на случай, если придётся обращаться в Роскомнадзор или в суд.

Шаг 4. Ожидайте ответа в установленный законом срок

В действующей редакции Закона о персональных данных на ответ на запрос субъекта отводится десять рабочих дней с момента обращения либо получения оператором запроса. Этот срок может быть продлён, но не более чем на пять рабочих дней, в случае направления оператором в адрес субъекта

мотивированного уведомления с указанием причин продления.

Обратите внимание: срок исчисляется в рабочих днях, а не в календарных. Выходные и нерабочие праздничные дни в него не включаются. Если вы отправили запрос почтой, срок, как правило, начинает течь с момента получения запроса оператором, поэтому полезно отслеживать доставку.

Для отдельных требований закон устанавливает собственные сроки. Ориентировочно, в действующей редакции:

- уточнение данных при представлении подтверждающих сведений — в течение семи рабочих дней;
- прекращение неправомерной обработки — в течение трёх рабочих дней с даты выявления, а при невозможности обеспечить правомерность — уничтожение в течение десяти рабочих дней;
- уничтожение при достижении целей или отзыве согласия — по общему правилу в течение тридцати дней, если иное не предусмотрено договором, соглашением или законом;
- прекращение обработки по требованию субъекта — в течение десяти рабочих дней с возможностью продления на пять рабочих дней с мотивированным уведомлением;
- прекращение рекламных контактов по требованию — немедленно;
- прекращение передачи данных, разрешённых для распространения, — в течение трёх рабочих дней.

Если оператор отказывает в предоставлении сведений или в выполнении требования, он обязан дать мотивированный ответ со ссылкой на положение закона, являющееся основанием для отказа, в тот же установленный срок.

Шаг 5. Если ответа нет или ответ неудовлетворительный

Первое, что стоит сделать, — проверить, действительно ли запрос был получен. Посмотрите статус почтового отправления, проверьте папку «Спам» в почтовом ящике, на который мог прийти ответ. Иногда ответ отправлен, но затерялся.

Если срок истёк и ответа нет, можно направить повторное напоминание оператору, указав дату первоначального запроса и сославшись на истечение срока. Это не обязательно, но иногда ускоряет решение и, опять же, укрепляет доказательную базу.

Если ответ не получен и после напоминания, либо ответ формальный, неполный, необоснованный, вы вправе обратиться в Роскомнадзор (территориальное управление по месту нахождения оператора или по месту вашего жительства — на практике ведомство само передаст обращение по компетенции). Приложите копию запроса, доказательства его отправки и получения, копию ответа, если он был, и кратко опишите, в чём, по вашему мнению, заключается нарушение.

Параллельно или после обращения в надзорный орган вы вправе обратиться в суд с требованием обязать оператора исполнить обязанности и, при наличии оснований, взыскать убытки и компенсацию морального вреда. Если сумма требований значительна или ситуация сложная, имеет смысл получить консультацию юриста.

Если нарушение связано с рекламными рассылками, дополнительно можно обратиться в антимонопольный орган, который контролирует соблюдение законодательства о рекламе.

Ведите хронологию: даты отправки, получения, ответов, звонков, сообщений. Короткая таблица в блокноте или файле с датами и событиями экономит много сил при составлении жалобы.

Шаг 6. Общие советы по составлению текста

Пишите кратко, конкретно и вежливо. Эмоциональный тон понятен, но для юридического документа лучше подходит спокойное изложение фактов и требований. Чётко указывайте, чего вы просите, и в каком виде хотите получить ответ.

Ссылайтесь на закон в общих чертах, без необходимости цитировать его дословно. Достаточно указать, что вы действуете на основании Федерального закона «О персональных данных». Если вы уверены в номере статьи, можно его указать; если нет — лучше обойтись без номера, чем ошибиться.

Не включайте в запрос лишние персональные данные о себе и тем более о других людях. Указывайте только то, что нужно для идентификации и для сути требования.

Датируйте и подписывайте документ. Сохраните копию для себя.

Образец 1. Запрос о предоставлении сведений об обработке персональных данных

Кому: [наименование Оператора]. Адрес: [адрес Оператора — см. раздел 1 Политики].

От: [ФИО], [сведения о документе, удостоверяющем личность: вид, серия и номер, дата выдачи, выдавший орган — либо иные сведения, позволяющие идентифицировать заявителя]. Контакт для ответа: [контакт для ответа].

Запрос о предоставлении сведений, касающихся обработки персональных данных.

Я, [ФИО], на основании Федерального закона «О персональных данных» прошу предоставить мне сведения, касающиеся обработки моих персональных данных. Моё взаимодействие с Оператором выражалось в следующем: [например: [дата] я откликнулся на вакансию курьера на площадке [название площадки], вёл переписку с контактом [имя или номер контакта], заполнял анкету; либо: [дата] я оформил заявку на сайте Оператора, номер заявки [номер], указанный телефон [номер телефона]].

Прошу сообщить: подтверждаете ли вы факт обработки моих персональных данных; правовые основания и цели обработки; применяемые способы обработки; какие именно мои персональные данные обрабатываются и из какого источника они получены; сроки обработки, в том числе сроки хранения; сведения о лицах, которые имеют доступ к моим данным или которым они могут быть раскрыты, а также о лицах, осуществляющих обработку по поручению Оператора; информацию об осуществлённой или предполагаемой трансграничной передаче моих данных; порядок осуществления моих прав; иные сведения, предусмотренные законом.

Ответ прошу направить [способ: на почтовый адрес / на адрес электронной почты], указанный выше, в срок, установленный законом.

Дата: [дата]. Подпись: [подпись] / [ФИО].

Образец 2. Требование об уточнении персональных данных

Кому: [наименование Оператора]. Адрес: [адрес Оператора — см. раздел 1 Политики].

От: [ФИО], [сведения о документе, удостоверяющем личность, или иные сведения, позволяющие идентифицировать заявителя]. Контакт для ответа: [контакт для ответа].

Требование об уточнении персональных данных.

Я, [ФИО], являюсь субъектом персональных данных, обрабатываемых Оператором в связи с [описание отношений: отклик на вакансию / заявка на сайте / договор от [дата] № [номер]]. Мне стало известно,

что Оператор обрабатывает следующие неточные (неполные, устаревшие) сведения обо мне: [указать, какие сведения неверны, например: номер телефона [неверный номер]; фамилия [прежняя фамилия]].

Верными являются следующие сведения: [указать верные сведения]. В подтверждение прилагаю: [перечень подтверждающих документов, если нужно, например копию свидетельства о перемене фамилии; либо указать, что подтверждающие сведения могут быть проверены иным способом].

На основании Федерального закона «О персональных данных» прошу внести необходимые изменения в мои персональные данные, на время проверки заблокировать неточные сведения, а также уведомить меня о внесённых изменениях и о принятых мерах по адресу, указанному выше.

Дата: [дата]. Подпись: [подпись] / [ФИО].

Образец 3. Требование об уничтожении персональных данных

Кому: [наименование Оператора]. Адрес: [адрес Оператора — см. раздел 1 Политики].

От: [ФИО], [сведения о документе, удостоверяющем личность, или иные сведения, позволяющие идентифицировать заявителя]. Контакт для ответа: [контакт для ответа].

Требование о прекращении обработки и уничтожении персональных данных.

Я, [ФИО], ранее взаимодействовал с Оператором: [описание, например: [дата] направил отклик на вакансию курьера и по просьбе представителя Оператора прислал [перечень переданных сведений, например фото документа, анкету]]. Трудовые или иные договорные отношения между мной и Оператором не возникли [либо: прекращены [дата]].

Считаю, что цели обработки моих персональных данных достигнуты [либо: что мои персональные данные не являются необходимыми для заявленной цели обработки / получены без законного основания]. На основании Федерального закона «О персональных данных» требую прекратить обработку и уничтожить следующие мои персональные данные: [перечень данных, например: копию паспорта, анкету, номер телефона, переписку], а также обеспечить их уничтожение лицами, которым они были переданы или поручена их обработка.

Если Оператор полагает, что какие-либо из указанных сведений должны храниться в силу закона, прошу сообщить, какие именно сведения, на каком основании и в течение какого срока будут храниться, и подтвердить, что они не будут использоваться в иных целях.

Прошу уведомить меня об уничтожении персональных данных по адресу, указанному выше.

Дата: [дата]. Подпись: [подпись] / [ФИО].

Образец 4. Отзыв согласия на обработку персональных данных

Кому: [наименование Оператора]. Адрес: [адрес Оператора — см. раздел 1 Политики].

От: [ФИО], [сведения о документе, удостоверяющем личность, или иные сведения, позволяющие идентифицировать заявителя]. Контакт для ответа: [контакт для ответа].

Отзыв согласия на обработку персональных данных.

Я, [ФИО], [дата или примерный период] дал(а) согласие на обработку моих персональных данных Оператору [указать, при каких обстоятельствах, например: при заполнении анкеты кандидата на сайте / при оформлении заявки на сайте / при подписке на рассылку]. Настоящим, на основании Федерального закона «О персональных данных», я отзываю указанное согласие [полностью / в части: перечислить цели, например: в части получения рекламных и информационных сообщений; в части обработки

данных в целях подбора персонала; в части распространения моих фотографии и имени].

Прошу прекратить обработку моих персональных данных, основанную на этом согласии, и уничтожить их в установленный законом срок, если отсутствуют иные законные основания для их обработки. Если такие основания имеются, прошу сообщить, какие именно данные, на каком основании и в течение какого срока будут обрабатываться.

Прошу подтвердить получение настоящего отзыва и сообщить о принятых мерах по адресу, указанному выше.

Дата: [дата]. Подпись: [подпись] / [ФИО].

Образец 5. Требование о немедленном прекращении рекламных контактов

Кому: [наименование Оператора]. Адрес: [адрес Оператора — см. раздел 1 Политики].

От: [ФИО], контактные данные, на которые поступают сообщения: [номер телефона и (или) адрес электронной почты]. Контакт для ответа: [контакт для ответа].

Требование о прекращении обработки персональных данных в целях продвижения товаров, работ, услуг.

Начиная с [дата], на мой номер телефона [номер] (адрес электронной почты [адрес]) поступают звонки и (или) сообщения рекламного характера от имени Оператора, в частности: [дата, способ, краткое содержание]. [Указать одно из двух: я не давал(а) предварительного согласия на получение таких сообщений / ранее данное согласие я отзываю].

На основании Федерального закона «О персональных данных», а также законодательства о рекламе, требую немедленно прекратить обработку моих персональных данных в целях продвижения товаров, работ, услуг, в том числе прекратить звонки и рассылки по указанным контактам. Прошу также сообщить, из какого источника получены мои контактные данные.

Дата: [дата]. Подпись: [подпись] / [ФИО].

Образец 6. Жалоба в уполномоченный орган по защите прав субъектов персональных данных

Кому: в территориальное управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций [наименование управления, если известно].

От: [ФИО], [почтовый адрес], [контакт для ответа].

Жалоба на нарушение прав субъекта персональных данных.

Сообщаю, что [наименование Оператора], место нахождения: [адрес Оператора — см. раздел 1 Политики], по моему мнению, нарушает мои права как субъекта персональных данных.

Обстоятельства: [кратко и по хронологии: когда и при каких обстоятельствах Оператор получил ваши данные; какие данные; что вы просили; когда и каким способом направили запрос или требование; был ли получен ответ и каков он].

[Дата] я направил(а) Оператору [запрос о предоставлении сведений / требование об уничтожении / отзыв согласия], что подтверждается [почтовой квитанцией, уведомлением о вручении, копией электронного письма]. Срок, установленный Федеральным законом «О персональных данных» для ответа, истёк [дата]. Ответ [не получен / получен, но не содержит запрошенных сведений / содержит отказ без указания законного основания]. [Если применимо: после моего требования обработка

продолжается, а именно: описать факты].

Прошу провести проверку изложенных обстоятельств, принять меры, предусмотренные законодательством, для восстановления моих прав, в том числе потребовать от Оператора [предоставить сведения / прекратить обработку / уничтожить персональные данные], и сообщить мне о результатах рассмотрения жалобы.

Приложения: [копия запроса Оператору; доказательства отправки и получения; копия ответа Оператора, если имеется; скриншоты и иные материалы].

Дата: [дата]. Подпись: [подпись] / [ФИО].

Как пользоваться образцами

Образцы — это отправная точка, а не обязательная форма. Закон не требует использовать какой-либо конкретный бланк: важно, чтобы обращение содержало сведения, необходимые для идентификации, сведения об отношениях с оператором, ясно сформулированное требование и подпись. Удаляйте лишние варианты в квадратных скобках и вписывайте свои обстоятельства.

Старайтесь не смешивать в одном абзаце разные требования. Если вы одновременно отзываете согласие и просите сведения, удобнее оформить это двумя частями обращения или двумя документами. Так проще проследить за выполнением каждого требования в установленный срок.

Если вы действуете как представитель, добавьте в начало сведения о себе и указание, в чьих интересах вы действуете, а также перечислите в приложениях документ о полномочиях. Для законного представителя несовершеннолетнего — например, копию свидетельства о рождении; для представителя по доверенности — копию доверенности.

Если вы не знаете точных сведений, например номера заявки или даты отклика, укажите то, что помните: примерный период, площадку, контакт, с которым вы общались, номер телефона, с которого вы писали. Оператор обязан приложить разумные усилия к поиску ваших данных, а не отказывать лишь из-за неполноты деталей, если идентифицировать вас всё же возможно.

После отправки отметьте в календаре дату, когда истекает срок ответа. Рабочие дни считайте без учёта выходных и праздников. Если к этой дате ответа нет — переходите к шагу 5.

Частые вопросы

Можно ли отправить запрос просто сообщением в мессенджере? Можно попробовать, и иногда это решает простые вопросы быстро, например отписку от рассылки. Но для юридически значимого обращения такой способ ненадёжен: сложно подтвердить личность отправителя, дату получения и то, что сообщение дошло до ответственного лица. Для серьёзных требований используйте письменную форму или электронный документ с подписью через официальные каналы оператора.

Нужно ли объяснять, зачем мне сведения о себе? Нет. Право на доступ не зависит от мотивов. Объяснения могут понадобиться только при повторном запросе ранее установленного законом срока, если первый ответ был неполным.

Могут ли с меня взять плату за ответ? Закон о персональных данных не предусматривает взимания с субъекта платы за предоставление сведений об обработке его данных. Сведения предоставляются в доступной форме.

Что делать, если оператор просит прислать скан паспорта целиком для проверки личности? Разумно уточнить, зачем это нужно и нельзя ли ограничиться сведениями о документе, как это предусмотрено

законом. Если вы всё же передаёте копию, можно закрыть сведения, не нужные для идентификации, и сделать на копии надпись о цели передачи и дате.

Что делать, если ответ пришёл, но он непонятен? Вы вправе попросить разъяснений. Закон требует предоставлять сведения в доступной форме. Если разъяснения так и не последовали, это можно отразить в жалобе.

Что, если я отозвал согласие, а мне всё равно звонят? Зафиксируйте звонки и сообщения с датами, направьте повторное требование со ссылкой на первое и, если ситуация не меняется, обращайтесь в Роскомнадзор, а при рекламном характере контактов — также в антимонопольный орган.

Можно ли обратиться сразу в суд, минуя оператора и надзорный орган? Право на судебную защиту не обусловлено обязательным досудебным обращением в Роскомнадзор. Однако предварительное обращение к оператору почти всегда полезно: оно может решить вопрос без суда, а если нет — даст вам доказательства.

Сколько хранить свои копии обращений и ответов? Разумно хранить их как минимум до полного разрешения ситуации, а лучше — ещё некоторое время после этого, поскольку для обращения в суд действуют сроки исковой давности, а доказательства могут понадобиться позже.

Итог

Права субъекта персональных данных — это не формальность, а действующий механизм, которым может воспользоваться любой человек: кандидат, который передумал работать курьером, посетитель, оставивший телефон на сайте, бывший сотрудник, чья фотография осталась в материалах компании. Механизм этот прост: узнать, исправить, остановить, удалить и, если нужно, обжаловать. Главные условия успеха — конкретность обращения, соблюдение формы, внимание к срокам и сохранение доказательств. Добросовестный оператор заинтересован в том, чтобы такие обращения рассматривались быстро и по существу, а закон даёт человеку инструменты на случай, если этого не происходит.

Приложение 5. Файлы cookie и похожие технологии: справочник

Справочный материал. Не является частью Политики и не устанавливает обязательств Оператора. Сведения о том, какие данные обрабатывает Оператор, в каких целях и в какие сроки, содержатся только в Политике (раздел I).

Это приложение носит справочный и просветительский характер. Оно не является частью Политики обработки персональных данных, не устанавливает прав и обязанностей и не описывает, какие конкретно технологии применяются на сайтах и в сервисах курьерской службы GGCO (ООО «Гепард»). Какие именно технологии использует сайт, указано в Политике использования cookie. Здесь же собраны общие сведения о том, как устроены cookie и родственные им механизмы, зачем они нужны, какие у них бывают риски и как человек может ими управлять. Текст написан для читателя без технической подготовки: курьера, кандидата на вакансию, клиента, который отслеживает посылку, или просто посетителя сайта, которому интересно, что происходит «под капотом» браузера.

Что такое cookie простыми словами

Cookie (по-русски их иногда называют «куки») — это небольшие текстовые записи, которые сайт просит браузер сохранить у себя и затем возвращать обратно при следующих обращениях к этому же сайту. Название пришло из программистского жаргона: так когда-то называли небольшой фрагмент данных, который одна программа передаёт другой, чтобы та «узнала» её при следующей встрече. Можно представить cookie как номерок в гардеробе. Вы сдаёте пальто, вам выдают номерок, и когда вы возвращаетесь, гардеробщик по номерку понимает, какое пальто ваше. Сам номерок не содержит вашего пальто и обычно ничего не говорит о вас лично, но позволяет связать вас с тем, что хранится у гардеробщика.

Зачем вообще нужен такой номерок? Дело в том, что базовый протокол, по которому браузер общается с сайтом, изначально «забывчивый». Каждый запрос страницы для сервера выглядит как отдельное, никак не связанное с предыдущими обращение. Если бы не было никакого способа запомнить посетителя, сайт не смог бы удержать вас в личном кабинете после входа: при переходе на каждую новую страницу пришлось бы заново вводить логин и пароль. Корзина интернет-магазина опустошалась бы при каждом клике, выбранный язык сбрасывался бы, а форма из нескольких шагов теряла бы уже введённые данные. Cookie решают именно эту проблему: они дают сайту короткую память о том, что происходило раньше.

Важно понимать, что cookie — это не программа и не вирус. Это пассивные данные: строчка текста, которую браузер хранит и отправляет. Сама по себе cookie ничего не запускает на компьютере, не читает файлы на диске и не может «заразить» устройство. Вопросы, которые возникают вокруг cookie, связаны не с их опасностью для техники, а с тем, какую информацию с их помощью можно накопить о поведении человека и кому эта информация потом становится доступна.

Из чего состоит cookie

У каждой cookie есть несколько составных частей. Их не нужно запоминать, но понимание этих частей помогает разобраться, почему одни cookie безобидны, а другие вызывают вопросы.

Имя. Это короткий ярлык, по которому сайт отличает одну свою запись от другой. Например, одна cookie может отвечать за выбранный язык интерфейса, другая — за признак того, что пользователь уже закрыл баннер с уведомлением, третья — за идентификатор сеанса входа. Имена часто выглядят непонятно для человека, потому что выбираются разработчиками для удобства программы, а не читателя.

Значение. Это собственно содержимое записи. Иногда значение понятно на глаз, например «ru» для русского языка. Гораздо чаще это длинный набор случайных букв и цифр. Такой набор сам по себе ничего не означает, но служит ключом: сервер хранит у себя связанную с этим ключом информацию, а cookie лишь напоминает ему, какой именно ключ ваш. Хорошо устроенные сайты не кладут в cookie пароли, номера документов и иные чувствительные сведения в открытом виде, а хранят только такие обезличенные идентификаторы.

Домен. Это адрес сайта, которому принадлежит cookie и которому браузер будет её возвращать. Браузер строго следит, чтобы cookie, поставленная одним сайтом, не отправлялась другому, постороннему сайту. Если cookie записана для определённого домена, то, заходя на совершенно другой домен, браузер её туда не передаст. Существуют нюансы с поддоменами: cookie может быть настроена так, чтобы её видели и основной сайт, и его разделы на поддоменах, а может быть ограничена только одним конкретным адресом.

Путь. Это дополнительное ограничение внутри одного сайта. Можно указать, что cookie относится только к определённому разделу, например только к личному кабинету. Тогда при посещении других разделов того же сайта браузер не будет её отправлять. На практике путь чаще всего указывают максимально широким, то есть весь сайт целиком.

Срок действия. Это момент, когда браузер должен удалить cookie. Срок может быть очень коротким, например до закрытия браузера, или долгим — дни, месяцы, а иногда и годы. Отдельно браузеры вводят собственные ограничения на максимальный срок жизни некоторых видов cookie, так что даже если сайт попросит хранить запись очень долго, браузер может её удалить раньше.

Флаг Secure. Если у cookie стоит такая пометка, браузер будет передавать её только по защищённому соединению, то есть когда адрес сайта начинается с https и рядом с адресом отображается признак защищённого подключения. Это важно, потому что при незащищённом соединении данные идут по сети в открытом виде, и их теоретически может подсмотреть кто-то, кто находится в той же сети. Пометка Secure защищает от такой утечки.

Флаг HttpOnly. Эта пометка запрещает сценариям, работающим на самой странице, читать cookie. Cookie по-прежнему отправляется на сервер вместе с запросами, но программный код внутри страницы не может её «достать». Зачем это нужно? Если на страницу каким-то образом попадёт вредоносный код, например через уязвимость, он не сможет украсть идентификатор вашего сеанса и войти в ваш кабинет от вашего имени. Для cookie, отвечающих за вход в учётную запись, такая пометка считается хорошей практикой.

Флаг SameSite. Эта пометка определяет, отправлять ли cookie, когда запрос к сайту инициирован с другого сайта. Представим, что вы находитесь на странице одного сайта, а она обращается к другому: загружает с него картинку, отправляет форму или переводит вас по ссылке. Режим SameSite подсказывает браузеру, как себя вести в такой ситуации. Самый строгий вариант означает, что cookie будет отправляться только тогда, когда вы находитесь непосредственно на «родном» сайте. Промежуточный вариант разрешает отправку при обычном переходе по ссылке, но не при скрытых фоновых запросах с чужих страниц. Самый мягкий вариант разрешает отправку всегда, но современные браузеры требуют, чтобы такая cookie обязательно была ещё и с пометкой Secure. SameSite помогает защититься от атак, при которых чужой сайт пытается выполнить действие в вашей учётной записи без вашего ведома, а заодно ограничивает возможности отслеживания между сайтами.

Если коротко подытожить: имя и значение — это что записано, домен и путь — кому и где это показывать, срок — как долго хранить, а флаги — в каких условиях это можно передавать и кто может это читать.

Собственные и сторонние cookie

Одно из самых важных различий — между собственными и сторонними cookie. От него во многом зависит, можно ли с помощью cookie следить за человеком в интернете.

Собственные cookie (их ещё называют cookie первой стороны) ставит тот сайт, адрес которого вы видите в адресной строке. Если вы открыли сайт курьерской службы и он запомнил, что вы выбрали город, — это собственная cookie. Она видна только этому сайту и возвращается только ему. Собственные cookie обслуживают в основном работу самого сайта: вход в кабинет, настройки, корзину, защиту форм.

Сторонние cookie (cookie третьей стороны) ставит не тот сайт, который вы открыли, а какой-то другой, чьё содержимое встроено в страницу. Страница современного сайта редко состоит только из собственного материала. На ней могут быть встроённая карта, видеоролик, кнопка соцсети, рекламный блок, счётчик посещаемости, чат поддержки от внешнего поставщика. Каждый такой элемент загружается с серверов своего владельца, и этот владелец может установить в браузере свою cookie — уже для своего домена.

Почему это важно? Потому что один и тот же внешний сервис может быть встроён в тысячи разных сайтов. Если вы посещаете сайт про погоду, затем интернет-магазин, затем новостной портал, и на всех трёх стоит один и тот же внешний рекламный или аналитический элемент, этот элемент видит одну и ту же свою cookie в вашем браузере на всех трёх площадках. Так он может сложить картину: этот браузер интересовался погодой, потом смотрел обувь, потом читал о путешествиях. Именно на этом механизме исторически строилась значительная часть таргетированной рекламы.

Из-за этого производители браузеров в последние годы всё сильнее ограничивают сторонние cookie. Некоторые браузеры по умолчанию блокируют их полностью или изолируют, то есть хранят отдельный набор cookie внешнего сервиса для каждого посещаемого сайта, так что сложить общую картину становится невозможно. Политика разных браузеров на этот счёт отличается и со временем меняется, поэтому точное поведение лучше уточнять в справке своего браузера.

Не все сторонние cookie служат рекламе. Внешний сервис оплаты, встроённый виджет поддержки или защита от автоматических ботов тоже могут использовать сторонние cookie, и без них соответствующая функция может работать хуже. Поэтому полная блокировка сторонних cookie иногда приводит к тому, что отдельные встроённые элементы перестают корректно работать.

Сессионные и постоянные cookie

Ещё одно деление cookie — по сроку жизни.

Сессионные cookie живут, пока открыт браузер. У них не указан срок действия, и браузер удаляет их, когда сеанс работы заканчивается. Типичный пример — запоминание того, что вы находитесь на втором шаге заполнения формы, или временный идентификатор, позволяющий серверу понимать, что все ваши клики в течение визита относятся к одному посетителю. Стоит оговориться, что у некоторых браузеров есть функция восстановления вкладок при повторном запуске, и в этом режиме сессионные cookie могут сохраняться дольше, чем ожидает пользователь, потому что браузер фактически продолжает прежний сеанс.

Постоянные cookie имеют явный срок действия и сохраняются после закрытия браузера. Благодаря им сайт «помнит» вас при следующем визите через день или через неделю: не нужно снова выбирать язык, не нужно снова закрывать баннер, можно остаться авторизованным, если вы поставили отметку «запомнить меня». Постоянные cookie удобны, но именно они позволяют накапливать историю посещений во времени, поэтому их сроки хранения и цели использования обычно описываются в политиках сайтов особенно подробно.

Длительный срок сам по себе не делает cookie опасной, а короткий — безопасной. Значение имеет назначение записи. Cookie, которая хранит выбранный язык на год, безобиднее, чем рекламный идентификатор, живущий месяц, но собирающий сведения о посещениях множества сайтов.

Категории cookie по назначению

Чаще всего cookie группируют по тому, для чего они нужны. Названия категорий в разных документах немного отличаются, но в целом выделяют четыре основные группы. Ниже приведены типичные примеры для каждой категории; они описывают распространённую практику в интернете, а не конкретный сайт.

Строго необходимые cookie. Без них сайт не может выполнять базовые функции, о которых просит сам пользователь. Сюда относятся записи, удерживающие вход в учётную запись, сохраняющие содержимое корзины или черновик заявки, защищающие формы от подделки запросов, распределяющие нагрузку между серверами, запоминающие сам выбор пользователя относительно cookie. Например, если вы отказались от аналитических cookie, сайт должен где-то запомнить этот отказ, чтобы не спрашивать вас снова на каждой странице, и делает это с помощью необходимой cookie. Как правило, такие cookie устанавливаются без отдельного согласия, поскольку без них сайт попросту не работает, и они не используются для отслеживания вне сайта.

Функциональные cookie. Они делают пользование сайтом удобнее, но без них сайт в целом продолжит работать. Примеры: запоминание выбранного языка или региона, размера шрифта, тёмной или светлой темы, последнего введённого города для расчёта стоимости доставки, свёрнутого или развёрнутого состояния меню. Отказ от функциональных cookie обычно означает, что эти настройки придётся выставлять заново при каждом визите.

Аналитические cookie. Они помогают владельцу сайта понимать, как посетители пользуются сайтом: сколько людей заходит, с каких страниц приходят, на каких уходят, где возникают ошибки, сколько времени занимает загрузка, какие разделы почти никто не открывает. Как правило, такие сведения используются в обобщённом виде — в виде графиков и статистики, а не для изучения конкретного человека. Тем не менее аналитические системы часто предоставляются внешними компаниями, и данные о посещениях передаются на их серверы. Некоторые аналитические инструменты умеют записывать движения мыши и прокрутку страницы, чтобы показать владельцу, где посетители «застревают». Подобные функции требуют особой аккуратности, чтобы в запись не попали вводимые в формы личные данные.

Рекламные и маркетинговые cookie. Они используются, чтобы показывать рекламу, которая предположительно будет интересна человеку, ограничивать количество повторных показов одного объявления, измерять, привела ли реклама к посещению или покупке, а также для так называемого ретаргетинга — когда вы посмотрели товар на одном сайте, а потом видите его рекламу на других. Именно эта категория чаще всего связана со сторонними cookie и с отслеживанием между сайтами, поэтому для неё, как правило, запрашивается явное согласие, а отказ не должен мешать пользоваться

сайтом.

Иногда выделяют и другие категории, например cookie социальных сетей, которые появляются при встраивании кнопок «поделиться» или виджетов с публикациями, или cookie безопасности, которые помогают распознавать подозрительную активность. По сути они обычно укладываются в одну из четырёх основных групп.

Важно помнить: категория определяется не техническим устройством записи, а её целью. Одна и та же по виду cookie может быть необходимой на одном сайте и аналитической на другом. Поэтому единственный надёжный источник сведений о том, какие cookie использует конкретный сайт и зачем, — его собственная политика использования cookie. Какие именно технологии использует сайт GGCO, указано в Политике использования cookie.

Локальное хранилище: `localStorage` и `sessionStorage`

Кроме cookie, в браузерах есть и другие способы хранения данных на стороне пользователя. Самые распространённые из них — так называемое веб-хранилище, которое бывает двух видов: `localStorage` (локальное хранилище) и `sessionStorage` (хранилище сеанса).

Главное отличие веб-хранилища от cookie состоит в том, что эти данные не отправляются на сервер автоматически с каждым запросом. Cookie браузер прикладывает к каждому обращению к сайту сам, а данные из веб-хранилища остаются в браузере, и их может прочитать только программный код самой страницы. Если код решит, он может отправить их на сервер, но это будет отдельное действие, а не автоматическое поведение браузера.

Второе отличие — объём. Cookie рассчитаны на очень небольшие записи, а веб-хранилище позволяет сохранить заметно больше информации. Поэтому сайты используют его, например, для хранения черновика длинной формы, чтобы вы не потеряли введённый текст при случайном обновлении страницы, для запоминания настроек интерфейса, для кэширования данных, которые не хочется загружать заново при каждом открытии.

`localStorage` хранит данные бессрочно, пока их не удалит сам сайт или пользователь, очистив данные сайтов в настройках браузера. Заккрытие браузера и перезагрузка компьютера на него не влияют.

`sessionStorage` живёт, пока открыта конкретная вкладка. Если закрыть вкладку, данные исчезают. Если открыть тот же сайт в другой вкладке, у неё будет своё отдельное хранилище сеанса. Это удобно, например, для многошаговых процессов, которые не должны «перетекать» из одной вкладки в другую.

Существуют и более сложные механизмы хранения в браузере, например встроенные базы данных и кэш, которые используют современные веб-приложения, чтобы работать быстрее или даже без подключения к интернету. С точки зрения пользователя они похожи на веб-хранилище: данные хранятся в браузере, привязаны к сайту и удаляются вместе с прочими данными сайтов.

С точки зрения приватности веб-хранилище и cookie похожи: и то и другое может хранить идентификатор, по которому сайт узнаёт браузер при повторных визитах. Поэтому законодательство и добросовестная практика обычно рассматривают их вместе, и в политиках сайтов под словом «cookie» часто подразумеваются и эти родственные технологии. Удаляются они, как правило, той же командой браузера — очисткой файлов cookie и данных сайтов.

Пиксели и веб-маяки

Пиксель, или веб-маяк, — это способ узнать, что определённая страница была открыта или определённое письмо было прочитано. Классический вариант выглядит так: в страницу или в письмо вставляется крошечная картинка размером в одну точку, часто прозрачная, которую человек не видит. Эта картинка загружается не с того сервера, где лежит сама страница, а с сервера того, кто хочет получить сведения. Когда браузер или почтовая программа загружает картинку, этот сервер получает запрос и вместе с ним сведения: время открытия, адрес, с которого пришёл запрос, тип браузера и устройства, а иногда и его cookie, если они ранее были установлены.

Современные пиксели чаще представляют собой не картинку, а небольшой фрагмент программного кода, который выполняет ту же задачу, но может передавать больше информации: какие кнопки нажал посетитель, оформил ли он заявку, сколько времени провёл на странице. Рекламные системы используют такие пиксели, чтобы понять, привела ли реклама к целевому действию, например к отправке заявки или покупке.

В электронной почте пиксели позволяют отправителю рассылки узнать, открыто ли письмо и когда. Многие почтовые сервисы и программы умеют блокировать загрузку внешних картинок по умолчанию или загружают их через собственный промежуточный сервер, чтобы отправитель не узнал адрес и точное время открытия. Если вы не хотите сообщать отправителям о прочтении писем, можно включить в настройках почтовой программы запрет на автоматическую загрузку изображений.

Пиксели сами по себе не хранят данных в браузере, но часто работают в паре с cookie: пиксель сообщает о событии, а cookie позволяет связать это событие с конкретным браузером. Поэтому на пиксели распространяются те же правила, что и на cookie соответствующей категории: если вы отказались от рекламных cookie, добросовестный сайт не должен загружать и рекламные пиксели.

Встроенные виджеты и iframe: карты, видео, рейтинги

Многие сайты встраивают в свои страницы готовые элементы от внешних сервисов. Это удобно: не нужно самостоятельно рисовать карту, разрабатывать видеоплеер или систему отзывов. Техническим способом такого встраивания часто служит так называемый iframe — «окно» внутри страницы, через которое показывается содержимое другого сайта. Также встречаются встраиваемые сценарии, которые загружаются с чужого сервера и рисуют элемент прямо на странице.

Примеры таких элементов: интерактивная карта с расположением пунктов выдачи или офиса; видеоролик с инструкцией, загруженный на видеохостинг; блок с рейтингом и отзывами от внешнего сервиса отзывов; кнопки «поделиться» и ленты соцсетей; окно онлайн-чата поддержки; капча — проверка «я не робот»; встроенная форма оплаты.

Почему встроенные элементы передают данные своим владельцам? Потому что, технически, браузер для их показа обращается напрямую к серверам этих владельцев. Чтобы показать карту, браузер запрашивает у картографического сервиса фрагменты изображения. Чтобы показать видео, он загружает плеер и сам ролик с видеохостинга. При каждом таком обращении внешний сервер, как и любой сервер в интернете, получает адрес вашего подключения, сведения о браузере и устройстве, адрес страницы, на которой встроен элемент, а также собственные cookie этого сервиса, если они у вас есть. Если вы вошли в свою учётную запись у этого внешнего сервиса, например в видеохостинг или в соцсеть, то он может связать посещение страницы с вашим профилем.

Владелец сайта, на котором размещён виджет, в большинстве случаев не управляет тем, что именно внешний сервис собирает и как использует. Обработка этих данных регулируется правилами самого

внешнего сервиса. Поэтому добросовестная практика состоит в том, чтобы предупреждать посетителей о встроенных элементах, а в ряде случаев — загружать их только после того, как пользователь нажал кнопку, например «Показать карту» или «Воспроизвести видео». До этого момента на странице показывается лишь статичная заглушка, и данные внешнему сервису не уходят.

Если вам важно, чтобы внешние сервисы знали о вас меньше, можно выходить из своих учётных записей в соцсетях и на видеохостингах, когда они не нужны, пользоваться отдельным профилем браузера для личных аккаунтов, включить в браузере защиту от отслеживания или блокировку сторонних cookie. При этом некоторые встроенные элементы могут перестать отображаться или работать не полностью.

Отпечаток браузера (fingerprinting)

Отпечаток браузера — это способ узнать браузер повторно без сохранения у него каких-либо записей. Если cookie похожи на номерок, который вам выдали, то отпечаток похож на опознание по приметам: рост, цвет глаз, походка, одежда. Ни одна из примет по отдельности не уникальна, но их сочетание может выделить человека из толпы.

У браузера тоже есть множество «примет», которые он сообщает сайтам или которые можно выяснить, выполнив на странице несложный код: версия браузера и операционной системы, размер и разрешение экрана, установленный язык и часовой пояс, набор доступных шрифтов, особенности того, как устройство рисует графику, количество ядер процессора, объём памяти, поддерживаемые технологии и форматы. Каждый параметр по отдельности есть у миллионов людей, но их комбинация может оказаться очень редкой или даже уникальной.

С приватностью отпечаток связан по двум причинам. Во-первых, его нельзя просто удалить, как cookie: он вычисляется заново при каждом визите из характеристик самого устройства. Во-вторых, человек обычно не видит, что его браузер «опознают» таким способом. Поэтому производители браузеров принимают меры против отпечатков: ограничивают количество сообщаемых сведений, специально добавляют небольшой случайный «шум» в отдельные параметры, делают характеристики одинаковыми для многих пользователей, чтобы те сливались в общей массе.

Справедливости ради, у похожих техник есть и легитимное применение — защита от мошенничества. Банки, платёжные сервисы и крупные площадки анализируют характеристики устройства, чтобы заметить, что в учётную запись пытаются войти с совершенно незнакомого компьютера, и запросить дополнительное подтверждение. Граница между защитой и слежкой определяется целью использования, прозрачностью для пользователя и соблюдением закона.

Полностью защититься от отпечатков обычному пользователю сложно, а попытки радикально «замаскировать» браузер с помощью множества расширений иногда делают его даже более заметным, потому что редкое сочетание настроек само становится приметой. Разумный подход — пользоваться актуальной версией распространённого браузера, включить встроенную защиту от отслеживания и не устанавливать лишних расширений.

Как управлять cookie в популярных браузерах

Все современные браузеры позволяют просматривать, удалять и блокировать cookie. Названия пунктов меню и их расположение меняются от версии к версии, поэтому ниже описаны общие шаги, а не точные пути. Если нужный пункт найти не удаётся, надёжный способ — открыть настройки браузера и воспользоваться встроенным поиском по настройкам, набрав слово «cookie», «файлы cookie» или «данные сайтов».

Общие возможности, которые есть практически везде:

- удалить все cookie и данные сайтов сразу, обычно вместе с очисткой истории за выбранный период;
- посмотреть и удалить cookie конкретного сайта, не трогая остальные;
- заблокировать сторонние cookie целиком;
- разрешить или запретить cookie для отдельных сайтов в виде исключений;
- настроить автоматическую очистку cookie при закрытии браузера;
- включить встроенную защиту от отслеживания или режим повышенной приватности.

Google Chrome. Управление cookie находится в разделе настроек, посвящённом конфиденциальности и безопасности. Там можно выбрать режим обработки сторонних cookie, открыть список всех сохранённых данных сайтов и удалить их выборочно или полностью, а также добавить сайты в списки исключений. Очистка истории позволяет удалить cookie вместе с кэшем за выбранный интервал времени. Для текущего сайта сведения о cookie можно также открыть, нажав на значок слева от адреса в адресной строке.

Mozilla Firefox. В настройках приватности и защиты Firefox предлагает несколько уровней защиты от отслеживания, от стандартного до строгого, а также пользовательскую настройку. В стандартном режиме браузер по умолчанию изолирует cookie сторонних сервисов для каждого сайта отдельно. В том же разделе можно управлять cookie и данными сайтов, удалить их, задать исключения и включить удаление при закрытии браузера. Значок щита рядом с адресной строкой показывает, что браузер заблокировал на текущей странице.

Safari. В браузере Safari на компьютерах и устройствах Apple управление находится в настройках, в разделе конфиденциальности. Safari по умолчанию ограничивает межсайтовое отслеживание и сторонние cookie. Там же можно посмотреть и удалить данные отдельных сайтов или полностью заблокировать cookie. На iPhone и iPad соответствующие параметры находятся в общих настройках устройства в разделе, относящемся к Safari, а не внутри самого браузера.

Яндекс Браузер. Настройки cookie находятся в разделе, посвящённом сайтам или конфиденциальности, — в зависимости от версии. Здесь можно запретить сторонние cookie, просмотреть и удалить данные сайтов, назначить исключения. Очистка истории также позволяет удалить cookie за выбранный период. Как и в других браузерах, через значок слева от адреса можно посмотреть разрешения и данные для текущего сайта.

Microsoft Edge. Edge, как и Chrome, построен на общей основе, поэтому настройки похожи. В разделе, посвящённом cookie и разрешениям сайтов, можно управлять cookie и удалять их, блокировать сторонние cookie, а в разделе конфиденциальности — выбрать уровень предотвращения отслеживания: базовый, сбалансированный или строгий. Строгий режим блокирует больше трекеров, но может нарушить работу отдельных сайтов.

Мобильные браузеры. На телефонах и планшетах принцип тот же, но меню устроено компактнее. Обычно нужно открыть меню браузера (часто это три точки или три полоски), перейти в настройки, найти раздел конфиденциальности, безопасности или настроек сайтов, а там — пункт про cookie или очистку данных. На некоторых устройствах часть настроек вынесена в системные настройки телефона. Кроме того, на мобильных устройствах стоит помнить про встроенные браузеры внутри приложений: когда вы открываете ссылку из мессенджера или соцсети, страница может загрузиться не в вашем обычном браузере, а во встроенном окне этого приложения, у которого свой набор cookie и свои настройки. Если вы хотите, чтобы ваши настройки приватности действовали, ссылку можно открыть в

обычном браузере через соответствующий пункт меню.

Кроме настроек самого браузера, многие сайты предлагают собственную панель управления согласием, обычно доступную через баннер при первом визите или по ссылке в нижней части страницы. Через неё можно включать и отключать отдельные категории cookie для этого сайта, не затрагивая остальные сайты. Стоит учитывать, что если вы очистите все cookie в браузере, сайт «забудет» и ваш выбор, и баннер появится снова.

Что происходит при отказе от cookie

Отказ от cookie — законное право пользователя, и в большинстве случаев он не мешает пользоваться основными функциями сайта. Однако последствия зависят от того, от каких именно cookie вы отказываетесь.

Если отказаться от рекламных cookie, вы, скорее всего, не заметите никакой разницы в работе сайта. Реклама, если она есть, не исчезнет, но станет менее персонализированной, то есть будет подбираться не по вашей истории, а, например, по содержанию страницы.

Если отказаться от аналитических cookie, сайт продолжит работать как обычно. Владелец сайта просто не будет учитывать ваш визит в своей статистике или будет учитывать его в обезличенном виде, если это позволяет используемый инструмент. Косвенное последствие — владельцу сложнее понять, что на сайте неудобно, и исправить это.

Если отказаться от функциональных cookie, придётся смириться с тем, что сайт не будет запоминать настройки: язык, регион, выбранный город, оформление. Их придётся выставлять заново.

Если заблокировать все cookie целиком, включая необходимые, через настройки браузера, часть сайтов может перестать работать. Не получится войти в личный кабинет или удержаться в нём, формы могут не отправляться из-за срабатывания защиты от подделки запросов, корзина и черновики не будут сохраняться, баннер о cookie будет появляться снова и снова, потому что сайту негде запомнить ваш ответ. Поэтому полную блокировку обычно рекомендуют только тем, кто понимает её последствия, а более разумный компромисс — блокировка сторонних cookie и отказ от необязательных категорий через панель согласия.

Важно понимать и то, что отказ от cookie не делает человека невидимым для сайта. Сервер в любом случае получает технические сведения, необходимые для доставки страницы: адрес подключения, тип браузера, запрашиваемую страницу. Эти сведения обычно фиксируются в служебных журналах сервера для обеспечения работоспособности и безопасности. Отказ от cookie ограничивает возможность связывать ваши визиты между собой и с внешними сервисами, но не отменяет того, что сайт технически обслуживает ваш запрос.

Режим инкогнито: что он делает и чего не делает

Режим инкогнито (в разных браузерах он называется по-разному: приватное окно, режим приватного просмотра, скрытый режим) часто воспринимают как способ стать невидимым в интернете. Это заблуждение. Режим инкогнито решает другую, гораздо более узкую задачу.

Что режим инкогнито делает:

- не сохраняет историю посещённых страниц на устройстве после закрытия приватного окна;
- удаляет cookie и данные сайтов, созданные в приватном окне, когда оно закрывается;
- не сохраняет введённые в формы данные и поисковые запросы в памяти браузера;

— начинает каждый приватный сеанс «с чистого листа», без cookie обычного режима, поэтому сайты не видят вас как уже знакомого посетителя и вы не авторизованы в своих учётных записях, пока сами не войдёте.

Чего режим инкогнито не делает:

- не скрывает ваш адрес подключения от сайтов, которые вы посещаете;
- не скрывает ваши действия от поставщика интернета, от администратора рабочей или учебной сети, от владельца точки Wi-Fi;
- не мешает сайтам видеть, что вы делаете, пока приватное окно открыто: аналитика, пиксели и cookie работают как обычно, просто удаляются после закрытия;
- не защищает от отпечатка браузера;
- не защищает от вирусов, фишинга и мошенников;
- не скрывает ваши действия, если вы вошли в свою учётную запись на каком-либо сервисе: сервис знает, что это вы;
- не удаляет файлы, которые вы скачали: они остаются на устройстве.

Режим инкогнито полезен в бытовых ситуациях: если вы пользуетесь чужим компьютером и не хотите оставлять на нём следы входа в почту, если нужно временно войти во второй аккаунт, если хочется проверить, как сайт выглядит для нового посетителя. Но он не заменяет ни защиты от слежки, ни осторожности.

Отдельное предупреждение для пользователей общих и чужих компьютеров: даже в режиме инкогнито всегда явно выходите из учётных записей и закрывайте приватное окно после работы. Если окно останется открытым, следующий человек за этим компьютером получит доступ к вашему сеансу.

Почему сайты спрашивают согласие

Многие сайты при первом посещении показывают баннер или окно с вопросом о cookie. У этого есть несколько причин.

Первая причина — правовая. Данные, собираемые с помощью cookie и похожих технологий, в определённых случаях позволяют прямо или косвенно определить человека и поэтому могут относиться к персональным данным. В России обработка персональных данных регулируется законодательством о персональных данных, которое требует законного основания для обработки, в том числе в ряде случаев — согласия субъекта, а также информирования о целях и способах обработки. В других странах действуют свои правила, некоторые из которых прямо требуют спрашивать согласие на установку необязательных cookie. Сайты, работающие с посетителями из разных стран, часто ориентируются на самые строгие требования.

Вторая причина — прозрачность. Даже там, где закон не требует отдельного согласия на конкретный вид cookie, добросовестная практика состоит в том, чтобы честно сообщить человеку, что происходит, и дать ему выбор. Посетитель вправе знать, какие внешние сервисы получают сведения о его визите и зачем.

Третья причина — доверие. Сайт, который открыто рассказывает о cookie и позволяет от них отказаться, вызывает больше доверия, чем сайт, который молча подключает десятки трекеров.

Как выглядит корректный запрос согласия? Хорошая практика предполагает, что:

- согласие на необязательные cookie запрашивается до того, как они установлены, а не после;

- отказаться так же легко, как согласиться, то есть кнопка отказа заметна и не спрятана за несколькими экранами;
- можно выбрать отдельные категории, а не только «всё или ничего»;
- строго необходимые cookie описаны, но не требуют согласия, потому что без них сайт не работает;
- согласие можно отозвать или изменить в любой момент, например по ссылке внизу страницы;
- из текста понятно, какие внешние сервисы участвуют и где прочитать подробности.

Если сайт не даёт отказаться от необязательных cookie или запутывает пользователя, это повод насторожиться. Пользователь в любом случае сохраняет возможность управлять cookie через настройки браузера.

Ещё раз подчеркнём: это приложение рассказывает о cookie в целом. Какие именно технологии использует сайт, указано в Политике использования cookie, и именно этот документ, а не настоящий справочник, определяет, какие cookie устанавливаются, для каких целей и как от них отказаться.

Краткий словарь терминов

- Браузер — программа для просмотра сайтов, например Chrome, Firefox, Safari, Яндекс Браузер, Edge.
- Домен — адрес сайта, к которому привязаны cookie и данные.
- Cookie первой стороны — запись, которую ставит сам открытый сайт.
- Cookie третьей стороны — запись, которую ставит внешний сервис, встроенный в страницу.
- Сессионная cookie — запись, которая удаляется после окончания сеанса браузера.
- Постоянная cookie — запись со сроком действия, сохраняющаяся после закрытия браузера.
- Веб-хранилище — localStorage и sessionStorage, способ хранения данных в браузере без автоматической отправки на сервер.
- Пиксель — невидимый элемент страницы или письма, сообщающий внешнему серверу о просмотре или действии.
- Iframe — «окно» внутри страницы, показывающее содержимое другого сайта.
- Отпечаток браузера — распознавание браузера по совокупности его характеристик без хранения записей.
- HTTPS — защищённый способ передачи данных между браузером и сайтом, при котором содержимое шифруется.

Приложение 6. Безопасность персональных данных: рекомендации пользователям

Справочный материал. Не является частью Политики и не устанавливает обязательств Оператора. Сведения о том, какие данные обрабатывает Оператор, в каких целях и в какие сроки, содержатся только в Политике (раздел I).

Это приложение также носит справочный характер и не является частью Политики обработки персональных данных. Оно не описывает внутренние меры защиты, которые применяет курьерская служба GGCO (ООО «Гепард»), и не заменяет официальных разъяснений банков, государственных органов и правоохранительных органов. Его задача — помочь курьерам, кандидатам на вакансии, клиентам и всем, кто имеет дело с курьерской доставкой, защитить себя от наиболее распространённых угроз: мошенников, фишинга, утечек документов и взлома учётных записей.

Личная безопасность в интернете похожа на безопасность дома. Хороший замок на двери важен, но не поможет, если вы сами откроете дверь незнакомцу, который представился сотрудником газовой службы. Большинство утечек персональных данных у обычных людей происходит не из-за сложного взлома, а из-за того, что человека убедили самостоятельно передать данные, код или документы. Поэтому значительная часть этого приложения посвящена именно распознаванию обмана.

Как распознать фишинг

Фишинг — это попытка выманить у человека личные данные, пароли, коды подтверждения или деньги, выдавая себя за кого-то, кому человек доверяет: банк, магазин, государственный сервис, работодателя, службу доставки, знакомого. Слово происходит от английского «рыбалка»: мошенник «забрасывает удочку» в виде письма, сообщения или звонка и ждёт, кто «клюнет».

Фишинговое сообщение может прийти по электронной почте, в SMS, в мессенджере, в соцсети, через сайт объявлений или по телефону. Оно почти всегда пытается добиться одного из следующих действий:

- перейти по ссылке и ввести на открывшемся сайте логин, пароль или данные карты;
- назвать код из SMS или из push-уведомления;
- скачать и установить файл или приложение;
- прислать фото документов или селфи с документом;
- перевести деньги — за «оформление», «страховку», «доставку», «разблокировку».

Типичные признаки фишинга:

- Срочность и давление. «Ваша посылка будет возвращена через два часа», «аккаунт заблокируют сегодня», «вакансия закрывается через 30 минут». Мошенникам выгодно, чтобы вы не успели подумать и проверить.
- Неожиданность. Вы не ждали посылку, не откликались на эту вакансию, не совершали этой покупки, но вам пишут именно об этом.
- Просьба назвать код. Настоящие банки, службы доставки, работодатели и государственные сервисы не просят сообщать коды из SMS, пароли и данные карты по телефону или в переписке. Код подтверждения — это ваша подпись под действием, и тот, кто его просит, просит вашу подпись.
- Странный адрес. Ссылка ведёт на сайт, адрес которого похож на настоящий, но отличается: лишняя буква, замена буквы на цифру, дополнительное слово, необычное окончание.

- Ошибки и несоответствия. Неаккуратный текст, странные обороты, обращение «уважаемый клиент» вместо имени, логотип низкого качества. Впрочем, современные мошенники пишут всё грамотнее, поэтому отсутствие ошибок ничего не гарантирует.
- Предложение, которое слишком хорошо, чтобы быть правдой. Выигрыш, компенсация, зарплата намного выше рынка за минимальные усилия.
- Смена канала. Вас просят перейти из официального приложения или сайта в личную переписку в мессенджере, позвонить по другому номеру, установить «специальное приложение».
- Требование секретности. «Никому не говорите», «это конфиденциальная операция», «не сообщайте в банк».

Главное правило против фишинга простое: если сообщение вызывает сильные эмоции и требует быстрых действий, остановитесь. Не переходите по ссылке из сообщения, а откройте сайт или приложение организации самостоятельно — через закладку, через официальное приложение, набрав адрес вручную. Не перезванивайте на номер из сообщения, а найдите официальный номер самостоятельно. Если это действительно важно, информация будет и в официальном канале.

Мошенники, которые представляются курьерской службой

Курьерская доставка — популярная «маска» для мошенников, потому что почти каждый человек время от времени чего-то ждёт и легко поверит сообщению о посылке. Ниже описаны распространённые общие сценарии, известные по открытым предупреждениям; они не относятся к какой-либо конкретной компании.

Сценарий «оплатите доставку». Приходит сообщение о том, что посылка задержана или не может быть доставлена, и для её получения нужно доплатить небольшую сумму или подтвердить адрес по ссылке. Ссылка ведёт на поддельную страницу оплаты, которая собирает данные карты. Небольшая сумма выбрана специально, чтобы человек не задумался.

Сценарий «назовите код для доставки». Звонит «курьер» и говорит, что для передачи посылки, записи на время доставки или смены адреса нужно назвать код, который придёт в SMS. На самом деле это код для входа в ваш аккаунт на государственном портале, в банк, в мессенджер или код подтверждения какой-то операции. После того как вы его назвали, мошенники получают доступ к вашей учётной записи.

Сценарий «продажа с безопасной доставкой». Вы продаёте вещь на сайте объявлений, и «покупатель» предлагает оформить «безопасную сделку с курьерской доставкой», присылая ссылку на страницу, где нужно «получить деньги», введя данные карты. Настоящие сервисы безопасной сделки работают внутри площадки объявлений, а не по ссылкам из личной переписки.

Сценарий «отслеживание посылки». Приходит ссылка на «отслеживание», которая на самом деле ведёт на загрузку вредоносного приложения для телефона или на страницу сбора данных.

Как защититься:

- Проверяйте статус посылки только через официальный сайт или приложение службы доставки, открытые самостоятельно, а не через ссылку из неожиданного сообщения.
- Никогда не называйте коды из SMS «курьеру», «оператору» или «службе поддержки». Курьеру для передачи посылки не нужен код от вашего банка или государственного портала. Если служба доставки использует код получения, он передаётся в рамках официального процесса, и его назначение указано в официальном сообщении; если сомневаетесь, сверьтесь с официальным

каналом службы.

- Не вводите данные карты на страницах, открытых по ссылке из переписки.
- Не устанавливайте приложения из ссылок в сообщениях. Устанавливайте приложения только из официальных магазинов приложений или по инструкции, полученной из официального источника.
- Если «курьер» звонит и давит, положите трубку и свяжитесь со службой доставки по официальным контактам.

Мошенники, которые представляются работодателем

Для курьеров и кандидатов на вакансии особенно актуальна другая разновидность обмана — фальшивые работодатели и фальшивые вакансии. Мошенники пользуются тем, что человек, ищущий работу, заинтересован, готов идти навстречу и привык, что работодатель может запросить документы.

Распространённые общие схемы:

- Плата за трудоустройство. Кандидата просят оплатить «обучение», «форму», «медицинскую книжку», «страховку», «термосумку», «доступ к заказам» или «залог» до начала работы, а после оплаты исчезают. Добросовестный работодатель может предлагать, например, выдачу оборудования на определённых условиях, но эти условия прозрачны, оформлены письменно и не сводятся к переводу денег незнакомому лицу на личную карту.
- Сбор документов. Под видом оформления у кандидата собирают фото паспорта, СНИЛС, ИНН, селфи с паспортом, иногда данные банковской карты. Затем эти данные используют для оформления займов, регистрации фиктивных компаний, открытия счетов и иных противоправных действий.
- Вовлечение в преступные схемы. Под видом «курьерской работы» человеку предлагают забирать и передавать наличные деньги у незнакомых людей, перевозить подозрительные свёртки, «обналичивать» переводы, предоставить свою банковскую карту или оформить на себя счёт. Такие «вакансии» могут быть связаны с участием в мошенничестве или иных преступлениях, и человек рискует сам стать соучастником. Любое предложение забирать деньги у пожилых людей, передавать свою карту или принимать переводы на свой счёт для последующей передачи — серьёзный тревожный сигнал.
- Работа «в обход». Кандидата уговаривают общаться только в личном мессенджере, не задавать вопросов, не обращаться в офис, получать оплату «в конверте» или через третьих лиц.

Признаки, которые должны насторожить:

- работодатель не может или не хочет назвать полное наименование организации и её реквизиты;
- нет возможности проверить организацию по открытым официальным источникам;
- от вас требуют деньги до начала работы;
- обещанный доход значительно выше, чем у других работодателей за похожую работу, без понятного объяснения;
- от вас торопятся получить документы, не объяснив, зачем они нужны и как будут храниться;
- просят код из SMS «для регистрации в системе»;
- просят оформить на себя банковскую карту, сим-карту или электронный кошелёк и передать их;
- суть работы описана туманно, а вопросы вызывают раздражение;

— переписка ведётся с аккаунта, который недавно создан, не имеет никакой истории или выдаёт себя за известную компанию, но не совпадает с её официальными контактами.

Если вы получили предложение от имени конкретной компании, проверьте его через её официальные контакты, указанные на официальном сайте. Спросите, действительно ли такая вакансия существует и действительно ли с вами общается её представитель. Добросовестный работодатель не обидится на проверку.

Как проверять вакансии

Проверка вакансии не требует специальных навыков. Вот несколько общих шагов, которые помогут отсеять большую часть недобросовестных предложений.

Узнайте, кто работодатель. В объявлении или в разговоре должно быть указано полное наименование организации. По наименованию и ИНН можно проверить в открытых официальных государственных сервисах, существует ли такая организация, действует ли она, где зарегистрирована и чем занимается. Если вам отказываются назвать реквизиты, это повод задуматься.

Сопоставьте контакты. Сравните телефон, адрес сайта, адрес электронной почты, с которых вам пишут, с теми, что указаны на официальном сайте компании. Мошенники часто создают похожие адреса и аккаунты с тем же названием и логотипом.

Почитайте отзывы, но критически. Отзывы о работодателях можно найти на разных площадках. Учитывайте, что отзывы бывают как поддельными положительными, так и необъективными отрицательными. Обращайте внимание на повторяющиеся конкретные жалобы, особенно о невыплатах и о сборе денег с кандидатов.

Уточните условия письменно. Попросите описать обязанности, график, порядок и размер оплаты, порядок оформления. Добросовестный работодатель способен объяснить, на каком основании будет строиться сотрудничество — трудовой договор, договор гражданско-правового характера, работа в статусе самозанятого или иное — и какие документы для этого нужны.

Не платите за трудоустройство. Требование перевести деньги до начала работы — один из самых надёжных признаков обмана.

Не передавайте документы до проверки. Сначала убедитесь, что работодатель реален, и только потом передавайте документы, причём лишь те, которые действительно нужны, и только через понятный и защищённый канал.

Прислушайтесь к своим ощущениям. Если вас торопят, сбивают с толку, не отвечают на прямые вопросы или требуют секретности, лучше отказаться от предложения. Потерянная возможность обычно обходится дешевле, чем потерянные документы и деньги.

Безопасная отправка копий документов

Паспорт и другие документы, удостоверяющие личность, — это ключи к вашей юридической жизни. Копию паспорта нельзя «отозвать» так же, как сменить пароль. Поэтому к передаче копий документов стоит относиться так же серьёзно, как к передаче самих документов.

Почему не стоит пересылать паспорт кому попало. Скан или фото паспорта в чужих руках может быть использован для попыток оформления займов в организациях с упрощённой проверкой, регистрации на различных сервисах от вашего имени, создания поддельных договоров, оформления сим-карт и иных действий, последствия которых придётся разбирать уже вам. Даже если большинство серьёзных

организаций проверяют личность тщательнее, чем по одной фотографии, лишние копии документов в интернете увеличивают риск.

Прежде чем отправлять документы, ответьте себе на несколько вопросов:

- Кто получатель? Это проверенная организация или человек, личность и полномочия которого вы можете подтвердить?
- Зачем ему этот документ? Получатель может объяснить, для какой цели нужна копия и на каком основании?
- Нужен ли весь документ? Возможно, достаточно отдельных страниц или отдельных сведений, а не всего паспорта.
- Каким способом передаются данные? Это официальная защищённая форма на сайте организации или личная переписка с неизвестным аккаунтом?
- Как долго будет храниться копия и что с ней будет потом? Добросовестная организация описывает это в своей политике обработки персональных данных.

Водяные знаки «для ...». Если вам всё же нужно отправить копию документа, полезно нанести на неё поверх изображения надпись, указывающую назначение, например «Копия для оформления в такую-то организацию, такая-то дата». Надпись лучше делать так, чтобы она проходила через изображение документа, но не закрывала сведения, которые получателю действительно необходимо прочитать. Такая пометка не делает утечку невозможной, но существенно затрудняет использование копии в других целях: любому, кто получит такую копию, будет видно, что она предназначалась для другого получателя и другой цели. Пометку можно нанести в любом графическом редакторе, в том числе встроенном в телефон. Учитывайте, что некоторые организации по своим правилам могут принимать только копии без пометок; в этом случае уточните, почему, и решите, доверяете ли вы этому получателю.

Проверка адреса сайта и HTTPS. Если документы загружаются через сайт, внимательно посмотрите на адресную строку браузера.

- Убедитесь, что адрес сайта точно совпадает с официальным адресом организации, а не похож на него. Мошенники регистрируют адреса с одной изменённой буквой, с дефисом, с другим окончанием.
- Убедитесь, что адрес начинается с https и браузер не показывает предупреждений о небезопасном соединении. HTTPS означает, что данные передаются в зашифрованном виде и их не подсмострит посторонний в сети.
- Помните, что HTTPS сам по себе не означает, что сайт честный. Мошенники тоже умеют настраивать защищённое соединение. HTTPS отвечает на вопрос «защищён ли канал», но не на вопрос «тот ли это сайт». Поэтому проверка точного адреса важнее значка замка.
- Лучше переходить на сайт организации самостоятельно, а не по ссылке из сообщения.

Другие практические советы:

- Не публикуйте фото документов в открытом доступе, в том числе в соцсетях, даже частично.
- После отправки документов в мессенджере подумайте, стоит ли удалить их из переписки и из галереи телефона, особенно если телефоном пользуются и другие люди или он синхронизирует фото в облако.

- Не храните фото документов в общих альбомах, общедоступных облачных папках и в переписке, к которой есть доступ у посторонних.
- Если вы отправляли документы по электронной почте, учитывайте, что они остаются в папке отправленных писем и у получателя.
- Ведите для себя простой список: кому, когда и какие документы вы отправляли. Это поможет быстро понять масштаб проблемы, если что-то пойдёт не так.

Пароли

Пароль — первая линия защиты большинства учётных записей. Плохой пароль можно подобрать, а один пароль на всех сайтах означает, что утечка с одного, даже малозначимого, сайта открывает доступ ко всем остальным.

Что делает пароль надёжным:

- Длина. Длинный пароль подобрать гораздо сложнее, чем короткий, даже если короткий содержит сложные символы. Хорошая идея — фраза из нескольких не связанных между собой слов.
- Уникальность. Для каждой важной учётной записи — свой пароль. Особенно это касается электронной почты, банка, государственных сервисов и мессенджеров. Почта особенно важна: через неё восстанавливается доступ к большинству других сервисов.
- Непредсказуемость. Не используйте имя, дату рождения, номер телефона, кличку питомца, название любимой команды, простые последовательности клавиш. Эти сведения часто можно узнать из соцсетей.

Как всё это запомнить? Удобнее всего пользоваться менеджером паролей — программой, которая хранит все пароли в зашифрованном виде под одним главным паролем и сама генерирует надёжные пароли. Менеджеры паролей встроены во многие браузеры и операционные системы, также существуют отдельные программы. Главный пароль от менеджера нужно сделать особенно надёжным и нигде не записывать в открытом виде.

Чего делать не стоит:

- записывать пароли на бумажке, приклеенной к монитору, или в записках телефона без защиты;
- сообщать пароль кому-либо, включая «службу поддержки», «администратора», «руководителя»; настоящая служба поддержки не спрашивает ваш пароль;
- вводить пароль на страницах, открытых по ссылке из сообщения;
- сохранять пароли в браузере на чужом или общем компьютере.

Если вы узнали, что сервис, которым вы пользуетесь, допустил утечку данных, смените пароль от этого сервиса и от всех других, где использовался такой же пароль.

Двухфакторная защита

Двухфакторная аутентификация — это дополнительная проверка при входе в учётную запись. Кроме пароля (то, что вы знаете), нужно подтвердить вход чем-то ещё: кодом из SMS, кодом из специального приложения-генератора, подтверждением на другом устройстве, физическим ключом безопасности или биометрией (то, что у вас есть, или то, чем вы являетесь). Даже если пароль украден, злоумышленник не войдёт без второго фактора.

Включите двухфакторную защиту везде, где она доступна, в первую очередь:

- в электронной почте;
- в мессенджерах — там это часто называется облачным паролем или PIN-кодом для подтверждения входа;
- в учётной записи на государственном портале;
- в банковских приложениях, если они дают такую возможность;
- в соцсетях и на сайтах объявлений;
- в учётной записи магазина приложений и облачного хранилища телефона.

Какой второй фактор лучше? Коды из SMS удобны и намного лучше, чем ничего, но они уязвимы: их могут выманить обманом, а в отдельных случаях злоумышленники пытаются перехватить номер, оформив дубликат сим-карты. Приложения-генераторы кодов и подтверждения на доверенном устройстве, как правило, надёжнее. Физические ключи безопасности считаются одним из самых надёжных вариантов, но требуют отдельного устройства.

Самое важное правило двухфакторной защиты: код подтверждения никогда и никому не сообщается. Двухфакторная защита работает только до тех пор, пока второй фактор остаётся у вас. Большинство успешных обманов с кодами происходит не из-за технического взлома, а из-за того, что человека убедили продиктовать код по телефону.

Сохраните резервные коды восстановления, которые многие сервисы выдают при включении двухфакторной защиты, в надёжном месте. Они понадобятся, если вы потеряете телефон.

Безопасность в мессенджерах

Мессенджеры стали основным каналом общения, в том числе по рабочим вопросам. Это делает их привлекательной целью для мошенников: взломанный аккаунт позволяет писать от вашего имени вашим родственникам, коллегам и знакомым, которые вам доверяют.

Настройки приватности. В большинстве мессенджеров можно ограничить, кто видит ваш номер телефона, фотографию профиля, время последнего посещения, кто может добавлять вас в группы и звонить вам. Разумная настройка — показывать номер телефона только контактам или никому, запретить добавлять себя в группы всем подряд, ограничить звонки от незнакомцев. Такие настройки снижают количество спама и мошеннических сообщений.

Защита входа. Включите в мессенджере дополнительный пароль или PIN-код для входа на новом устройстве, если такая функция есть. Периодически проверяйте список активных сеансов и подключённых устройств и завершайте сеансы, которых вы не узнаете. Если в списке появилось незнакомое устройство, это повод немедленно завершить его сеанс и сменить пароль.

Проверка собеседника. Мошенники часто создают аккаунты с именем и фотографией реального человека или организации. Имя и аватар в мессенджере может поставить кто угодно. Поэтому:

- если «знакомый» или «руководитель» внезапно просит денег, код, документы или срочно что-то оплатить, свяжитесь с ним другим способом, например позвоните по известному вам номеру;
- обращайте внимание на имя пользователя и номер, а не только на отображаемое имя;
- если вам пишет «служба поддержки» мессенджера или банка, помните, что настоящие службы поддержки, как правило, не начинают переписку первыми и не просят коды;
- будьте осторожны с аккаунтами, которые недавно созданы, не имеют истории и сразу переходят к просьбам;

— если от имени организации пишет человек с личного аккаунта, уточните через официальные контакты организации, действительно ли он её представитель.

Голосовые сообщения и видео. Современные технологии позволяют подделывать голос и даже изображение человека. Если вы получили голосовое сообщение или видеозвонок от знакомого с необычной просьбой о деньгах или данных, перезвоните ему самостоятельно и задайте вопрос, ответ на который знает только он.

Файлы и ссылки. Не открывайте файлы и ссылки, полученные от незнакомцев, а также неожиданные файлы от знакомых без пояснения. Особенно опасны файлы, которые на телефоне предлагают установить как приложение. Под видом «фото», «документа», «накладной» или «списка заказов» могут скрываться вредоносные программы, которые читают SMS, перехватывают коды и получают доступ к банковским приложениям.

Рабочие чаты. В рабочих чатах не публикуйте лишних персональных данных — своих и чужих: фото документов, домашние адреса, номера карт. Помните, что любое сообщение в групповом чате видят все его участники, а при пересылке оно может уйти дальше. Персональные данные клиентов, ставшие известными в ходе доставки, — адреса, телефоны, состав заказов — не следует пересылать посторонним, публиковать или использовать для личных целей.

Общедоступный Wi-Fi

Бесплатный Wi-Fi в кафе, торговых центрах, транспорте и на вокзалах удобен, но требует осторожности.

Какие есть риски:

- Поддельная точка доступа. Злоумышленник может создать сеть с названием, похожим на настоящее, например с названием кафе, и все, кто к ней подключился, будут передавать трафик через его устройство.
- Незащищённое соединение. В открытой сети без пароля передаваемые данные теоретически могут быть доступны другим участникам сети, если сайт не использует шифрование.
- Подмена страниц. Через контролируемую сеть злоумышленник может пытаться показывать поддельные страницы входа.

Как снизить риски:

- Уточняйте у персонала точное название официальной сети заведения.
- Не выполняйте в общественных сетях особо чувствительных операций, если без этого можно обойтись: вход в банк, оплата, отправка документов. Для таких операций лучше использовать мобильный интернет.
- Убеждайтесь, что сайты открываются по защищённому соединению и браузер не показывает предупреждений о сертификате. Если браузер предупреждает о небезопасном соединении на известном вам сайте, не продолжайте.
- Отключите на телефоне автоматическое подключение к известным открытым сетям, чтобы устройство не подключалось к поддельной сети с тем же названием само.
- После использования общественной сети можно удалить её из списка сохранённых.
- Не устанавливайте никаких программ и сертификатов, которые предлагает установить страница входа в общественную сеть.

Обновления устройств

Обновления операционной системы, браузера и приложений часто воспринимаются как досадная помеха. Но значительная часть обновлений закрывает уязвимости — ошибки, через которые злоумышленники могут получить доступ к устройству или данным. Как только уязвимость становится известной, её начинают активно использовать, и устройства без обновлений остаются беззащитными.

Практические рекомендации:

- Включите автоматическое обновление операционной системы и приложений, если это возможно.
- Не откладывайте надолго установку обновлений безопасности.
- Обновляйте браузер — через него вы работаете с большинством сайтов.
- Устанавливайте приложения только из официальных магазинов приложений или из официальных источников, указанных организацией-разработчиком. Приложения из случайных ссылок и неофициальных сборников могут содержать вредоносный код.
- Обращайте внимание на разрешения, которые запрашивает приложение. Если калькулятор просит доступ к SMS, контактам и микрофону, стоит задуматься, зачем ему это.
- Удаляйте приложения, которыми больше не пользуетесь: каждое лишнее приложение — потенциальная точка уязвимости.
- Учитывайте, что старые устройства со временем перестают получать обновления. Если ваш телефон больше не обновляется, особенно осторожно относитесь к банковским операциям на нём.
- Установите блокировку экрана — PIN-код, пароль, отпечаток или распознавание лица. Если телефон потеряется, это не позволит постороннему сразу получить доступ к вашим мессенджерам, почте и фото документов.
- Включите функцию поиска и удалённой блокировки устройства, которая есть в большинстве современных телефонов. Она позволит заблокировать телефон или стереть данные, если он потерян или украден.
- Делайте резервные копии важных данных, чтобы не потерять их при поломке, утере или атаке вредоносной программы.

Что делать, если документы попали к мошенникам

Если вы подозреваете или точно знаете, что копии ваших документов, данные карты или доступ к учётной записи оказались у посторонних, главное — не паниковать и действовать последовательно. Ниже приведён общий порядок действий. Конкретные процедуры, сроки и требования устанавливаются соответствующими организациями и государственными органами и могут меняться, поэтому уточняйте их на официальных сайтах и у официальных представителей.

Если речь идёт о банковской карте или доступе к банку:

- немедленно свяжитесь с банком по официальному номеру, указанному на обратной стороне карты, на официальном сайте или в официальном приложении;
- попросите заблокировать карту и, при необходимости, доступ к онлайн-банку;
- сообщите, какие данные могли быть скомпрометированы, и узнайте, какие операции проводились;
- если были несанкционированные списания, узнайте у банка порядок их оспаривания и сроки, в которые нужно обратиться;
- смените пароли и проверьте настройки уведомлений.

Если речь идёт об учётной записи на государственном портале:

- если доступ у вас сохранился, смените пароль, проверьте и обновите контактные данные (телефон, почту), включите или проверьте подтверждение входа, просмотрите историю действий и список активных сеансов, если такая возможность есть;
- если доступ утрачен, воспользуйтесь официальными способами восстановления, предусмотренными самим порталом, и обратитесь в его официальную службу поддержки;
- проверьте, не подавались ли от вашего имени заявления, о которых вы не знаете.

Если копии паспорта и других документов оказались у посторонних:

- подумайте, к каким вашим учётным записям и сервисам эти данные могут дать доступ, и усильте их защиту;
- в России предусмотрена возможность установить так называемый самозапрет на заключение договоров потребительского кредита и займа; он устанавливается через государственный портал или иными официальными способами, предусмотренными законом. Самозапрет затрудняет оформление кредитов на ваше имя без вашего участия. Актуальный порядок установки и снятия уточняйте на официальных ресурсах;
- периодически проверяйте свою кредитную историю: в России гражданин вправе получать сведения о своей кредитной истории, в том числе бесплатно в установленных законом пределах. Узнать, в каких бюро хранится ваша кредитная история, можно через официальные государственные сервисы. Если в истории появились незнакомые займы, это повод обратиться к кредитору и в правоохранительные органы;
- если паспорт был утрачен или похищен физически, обратитесь в уполномоченные органы для его замены в установленном порядке; утраченный паспорт признаётся недействительным, что снижает риски его использования;
- если вы подозреваете, что от вашего имени совершаются противоправные действия, обратитесь в полицию с заявлением. Сохраните всё, что может помочь: переписку, номера телефонов, адреса сайтов, снимки экрана, сведения о переводах.

Если взломан мессенджер, почта или соцсеть:

- если доступ сохранился, завершите все чужие сеансы, смените пароль, включите двухфакторную защиту;
- если доступ утрачен, воспользуйтесь официальной процедурой восстановления сервиса;
- предупредите близких, коллег и знакомых, что от вашего имени могут писать мошенники, и попросите не выполнять просьб о деньгах и кодах;
- проверьте, не настроена ли в почте пересылка писем на чужой адрес и не добавлены ли чужие способы восстановления доступа.

Если вы передали документы работодателю или организации, а потом засомневались в её добросовестности, вы вправе обратиться к ней с вопросом о том, как обрабатываются ваши персональные данные, и с требованиями, которые предусмотрены законодательством о персональных данных. Порядок обращения по вопросам обработки персональных данных в GGCO описан в самой Политике обработки персональных данных. Если вы считаете, что ваши права нарушены, вы также вправе обратиться в уполномоченный орган по защите прав субъектов персональных данных.

Общий принцип: чем раньше вы среагируете, тем меньше ущерб. Не стесняйтесь обращаться за помощью — жертвами мошенников становятся люди любого возраста и любого уровня образования, это вопрос не глупости, а мастерства обманщиков, которые профессионально давят на эмоции.

Безопасность курьера в повседневной работе

Курьерская работа связана с постоянным контактом с персональными данными — своими и чужими. Ниже несколько общих рекомендаций, которые касаются не правил конкретной компании, а здравого смысла.

- Используйте для рабочих задач только официальные каналы и приложения, указанные работодателем или заказчиком. Если кто-то просит перейти в другое приложение или чат «для удобства», уточните это через официальный канал.
- Не фотографируйте и не пересылайте лишнего: накладные, адреса, телефоны и имена получателей нужны для доставки, а не для хранения в галерее телефона.
- Не обсуждайте с посторонними, кому и что вы доставляете.
- Если получатель или отправитель просит вас сделать что-то необычное — передать посылку третьему лицу без подтверждения, взять наличные для передачи кому-то ещё, сообщить ему код, пришедший вам на телефон, — остановитесь и свяжитесь с диспетчером или руководителем через официальный канал.
- Блокируйте телефон, когда оставляете его без присмотра. В нём ваши рабочие и личные данные.
- Не передавайте никому доступ к своему рабочему аккаунту, логин и пароль, даже коллеге «на один день».
- Если вам звонят от имени работодателя и просят назвать код, пароль или данные карты, перезвоните по официальному номеру.

Безопасность клиента при получении и отправке посылок

Клиенту курьерской службы также стоит помнить о простых мерах предосторожности.

- Отслеживайте посылки только через официальный сайт или приложение службы доставки, открытые самостоятельно.
- Не сообщайте по телефону данные карты, пароли и коды от банка и государственных сервисов.
- При получении посылки обращайте внимание на то, что от вас просят. Курьеру может понадобиться подтверждение получения, но не доступ к вашим учётным записям.
- Утилизируйте упаковку с наклейками, на которых указаны ваше имя, адрес и телефон, так, чтобы эти данные нельзя было прочитать: можно сорвать и разрезать этикетку или закрасить сведения.
- Не публикуйте в соцсетях фотографии посылок с видимыми накладными.
- Если вам пришло сообщение о посылке, которую вы не ждёте, не переходите по ссылке и не перезванивайте на указанный номер; при необходимости уточните информацию через официальные контакты службы.

Защита данных детей и пожилых родственников

Мошенники нередко выбирают тех, кто хуже ориентируется в цифровой среде: пожилых людей и детей. Заботясь о своей безопасности, стоит позаботиться и о близких.

- Расскажите пожилым родственникам о правиле «код никому не называть». Объясните, что ни банк, ни полиция, ни служба доставки, ни социальная служба не будут просить код из SMS или перевести деньги на «безопасный счёт».
- Договоритесь о кодовом слове или простом правиле: при любом звонке с тревожной новостью о близком человеке сначала перезвонить ему самому.
- Помогите настроить на их телефонах блокировку экрана, обновления и ограничения на установку приложений.
- Детям объясните, что нельзя отправлять незнакомцам фото документов родителей, банковских карт, сообщать адрес и коды из SMS, даже если это нужно «для выигрыша в игре».

Памятка-чек-лист

Ниже — краткий список, который удобно перечитывать время от времени и проверять по нему свои привычки.

Против мошенников:

- Я никогда никому не называю коды из SMS и push-уведомлений, пароли и данные карты.
- Я не перехожу по ссылкам из неожиданных сообщений о посылках, выигрышах, блокировках и вакансиях.
- Я проверяю информацию через официальные сайты и номера, найденные самостоятельно.
- Я останавливаюсь, если меня торопят, пугают или просят держать что-то в секрете.
- Я не плачу за трудоустройство и не передаю никому свою банковскую карту, сим-карту или доступ к своему счёту.
- Я отказываюсь от «работы», связанной с получением чужих наличных или переводов для передачи третьим лицам.

Документы:

- Я передаю копии документов только проверенным получателям и только когда понимаю, зачем они нужны.
- Я по возможности ставлю на копиях пометку «для ...» с указанием получателя, цели и даты.
- Я загружаю документы только на сайты с точно совпадающим официальным адресом и защищённым соединением.
- Я не храню фото документов в общедоступных местах и не публикую их.
- Я знаю, кому и какие документы отправлял.

Учётные записи:

- У меня разные пароли для почты, банка, государственного портала и мессенджеров.
- Я пользуюсь менеджером паролей или другим надёжным способом их хранения.
- У меня включена двухфакторная защита в почте, мессенджерах и на государственном портале.
- Я сохранил резервные коды восстановления в надёжном месте.
- Я время от времени проверяю список активных сеансов и подключённых устройств.

Устройства и сети:

- На моём телефоне и компьютере включены обновления.

- Я устанавливаю приложения только из официальных источников и проверяю их разрешения.
- На телефоне стоит блокировка экрана и включён поиск устройства.
- Я не выполняю важных операций через общественный Wi-Fi без необходимости.
- Я делаю резервные копии важных данных.

Мессенджеры и общение:

- Мой номер телефона и профиль скрыты от посторонних настолько, насколько это возможно.
- Я проверяю, с кем общаюсь, и перезваниваю по известному номеру, если «знакомый» просит денег или данных.
- Я не открываю неожиданные файлы и не устанавливаю приложения из переписки.
- Я не публикую в рабочих и общих чатах лишние персональные данные — свои и чужие.

Если что-то случилось:

- Я сразу звоню в банк по официальному номеру и прошу заблокировать карту.
- Я восстанавливаю доступ к учётным записям официальными способами и меняю пароли.
- Я рассматриваю возможность установить самозапрет на кредиты и проверяю свою кредитную историю.
- Я предупреждаю близких и коллег, если от моего имени могут писать мошенники.
- Я сохраняю доказательства и обращаюсь в полицию, если от моего имени совершаются противоправные действия.
- Я знаю, что могу направить обращение о своих персональных данных организации, которая их обрабатывает, в порядке, описанном в её политике.

Заключение к приложениям

Cookie, веб-хранилища, пиксели и встроенные элементы — обычная часть устройства современного интернета. Сами по себе они не хороши и не плохи: всё зависит от того, для чего и насколько прозрачно они используются. Понимание того, как они работают, позволяет осознанно решать, на что давать согласие, а от чего отказываться, и пользоваться инструментами управления, которые есть в каждом браузере.

Точно так же безопасность персональных данных — это не только задача организаций, которые их обрабатывают, но и привычки самого человека. Большинство неприятностей можно предотвратить несколькими простыми правилами: не сообщать коды, проверять адреса и собеседников, не торопиться под давлением, беречь документы и включать двухфакторную защиту. Эти правила одинаково полезны курьеру, кандидату на вакансию, клиенту и любому пользователю интернета.

Ещё раз напомним, что настоящие приложения являются справочными. Порядок и условия обработки персональных данных определяются Политикой обработки персональных данных, а сведения о том, какие технологии использует сайт, — Политикой использования cookie.

Приложение 7. Вопросы и ответы

Справочный материал. Не является частью Политики и не устанавливает обязательств Оператора. Сведения о том, какие данные обрабатывает Оператор, в каких целях и в какие сроки, содержатся только в Политике (раздел I).

Это приложение носит справочный и просветительский характер. Оно не является частью Политики обработки персональных данных и не меняет ни её положений, ни условий Согласия на обработку персональных данных. Здесь простыми словами объясняются понятия, с которыми человек сталкивается, когда оставляет свои данные на сайте, откликается на вакансию или работает курьером. Если ответ ниже расходится с текстом Политики или Согласия, применяется текст Политики и Согласия. На вопросы о том, как именно поступает компания, приложение не отвечает по существу, а указывает, где это описано.

Что такое персональные данные?

Персональные данные — это любая информация, которая относится к конкретному человеку и позволяет прямо или косвенно его определить. Очевидные примеры — фамилия, имя, отчество, номер телефона, адрес электронной почты, паспортные данные. Но к персональным данным может относиться и менее очевидная информация: сведения об опыте работы, фотография, история переписки, адрес, по которому человек живёт, если всё это можно связать с ним.

Важно понимать, что одна и та же информация может быть персональными данными в одной ситуации и не быть ими в другой. Например, само по себе слово «Иван» никого не определяет. А сочетание имени, номера телефона и города уже указывает на конкретного человека. Поэтому закон определяет персональные данные широко, а оценка всегда делается с учётом того, можно ли по совокупности сведений понять, о ком идёт речь.

Кто такой оператор персональных данных?

Оператор — это организация или человек, который сам или совместно с другими решает, зачем обрабатываются персональные данные, какие именно данные нужны и что с ними делается. Проще говоря, оператор — это тот, кто отвечает за обработку и определяет её правила. Для сайта, на котором вы оставляете заявку, оператором обычно является компания, которой этот сайт принадлежит.

Оператор не обязательно делает всё своими руками. Он может поручить часть работы другой организации — например, хостинг-провайдеру или сервису рассылок. В этом случае ответственность перед человеком всё равно несёт оператор, а тот, кому поручена обработка, действует по его поручению и в его интересах. Кто является оператором в отношении ваших данных, указано в Политике и в Согласии на обработку персональных данных.

Что значит «обработка» персональных данных?

В законе обработка понимается очень широко. Это практически любое действие с данными: сбор, запись, систематизация, накопление, хранение, уточнение, извлечение, использование, передача, обезличивание, блокирование, удаление и уничтожение. Даже простое хранение анкеты в базе данных уже считается обработкой.

Такое широкое определение сделано намеренно. Оно не позволяет организации сказать: «мы ничего с вашими данными не делаем, просто храним». Хранение — тоже обработка, и на него распространяются все требования закона, включая требования к защите и к срокам.

Зачем вообще нужно согласие на обработку персональных данных?

Согласие — это один из законных способов, которые позволяют организации обрабатывать ваши данные. Российское законодательство исходит из того, что информация о человеке принадлежит прежде всего ему, и обрабатывать её можно только при наличии законного основания. Согласие — самое понятное из таких оснований: человек сам говорит «да, я разрешаю использовать мои данные для этой цели».

Для самого человека согласие — это ещё и инструмент контроля. Оно фиксирует, для чего именно разрешено использовать данные, какие данные, какими способами и на какой срок. Если организация выходит за эти рамки, она нарушает закон. Поэтому согласие полезно читать: оно определяет границы того, что с вашими данными можно делать.

Согласие — это единственное основание для обработки?

Нет. Закон перечисляет несколько оснований, и согласие — лишь одно из них. Данные можно обрабатывать, например, если это нужно для заключения или исполнения договора, стороной которого является сам человек, если обработка необходима для выполнения обязанностей, которые возлагает на организацию закон, или в некоторых других случаях, прямо предусмотренных законом.

Это значит, что в отдельных ситуациях организация обрабатывает данные не потому, что вы дали согласие, а потому, что так требует закон. Например, работодатель обязан хранить определённые кадровые документы установленное время. На какие именно основания опирается компания в каждом случае, описано в Политике.

Можно ли не давать согласие и что тогда будет?

Да, давать согласие или нет — ваше право. Согласие по закону должно быть свободным: никто не может заставить вас его подписать. Вы вправе отказаться, и за сам отказ вас не могут наказать.

Однако у отказа есть естественные последствия. Если для какого-то действия данные действительно нужны, без них это действие невозможно. Например, нельзя рассмотреть отклик на вакансию, не зная, как связаться с кандидатом, и нельзя доставить посылку, не зная адреса. В таком случае организация просто не сможет оказать услугу или продолжить общение. Какие последствия наступают при отказе от согласия в отношении сервисов компании, описано в Согласии на обработку персональных данных и в Политике.

Что значит «отозвать согласие»?

Отозвать согласие — значит сообщить оператору, что вы больше не разрешаете обрабатывать ваши данные на основании ранее данного согласия. Это право прямо закреплено в законе, и оно действует в любой момент. Причину объяснять не нужно.

После отзыва оператор должен прекратить обработку и уничтожить данные в установленный законом срок, если у него нет другого законного основания продолжать обработку. Отзыв действует на будущее: он не делает незаконным то, что было сделано, пока согласие действовало. Как именно направить отзыв в компанию и куда, описано в Политике и в Согласии на обработку персональных данных.

Если я отозвал согласие, все мои данные удалят сразу?

Не всегда. Если обработка шла только на основании согласия, то после отзыва оператор должен прекратить её и уничтожить данные, как правило, в течение тридцати дней. Но если у оператора есть другое законное основание — например, обязанность хранить документы по закону или исполнение

договора, который ещё действует, — часть данных может храниться дальше, но только в объёме и на срок, которые нужны для этой другой цели.

Это не обход закона, а прямо предусмотренная им ситуация. Например, бухгалтерские и кадровые документы организация обязана хранить определённое время независимо от желания человека. Какие данные и на каком основании компания продолжает хранить после отзыва, описано в Политике.

Чем согласие отличается от политики?

Политика обработки персональных данных — это общий документ организации. В нём описаны её правила: какие категории данных она обрабатывает, для каких целей, на каких основаниях, как защищает данные и какие права есть у людей. Политику публикуют открыто, чтобы любой мог с ней ознакомиться. Сама по себе политика ничего не разрешает: это описание правил, а не ваше волеизъявление.

Согласие — это ваше личное решение, выраженное в отношении конкретной обработки. Его даёт человек, а не организация. Согласие должно быть конкретным, предметным, информированным, сознательным и однозначным. Иначе говоря, политика отвечает на вопрос «как здесь устроена работа с данными», а согласие — на вопрос «разрешаю ли я лично использовать мои данные вот так».

Почему согласие часто оформляется галочкой на сайте?

Закон допускает получение согласия в любой форме, позволяющей подтвердить факт его получения, если законом не требуется письменная форма. На сайте удобнее всего зафиксировать согласие отдельной отметкой рядом с формой, со ссылкой на текст согласия. Система сохраняет сведения о том, что отметка была поставлена.

Есть случаи, когда закон требует письменного согласия, — например, для некоторых особых категорий данных или для отдельных видов обработки. Письменная форма может быть и электронной, если она подписана электронной подписью в установленном порядке. Какая форма согласия используется в сервисах компании, указано в Согласии на обработку персональных данных.

Зачем работодателю данные кандидата?

Когда человек откликается на вакансию, работодателю нужно понять, подходит ли кандидат, и связаться с ним. Для этого используются контактные данные, сведения об опыте, о желаемом графике, о городе. Без этой информации подбор просто невозможен: нельзя пригласить на собеседование человека, о котором ничего не известно.

Закон при этом ограничивает работодателя. Данные кандидата можно использовать только для целей, связанных с подбором, и только в нужном объёме. Работодатель не вправе собирать сведения, которые не относятся к делу, — например, о политических взглядах или частной жизни, если это не связано с работой. Какие именно данные кандидатов собирает компания и зачем, описано в Политике и в Согласии на обработку персональных данных.

Что происходит с данными кандидата, которого не взяли на работу?

По общему правилу данные должны храниться не дольше, чем этого требует цель обработки. Если цель — рассмотрение конкретного отклика — достигнута, данные нужно уничтожить или обезличить, если нет другого основания для хранения. Таким основанием может быть, например, согласие кандидата на включение в кадровый резерв.

Конкретные сроки хранения данных кандидатов в компании и порядок их уничтожения описаны в Политике. Если вы хотите, чтобы ваши данные были удалены раньше, вы можете направить соответствующее обращение в порядке, указанном в Политике.

Можно ли узнать, какие данные обо мне хранятся?

Да. Это одно из основных прав, которые закон даёт человеку. Вы можете запросить у оператора сведения о том, обрабатывает ли он ваши данные, какие именно, для каких целей, на каком основании, каким способом, кому они передаются, сколько будут храниться и где можно получить дополнительные разъяснения.

Оператор обязан ответить в срок, установленный законом. Сейчас это десять рабочих дней с момента получения запроса, причём срок может быть продлён ещё не более чем на пять рабочих дней, если оператор направит человеку мотивированное уведомление о причинах продления. Сведения должны быть изложены в доступной форме и не должны содержать данных о других людях. Как направить такой запрос в компанию, описано в Политике.

Что должно быть в запросе о моих данных?

Закон требует, чтобы запрос позволял установить, кто его направил, и подтвердить, что этот человек действительно связан с оператором. Обычно в запросе указывают данные документа, удостоверяющего личность, сведения о том, как человек взаимодействовал с оператором (например, откликнулся на вакансию или оставлял заявку), и подпись — собственноручную или электронную.

Такие требования нужны для вашей же защиты. Если бы оператор отвечал любому, кто назовёт ваше имя, посторонний человек мог бы получить сведения о вас. Поэтому оператор вправе убедиться, что запрос исходит именно от вас. Конкретный адрес и способ направления запросов в компанию указаны в Политике.

Можно ли потребовать исправить неверные данные?

Да. Если данные неполные, устаревшие или неточные, вы вправе потребовать их уточнения. Оператор обязан внести изменения, если вы предоставите сведения, подтверждающие, что данные действительно неверны. Обычно это делается быстро, особенно если речь идёт о контактной информации.

Право на уточнение важно не только для вас, но и для самого оператора: работа с неверными данными приводит к ошибкам, например к звонкам не тому человеку или доставке не по адресу. Закон прямо требует, чтобы обрабатываемые данные были точными и достаточными для целей обработки.

Можно ли потребовать удалить мои данные?

Вы можете потребовать уничтожения данных, если они обрабатываются незаконно, если они не нужны для заявленной цели или если вы отозвали согласие, а другого основания для обработки нет. Оператор обязан рассмотреть такое требование и сообщить о результате.

Однако «право на удаление» в российском законе не абсолютно. Если хранение данных требуется по закону или для исполнения договора, оператор вправе отказать в удалении этой части данных, объяснив причину. Порядок рассмотрения таких требований компанией описан в Политике.

Почему сайт показывает окно про cookie?

Cookie — это небольшие файлы, которые сайт сохраняет в вашем браузере. Они помогают запоминать настройки, поддерживать вход в личный кабинет, считать посещаемость и понимать, какие страницы полезны. Часть cookie технически необходима для работы сайта, а часть используется для аналитики.

Сами по себе cookie обычно не содержат имени или телефона. Но в сочетании с другими сведениями — например, с IP-адресом, данными о браузере и действиями на сайте — они могут относиться к конкретному человеку. Поэтому многие сайты в России заранее сообщают об их использовании и просят согласия, чтобы обработка была прозрачной. Какие cookie и аналитические сервисы использует сайт компании, описано в Политике.

Что будет, если отказаться от cookie?

Обычно сайт продолжит работать, но некоторые функции могут стать менее удобными. Например, сайт может не запомнить выбранный город или настройки. Если отказаться и от технически необходимых cookie, отдельные функции — вход в личный кабинет, отправка форм — могут перестать работать.

Управлять cookie можно и в настройках самого браузера: удалить уже сохранённые файлы, запретить их сохранение для отдельных сайтов или включить режим, при котором они удаляются после закрытия окна. Это ваш выбор, и он не требует ни у кого разрешения.

Что такое трансграничная передача персональных данных?

Трансграничная передача — это передача персональных данных на территорию иностранного государства: иностранному государственному органу, иностранной организации или иностранному гражданину. Иными словами, если данные уходят за пределы России к получателю за рубежом, это трансграничная передача.

Закон регулирует её отдельно, потому что за рубежом действует иное право и российский человек может иметь там меньше возможностей защитить свои интересы. Поэтому оператор, прежде чем начать такую передачу, должен оценить, насколько надёжно данные будут защищены в стране получателя, и уведомить Роскомнадзор. Происходит ли трансграничная передача в деятельности компании и в каких случаях, описано в Политике.

Почему мессенджеры относятся к трансграничной передаче?

Многие популярные мессенджеры и почтовые сервисы принадлежат иностранным компаниям, а их серверы находятся за пределами России. Когда организация пересылает через такой мессенджер, например, данные кандидата или клиента, эти данные физически попадают на серверы за рубежом и обрабатываются иностранной компанией.

С точки зрения закона это может квалифицироваться как трансграничная передача, даже если отправитель и получатель сообщения находятся в одном городе. Поэтому организации всё чаще внимательно подходят к выбору каналов связи и описывают в своих документах, какими сервисами пользуются. Какие каналы связи использует компания и как это отражено в её документах, описано в Политике.

Что такое локализация баз данных в России?

Локализация — это требование закона, согласно которому при сборе персональных данных граждан России, в том числе через интернет, оператор должен обеспечить их запись, систематизацию, накопление, хранение, уточнение и извлечение с использованием баз данных, находящихся на территории России. Требование действует с 1 сентября 2015 года.

Важно понимать, что локализация не запрещает трансграничную передачу как таковую. Она требует, чтобы первичная база данных — та, в которую данные собираются и в которой они накапливаются, — находилась в России. Дальнейшая передача за рубеж возможна, но только с соблюдением отдельных правил. Как компания выполняет требование о локализации, описано в Политике.

Что делать, если я подозреваю утечку моих данных?

Сначала стоит понять, что именно произошло. Признаки утечки — звонки и сообщения от незнакомых людей, которые знают о вас то, что вы сообщали конкретной организации, письма о сбросе паролей, которых вы не запрашивали, уведомления сервисов о входе с незнакомого устройства.

Если вы считаете, что ваши данные утекли от конкретной организации, вы вправе обратиться к ней с запросом и потребовать разъяснений. Кроме того, можно подать обращение в Роскомнадзор — орган, который контролирует соблюдение законодательства о персональных данных. Параллельно разумно сменить пароли, включить двухфакторную аутентификацию там, где это возможно, и с осторожностью относиться к звонкам от «службы безопасности банка» и похожих собеседников.

Что обязана сделать организация при утечке?

Закон требует, чтобы оператор, обнаруживший неправомерную или случайную передачу персональных данных, которая повлекла нарушение прав людей, уведомил Роскомнадзор. Первичное уведомление направляется в течение двадцати четырёх часов с момента выявления инцидента, а сведения о результатах внутреннего расследования — в течение семидесяти двух часов.

Кроме того, оператор должен устранить последствия инцидента, выяснить его причины и принять меры, чтобы подобное не повторилось. Порядок действий компании при инцидентах описан в Политике.

Как понять, что организация защищает данные?

Снаружи это не всегда видно, но есть косвенные признаки. Добросовестная организация публикует политику обработки данных, объясняет, зачем ей нужна та или иная информация, не просит лишнего, даёт понятный способ связаться по вопросам данных и отвечает на запросы в срок.

Внутри защита включает организационные меры (назначение ответственного, внутренние правила, ограничение доступа сотрудников) и технические меры (шифрование, резервное копирование, контроль доступа, журналы событий). Конкретные меры, которые принимает компания, в общих чертах описаны в Политике.

Что такое редакция документа и почему у документов есть дата?

Редакция — это конкретная версия документа. Правила обработки данных со временем меняются: обновляется законодательство, появляются новые сервисы, меняются процессы. Поэтому документ периодически пересматривают и выпускают новую редакцию. Дата показывает, с какого момента действует текущая версия.

Дата нужна, чтобы можно было точно сказать, какие правила действовали в определённый момент. Если вы дали согласие год назад, важно понимать, на каких условиях это было сделано. Поэтому оператор обычно хранит предыдущие редакции, а актуальная версия всегда публикуется на видном месте.

Почему политика может меняться без моего согласия?

Политика — это документ самой организации, описывающий её внутренние правила. Организация вправе его обновлять, например, чтобы привести в соответствие с изменившимся законом или с новыми процессами. При этом изменение политики не может само по себе расширить то, на что вы дали согласие.

Если организация хочет обрабатывать ваши данные для новой цели, которая требует согласия, ей нужно получить новое согласие. Политика же лишь информирует о правилах. Порядок внесения изменений в Политику и информирования о них описан в самой Политике.

Что такое обезличивание?

Обезличивание — это действия, в результате которых становится невозможно без дополнительной информации определить, к какому конкретному человеку относятся данные. Например, в статистике вместо фамилий используются условные номера, а таблица соответствия хранится отдельно и под защитой.

Обезличивание полезно, когда организации нужна общая картина — сколько заявок пришло, из каких городов, сколько времени заняла доставка, — но не нужны сведения о конкретных людях. Это снижает риски: даже если обезличенный набор данных станет доступен посторонним, установить личности по нему значительно труднее.

Чем уничтожение данных отличается от удаления?

В законе используется термин «уничтожение» — это действия, в результате которых становится невозможно восстановить содержание персональных данных, и (или) уничтожаются материальные носители. Простое перемещение файла в корзину или скрытие записи в интерфейсе уничтожением не является, если данные можно вернуть.

Факт уничтожения оператор должен подтвердить в порядке, установленном уполномоченным органом. Обычно для этого оформляется акт, а при автоматизированной обработке — ещё и выгрузка из журнала событий. Порядок уничтожения в компании описан в Политике.

Что такое блокирование данных?

Блокирование — это временное прекращение обработки данных, кроме случаев, когда обработка нужна для уточнения данных. Например, если человек сообщил, что его данные неточны, оператор может заблокировать их на время проверки, чтобы не использовать неверную информацию.

Блокирование — промежуточная мера. По её итогам данные либо уточняются и обработка продолжается, либо, если обработка была неправомерной, данные уничтожаются.

Что такое специальные категории персональных данных?

Это наиболее чувствительные сведения: о расовой и национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, интимной жизни, а также о судимости. Закон по общему правилу запрещает их обработку, допуская её лишь в прямо перечисленных случаях, например при письменном согласии человека или когда это требуется по закону.

Работодатель, например, в некоторых случаях вправе обрабатывать сведения о состоянии здоровья, если они относятся к возможности выполнения работником трудовой функции. Но и здесь действуют строгие рамки. Обрабатывает ли компания специальные категории данных, описано в Политике.

Что такое биометрические персональные данные?

Биометрические данные — это сведения, которые характеризуют физиологические и биологические особенности человека и используются оператором для установления личности. Классический пример — изображение лица, используемое системой распознавания, или отпечатки пальцев.

Важная деталь: обычная фотография в анкете сама по себе ещё не биометрия. Она становится биометрическими данными, когда используется именно для установления личности, например автоматическим сравнением с эталоном. Обработка биометрии допускается, как правило, только с письменного согласия человека. Обрабатывает ли компания биометрические данные, описано в Политике.

Что такое общедоступные персональные данные?

Раньше закон позволял обрабатывать данные, которые человек сам сделал общедоступными, без отдельного согласия. С 1 марта 2021 года правила изменились: для распространения персональных данных — то есть раскрытия их неопределённому кругу лиц — требуется отдельное согласие, оформляемое отдельно от других согласий.

Это означает, что сам факт того, что информация о вас где-то опубликована, не даёт любому желающему права свободно её использовать и распространять. В таком согласии человек может установить запреты и условия на дальнейшую обработку своих данных.

Почему для распространения данных нужно отдельное согласие?

Распространение — это раскрытие данных неограниченному кругу людей, например публикация на сайте или в открытом канале. Последствия такой публикации гораздо серьёзнее, чем у обычной обработки внутри организации: данные могут скопировать и использовать кто угодно.

Поэтому законодатель выделил это согласие в отдельный документ, чтобы человек не дал его случайно, «заодно» с другими согласиями. В нём человек вправе указать, какие данные можно распространять, а какие нет, и запретить их передачу третьим лицам.

Что такое поручение обработки?

Поручение — это ситуация, когда оператор доверяет обработку данных другой организации на основании договора. Например, оператор может пользоваться услугами облачного хостинга, сервиса рассылок, бухгалтерской фирмы. Эти организации обрабатывают данные не для своих целей, а по заданию оператора.

Закон требует, чтобы в поручении были указаны перечень действий с данными, цели обработки, обязанность соблюдать конфиденциальность и требования к защите. Ответственность перед человеком несёт оператор. Кому компания поручает обработку данных, описано в Политике.

Что такое конфиденциальность персональных данных?

Конфиденциальность означает обязанность операторов и иных лиц, получивших доступ к персональным данным, не раскрывать их третьим лицам и не распространять без согласия человека, если иное не предусмотрено законом. Это базовое требование, которое действует независимо от того, подписывал ли человек что-то дополнительно.

На практике это значит, что сотрудник организации не может, например, сообщить номер телефона кандидата своему знакомому или опубликовать данные клиента в открытом доступе. Нарушение этой обязанности может повлечь ответственность.

Почему меня просят подтвердить согласие ещё раз?

Повторный запрос согласия бывает в нескольких случаях: изменилась цель обработки, понадобились новые категории данных, обновилась редакция документа так, что затронуты условия согласия, или прежнее согласие истекло. Кроме того, для разных целей могут требоваться разные согласия.

Это не формальность, а способ сохранить прозрачность: вы каждый раз заново решаете, согласны ли вы на изменившиеся условия. Если не согласны — вы вправе отказаться.

Кто может видеть мои данные внутри организации?

Закон требует ограничивать доступ к персональным данным: работать с ними должны только те сотрудники, которым это нужно для выполнения своих обязанностей. Например, данные кандидата нужны тому, кто ведёт подбор, но не обязательно всем остальным сотрудникам.

Порядок допуска сотрудников к данным, их обязанности по сохранению конфиденциальности и меры контроля определяются внутренними документами оператора. Общие принципы организации доступа в компании описаны в Политике.

Что такое ответственный за организацию обработки персональных данных?

Закон обязывает оператора-организацию назначить лицо, ответственное за организацию обработки персональных данных. Этот человек следит за соблюдением законодательства внутри организации, доводит до сотрудников правила работы с данными и организует приём и обработку обращений граждан.

Наличие такого ответственного делает работу с данными управляемой: есть конкретный человек, который отвечает за порядок, а не «все и никто». Способ связи по вопросам обработки персональных данных в компании указан в Политике.

Можно ли передавать мои данные третьим лицам без моего ведома?

По общему правилу — нет. Передача третьим лицам допускается при наличии законного основания: согласия человека, требования закона, необходимости исполнить договор с человеком и других случаев, прямо указанных в законе. Например, по законному запросу суда или правоохранительных органов организация обязана предоставить сведения.

Человек вправе знать, кому передаются его данные. Именно поэтому в ответе на запрос о данных оператор должен указать получателей или их категории. Кому компания передаёт данные, описано в Политике и в Согласии на обработку персональных данных.

Почему курьерской службе нужен адрес и телефон получателя?

Это прямо следует из сути услуги: доставить отправление можно только по конкретному адресу и связаться с получателем, чтобы договориться о времени или уточнить детали. Без этих сведений услуга невыполнима.

Одновременно это хороший пример принципа минимизации: для доставки нужны адрес и способ связи, но, как правило, не нужны многие другие сведения о получателе. Какие данные клиентов и получателей обрабатывает компания и сколько их хранит, описано в Политике.

Что такое принцип минимизации данных?

Закон требует, чтобы содержание и объём обрабатываемых данных соответствовали заявленным целям и не были избыточными. Если для цели достаточно имени и телефона, не нужно спрашивать дату рождения и паспорт.

Этот принцип защищает и человека, и саму организацию. Чем меньше лишних данных хранится, тем меньше ущерб в случае инцидента и тем проще соблюдать требования к хранению и уничтожению.

Что значит «ограничение цели»?

Данные собираются для конкретных, заранее определённых и законных целей. Использовать их для другой, несовместимой цели нельзя. Например, данные, собранные для рассмотрения отклика на вакансию, нельзя без отдельного основания использовать для рекламных рассылок.

Поэтому в документах оператора цели перечисляются явно. Это не бюрократия, а рамка, которая определяет, что с данными можно делать, а что нельзя. Цели обработки данных компанией перечислены в Политике.

Сколько времени можно хранить персональные данные?

Закон не устанавливает единого срока для всех случаев. Общее правило — хранить данные в форме, позволяющей определить человека, не дольше, чем этого требуют цели обработки, если срок не установлен законом или договором. Для отдельных видов документов, например кадровых и бухгалтерских, сроки хранения установлены специальными нормативными актами.

После достижения цели или истечения срока данные должны быть уничтожены или обезличены. Сроки хранения различных категорий данных в компании описаны в Политике.

Какие права у меня есть, если мои права нарушены?

Вы вправе обратиться к оператору с требованием устранить нарушение. Если это не помогло или вы не хотите обращаться к оператору, можно подать жалобу в Роскомнадзор, который рассмотрит её и при необходимости проведёт проверку или примет меры.

Кроме того, вы вправе защищать свои права в суде, в том числе требовать возмещения убытков и компенсации морального вреда. Закон прямо предусматривает, что моральный вред, причинённый нарушением правил обработки персональных данных, подлежит возмещению независимо от возмещения имущественного вреда.

Что такое Роскомнадзор и чем он может помочь?

Роскомнадзор — Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций. В сфере персональных данных это уполномоченный орган по защите прав субъектов персональных данных. Он ведёт реестр операторов, принимает уведомления, проводит контрольные мероприятия и рассматривает обращения граждан.

Если вы считаете, что ваши данные обрабатываются незаконно, вы можете направить обращение в Роскомнадзор, в том числе через его официальный сайт. Служба вправе потребовать от оператора уточнить, заблокировать или уничтожить недостоверные или незаконно полученные данные.

Что такое реестр операторов?

Это публичный перечень организаций и лиц, которые уведомили Роскомнадзор о том, что обрабатывают персональные данные. В нём указываются, например, цели обработки, категории данных, правовые основания, сведения о месте нахождения баз данных и о трансграничной передаче.

Любой человек может проверить, есть ли интересующая его организация в реестре, и узнать, какие сведения о своей обработке она заявила. Это ещё один инструмент прозрачности.

Нужно ли мне самому что-то делать, чтобы мои данные были защищены?

Основные обязанности по защите лежат на операторе, но разумная осторожность никогда не помешает. Не стоит отправлять копии документов через случайные каналы, если организация предлагает защищённый способ. Полезно проверять, что вы находитесь на настоящем сайте организации, а не на поддельной странице.

Стоит также помнить, что организации, как правило, не запрашивают пароли, коды из СМС и данные банковских карт в мессенджерах и по телефону. Если кто-то делает это от имени работодателя или службы доставки, лучше прервать разговор и проверить информацию по официальным каналам.

Что делать, если мне звонят и называют себя сотрудником службы доставки?

Если звонок неожиданный, а собеседник просит назвать код из СМС, перейти по ссылке или оплатить «доставку» по реквизитам, это типичные признаки мошенничества. Настоящий курьер может уточнить адрес и время, но код подтверждения из банковского приложения ему не нужен.

Если сомневаетесь, завершите звонок и свяжитесь с организацией по контактам, указанным на её официальном сайте. Такая проверка занимает пару минут и защищает от наиболее распространённых схем обмана.

Если я курьер, то какие права на мои данные есть у компании?

У компании, с которой вы взаимодействуете как курьер, есть право обрабатывать данные, которые нужны для оформления отношений, выплат, организации работы и выполнения требований закона. Объём зависит от формы отношений: трудовой договор, гражданско-правовой договор или иная форма.

При этом ваши права как субъекта персональных данных сохраняются в полной мере: вы вправе знать, какие данные обрабатываются, требовать их уточнения и обращаться с вопросами. Какие данные курьеров обрабатывает компания и для каких целей, описано в Политике и в Согласии на обработку персональных данных.

Может ли работодатель получать данные обо мне от третьих лиц?

Трудовой кодекс устанавливает, что все персональные данные работника следует получать у него самого. Если данные можно получить только у третьей стороны, работник должен быть заранее об этом уведомлен и дать письменное согласие. Работодатель должен сообщить, о целях, источниках и способах получения данных.

Это правило защищает работника от сбора сведений «за спиной». Получает ли компания какие-либо данные из других источников, описано в Политике.

Что такое геолокация и относится ли она к персональным данным?

Геолокация — это сведения о местоположении устройства. Если устройство связано с конкретным человеком, сведения о его перемещениях являются персональными данными. В курьерской работе геолокация может использоваться, например, для построения маршрутов и контроля доставки.

Как и любые персональные данные, геолокация должна обрабатываться на законном основании, для определённых целей и в необходимом объёме. Используется ли геолокация в сервисах компании, описано в Политике.

Почему не стоит пересылать фото паспорта в открытых чатах?

Фото паспорта — это набор сведений, которых достаточно для многих мошеннических действий. Открытый или групповой чат легко пересылается, копируется и может оказаться у посторонних. Даже если чат кажется закрытым, у его участников могут быть заражённые устройства.

Если организации действительно нужна копия документа, она должна предложить защищённый способ её передачи и объяснить, зачем она нужна. Как компания запрашивает и хранит документы, описано в Политике.

Что делать, если у меня остались вопросы?

Если что-то в этом приложении или в документах осталось непонятным, лучше задать вопрос, чем гадать. Способ связи по вопросам обработки персональных данных указан в Политике. В обращении стоит прямо написать, что именно непонятно, — так ответ будет точнее.

Помните, что задать вопрос о своих данных — ваше законное право, и для этого не нужно объяснять причины.

Приложение 8. Обзор законодательства Российской Федерации о персональных данных

Справочный материал. Не является частью Политики и не устанавливает обязательств Оператора. Сведения о том, какие данные обрабатывает Оператор, в каких целях и в какие сроки, содержатся только в Политике (раздел I).

Это приложение даёт общее представление о том, как устроено российское законодательство о персональных данных. Оно не является юридической консультацией и не заменяет чтения самих нормативных актов. Законодательство в этой сфере регулярно меняется, поэтому для решения конкретных вопросов всегда нужно сверяться с актуальными редакциями документов.

Конституция Российской Федерации

Основа всего регулирования заложена в Конституции. Она закрепляет право каждого на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени, а также на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение тайны связи допускается только на основании судебного решения.

Отдельно Конституция устанавливает, что сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются. Это положение можно считать конституционным корнем всей идеи согласия на обработку персональных данных. Кроме того, органы власти и должностные лица обязаны обеспечить каждому возможность ознакомиться с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.

Конституционные нормы сформулированы в общем виде. Они задают ценности и рамку, а конкретные правила устанавливают федеральные законы. При этом в случае сомнений при толковании законов суды и органы власти исходят из того, что частная жизнь человека находится под защитой, а её ограничение должно быть обоснованным и соразмерным.

Конституция также допускает ограничение прав и свобод федеральным законом, но только в той мере, в какой это необходимо для защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства. Именно поэтому в законах о персональных данных встречаются случаи, когда данные можно обрабатывать без согласия: такие исключения должны иметь законную и обоснованную цель.

Федеральный закон «О персональных данных»

Центральный акт в этой сфере — Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных». Он регулирует отношения, связанные с обработкой персональных данных государственными органами, органами местного самоуправления, юридическими и физическими лицами, как с использованием средств автоматизации, так и без них, если обработка без автоматизации по своему характеру соответствует автоматизированной.

Целью закона названо обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну. Закон многократно изменялся. Особенно заметные изменения вступили в силу в 2015 году (локализация), в 2021 году (отдельное согласие на распространение) и в 2022–2023 годах (расширение сферы действия, новые правила трансграничной передачи, обязанности при утечках, сокращение сроков ответа на запросы).

Структура закона в общих чертах такова. Сначала идут общие положения: сфера действия, цель,

основные понятия. Затем — принципы и условия обработки, в том числе положения о согласии, о специальных категориях и биометрических данных, о трансграничной передаче. Далее следуют права субъекта персональных данных, обязанности оператора, положения о государственном контроле и надзоре и об ответственности.

Основные понятия закона

Закон вводит ряд понятий, на которых строится всё регулирование. Персональные данные — любая информация, относящаяся к прямо или косвенно определённом или определяемому физическому лицу. Субъект персональных данных — это сам человек, к которому относятся данные. Оператор — лицо, самостоятельно или совместно с другими организующее и (или) осуществляющее обработку, а также определяющее её цели, состав данных и действия с ними.

Обработка определена как любое действие или совокупность действий с персональными данными: сбор, запись, систематизация, накопление, хранение, уточнение, извлечение, использование, передача (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение. Отдельно определены автоматизированная обработка, распространение (действия, направленные на раскрытие данных неопределённому кругу лиц) и предоставление (раскрытие определённом лицу или кругу лиц).

Закон также определяет блокирование как временное прекращение обработки, кроме случаев, когда обработка необходима для уточнения данных; уничтожение — как действия, в результате которых невозможно восстановить содержание данных в информационной системе и (или) уничтожаются материальные носители; обезличивание — как действия, в результате которых невозможно без дополнительной информации определить принадлежность данных конкретному субъекту. Ещё одно важное понятие — информационная система персональных данных, то есть совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Принципы обработки

Закон устанавливает принципы, которые должны соблюдаться при любой обработке. Обработка должна быть законной и справедливой. Она должна ограничиваться достижением конкретных, заранее определённых и законных целей. Не допускается обработка, несовместимая с целями сбора.

Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в несовместимых между собой целях. Обработке подлежат только те данные, которые отвечают целям обработки, а их содержание и объём должны соответствовать заявленным целям и не быть избыточными. При обработке должна обеспечиваться точность данных, их достаточность и, в необходимых случаях, актуальность. Оператор должен принимать меры по удалению или уточнению неполных или неточных данных.

Хранение данных должно осуществляться в форме, позволяющей определить субъекта, не дольше, чем этого требуют цели обработки, если срок не установлен законом или договором. По достижении целей или в случае утраты необходимости в их достижении данные подлежат уничтожению или обезличиванию, если иное не предусмотрено законом.

Эти принципы на первый взгляд выглядят общими, но на практике они являются рабочими критериями. Именно на них ссылаются надзорные органы и суды, оценивая, была ли обработка правомерной. Например, сбор лишних данных «на всякий случай» нарушает принцип соответствия объёма данных целям, даже если человек формально дал согласие.

Условия обработки и согласие

Закон перечисляет случаи, когда обработка допускается. Это обработка с согласия субъекта; обработка, необходимая для достижения целей, предусмотренных международным договором или законом, для выполнения возложенных на оператора законом функций и обязанностей; для осуществления правосудия и исполнения судебных актов; для исполнения договора, стороной которого, выгодоприобретателем или поручителем по которому является субъект, а также для заключения договора по его инициативе; для защиты жизни, здоровья или иных жизненно важных интересов субъекта; для осуществления прав и законных интересов оператора или третьих лиц при условии, что не нарушаются права субъекта; и ряд других случаев.

Согласие должно быть конкретным, предметным, информированным, сознательным и однозначным. Оно может быть дано самим субъектом или его представителем в любой позволяющей подтвердить факт его получения форме, если законом не установлено иное. Обязанность доказать получение согласия или наличие иного основания лежит на операторе.

В случаях, прямо предусмотренных законом, требуется письменное согласие. Закон определяет его обязательные элементы: сведения о субъекте и операторе, цель обработки, перечень данных, перечень действий и общее описание способов обработки, срок действия согласия и способ его отзыва, а также, если обработка поручается другому лицу, сведения об этом лице. равнозначным письменному считается согласие в форме электронного документа, подписанного электронной подписью в соответствии с законодательством.

Согласие может быть отозвано. В случае отзыва оператор вправе продолжить обработку без согласия только при наличии иных оснований, указанных в законе. При отсутствии таких оснований оператор обязан прекратить обработку и уничтожить данные в срок, не превышающий тридцати дней с даты поступления отзыва, если иное не предусмотрено договором или соглашением с субъектом.

Согласие на распространение

С 1 марта 2021 года действует отдельная статья о данных, разрешённых субъектом для распространения. Согласие на обработку таких данных оформляется отдельно от иных согласий. Оператор обязан обеспечить субъекту возможность определить перечень данных по каждой категории, указанной в согласии.

Субъект вправе установить запреты на передачу данных неограниченному кругу лиц, а также запреты на обработку или условия обработки, кроме получения доступа. Молчание или бездействие субъекта ни при каких обстоятельствах не считается согласием на распространение. Если из согласия не следует, что субъект разрешил распространение, данные обрабатываются оператором без права распространения.

Субъект вправе в любой момент потребовать прекратить передачу (распространение, предоставление, доступ) таких данных. Это новшество было введено в ответ на массовую практику, когда сведения из открытых источников собирались и использовались без какого-либо контроля со стороны людей, которых они касались.

Специальные категории и биометрия

Отдельные статьи посвящены специальным категориям данных — касающимся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, — а также сведениям о судимости. Их обработка по общему правилу не

допускается, за исключением прямо перечисленных в законе случаев. К таким случаям относятся, например, письменное согласие субъекта или обработка в соответствии с трудовым законодательством, законодательством о социальном обеспечении и в некоторых других сферах.

Биометрические персональные данные — сведения, характеризующие физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для этого, — могут обрабатываться только при наличии письменного согласия, за исключением случаев, предусмотренных законом. Отказ субъекта дать согласие на обработку биометрии, как правило, не может служить основанием для отказа в обслуживании, если иное не установлено законом. Правила использования биометрии в целях идентификации дополнительно регулируются специальным законодательством.

Права субъекта персональных данных

Ключевое право субъекта — право на получение сведений об обработке своих данных. Закон перечисляет, что именно должно сообщаться: подтверждение факта обработки, правовые основания и цели, применяемые способы обработки, наименование и место нахождения оператора, сведения о лицах, которые имеют доступ к данным или которым они могут быть раскрыты, обрабатываемые данные и источник их получения, сроки обработки и хранения, порядок осуществления прав, информация о трансграничной передаче, сведения о лице, которому поручена обработка, и иные сведения.

Субъект вправе требовать уточнения своих данных, их блокирования или уничтожения, если они являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели, а также принимать предусмотренные законом меры по защите своих прав. Право на доступ может быть ограничено в случаях, указанных в законе, например если доступ нарушает права и законные интересы третьих лиц.

Закон отдельно регулирует принятие решений на основании исключительно автоматизированной обработки, порождающих юридические последствия или иным образом затрагивающих права и законные интересы человека. Такие решения допускаются только при наличии согласия в письменной форме или в случаях, предусмотренных законом. Оператор обязан разъяснить порядок принятия такого решения и возможные последствия, а также предоставить возможность заявить возражение.

Субъект также вправе обжаловать действия или бездействие оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке, если считает, что обработка нарушает требования закона или иным образом нарушает его права и свободы. Он имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и компенсацию морального вреда.

Обязанности оператора

Оператор обязан при сборе данных предоставить субъекту по его просьбе информацию об обработке. Если данные получены не от самого субъекта, оператор, за рядом исключений, обязан до начала обработки сообщить субъекту своё наименование, цель и основание обработки, предполагаемых пользователей, права субъекта и источник получения данных.

Оператор обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных законом. К таким мерам закон относит, в частности, назначение ответственного за организацию обработки, издание документа, определяющего политику оператора в отношении обработки персональных данных, локальных актов по вопросам обработки и по

предотвращению и выявлению нарушений, применение правовых, организационных и технических мер защиты, осуществление внутреннего контроля, оценку вреда, который может быть причинён субъектам, и ознакомление работников с требованиями законодательства и внутренними документами.

Оператор обязан опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки персональных данных, и к сведениям о реализуемых требованиях к защите. Если оператор собирает данные через интернет, он должен опубликовать такую политику на соответствующих страницах сайта, с использованием которых собираются данные. Именно поэтому на сайтах организаций размещаются политики обработки персональных данных.

Отдельная статья посвящена мерам по обеспечению безопасности при обработке. Оператор обязан принимать правовые, организационные и технические меры для защиты данных от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий. Закон перечисляет, в чём выражается обеспечение безопасности: определение угроз, применение мер защиты для выполнения требований к уровням защищённости, применение прошедших оценку соответствия средств защиты, оценка эффективности мер, учёт машинных носителей, обнаружение фактов несанкционированного доступа и реагирование на компьютерные инциденты, восстановление данных, установление правил доступа и контроль за принимаемыми мерами.

Оператор также обязан взаимодействовать с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак, включая информирование о компьютерных инцидентах, повлёкших неправомерную передачу персональных данных.

Ответы на запросы субъектов

Закон устанавливает сроки, в которые оператор обязан отвечать на обращения. После изменений, вступивших в силу в 2022 году, общий срок предоставления сведений субъекту составляет десять рабочих дней с момента обращения или получения запроса. Этот срок может быть продлён не более чем на пять рабочих дней, если оператор направит субъекту мотивированное уведомление с указанием причин продления.

Если оператор отказывает в предоставлении сведений, он обязан дать мотивированный ответ со ссылкой на положение закона, являющееся основанием для отказа. Если выявлены неточные данные, оператор обязан уточнить их на основании сведений, представленных субъектом, и снять блокирование. Если выявлена неправомерная обработка, оператор обязан прекратить её и, если обеспечить правомерность невозможно, уничтожить данные, уведомив об этом субъекта.

Запрос субъекта, по общему правилу, должен содержать сведения о документе, удостоверяющем личность, сведения, подтверждающие участие субъекта в отношениях с оператором или иным образом подтверждающие факт обработки, а также подпись субъекта или его представителя. Запрос может быть направлен и в форме электронного документа, подписанного электронной подписью.

Федеральный закон «Об информации, информационных технологиях и о защите информации»

Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» — базовый акт всей информационной сферы. Он принят в один день с законом о персональных данных, и эти два закона тесно связаны. Если закон о персональных данных регулирует конкретный вид информации, то закон об информации задаёт общие правила: что такое

информация, кто такой обладатель информации, что такое информационная система, каковы принципы правового регулирования в этой сфере.

Закон об информации закрепляет принцип неприкосновенности частной жизни и недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия. Он также устанавливает, что информация в зависимости от категории доступа делится на общедоступную и информацию, доступ к которой ограничен федеральными законами. Персональные данные относятся к информации ограниченного доступа: законом установлена обязанность обеспечивать их конфиденциальность.

Важное место в законе занимает защита информации. Под ней понимается принятие правовых, организационных и технических мер, направленных на обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также на соблюдение конфиденциальности информации ограниченного доступа и реализацию права на доступ к информации. Обладатель информации и оператор информационной системы обязаны обеспечивать эти меры в случаях, установленных законодательством.

Закон об информации также регулирует деятельность организаторов распространения информации в интернете, хранение отдельных видов информации на территории России, правила работы информационных систем и ответственность за нарушения. Для организаций, ведущих деятельность в интернете, это второй по значимости закон после закона о персональных данных.

Трудовой кодекс: защита персональных данных работника

Глава 14 Трудового кодекса Российской Федерации называется «Защита персональных данных работника». Она устанавливает специальные правила для трудовых отношений, дополняющие общие нормы закона о персональных данных. Персональные данные работника в этом контексте — это информация, необходимая работодателю в связи с трудовыми отношениями.

Кодекс устанавливает общие требования при обработке персональных данных работника. Обработка может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, получении образования и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества. Объем и содержание обрабатываемых данных определяются в соответствии с Конституцией, Трудовым кодексом и иными федеральными законами.

Все персональные данные работника следует получать у него самого. Если данные возможно получить только у третьей стороны, работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Работодатель должен сообщить о целях, предполагаемых источниках и способах получения данных, а также о характере подлежащих получению данных и последствиях отказа дать согласие.

Работодатель не имеет права получать и обрабатывать сведения о работнике, относящиеся к специальным категориям, за исключением случаев, предусмотренных законом. Работодатель не вправе получать и обрабатывать данные о членстве работника в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных законом. При принятии решений, затрагивающих интересы работника, работодатель не имеет права основываться на данных, полученных исключительно в результате их автоматизированной обработки или электронного получения.

Глава 14 регулирует также передачу персональных данных работника. Работодатель не должен сообщать данные третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо для предупреждения угрозы жизни и здоровью работника, а также в других случаях, установленных законом. Работодатель не должен сообщать данные в коммерческих целях без письменного согласия. Лица, получающие данные работника, должны быть предупреждены о том, что они могут использоваться лишь в целях, для которых сообщены.

Работники имеют право на полную информацию о своих персональных данных и их обработке, на свободный бесплатный доступ к своим данным, включая право на получение копий записей, за исключением случаев, предусмотренных законом. Они вправе требовать исключения или исправления неверных или неполных данных, а также данных, обработанных с нарушением требований. Работники и их представители должны быть ознакомлены под роспись с документами работодателя, устанавливающими порядок обработки данных, а также об их правах и обязанностях в этой области.

Кодекс устанавливает и ответственность: лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, привлекаются к дисциплинарной и материальной ответственности, а также к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

Важно учитывать, что нормы главы 14 применяются к трудовым отношениям. Если человек взаимодействует с организацией в иной форме, например по гражданско-правовому договору, к обработке его данных применяются общие правила закона о персональных данных, а нормы Трудового кодекса напрямую не действуют.

Локализация персональных данных

С 1 сентября 2015 года действует требование о локализации. При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети «Интернет», оператор обязан обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение) и извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации. Исключения из этого правила предусмотрены законом для ограниченного круга случаев.

На практике это означает, что первичная база, в которую поступают и в которой накапливаются данные российских граждан, должна размещаться в России. Использование иностранных серверов в качестве основного места накопления таких данных не допускается. При этом закон не запрещает последующую трансграничную передачу данных, если соблюдены установленные для неё правила.

Требование о локализации распространяется и на сведения, собираемые через формы на сайтах, мобильные приложения и иные онлайн-сервисы. Поэтому организации, работающие с гражданами России, должны понимать, где физически находятся их серверы и базы данных, а также базы подрядчиков, которым поручена обработка. Сведения о месте нахождения баз данных указываются, в том числе, в уведомлении об обработке, которое направляется в Роскомнадзор.

За нарушение требования о локализации законодательство предусматривает административную ответственность. Кроме того, исторически нарушение этого требования могло служить основанием для ограничения доступа к ресурсу на территории России.

Трансграничная передача персональных данных

Трансграничная передача — это передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу. С 1 марта 2023 года порядок трансграничной передачи существенно изменился.

Теперь оператор, прежде чем начать трансграничную передачу, обязан уведомить Роскомнадзор о своём намерении её осуществлять. Это уведомление направляется отдельно от уведомления об обработке персональных данных. В нём указываются, в частности, сведения об операторе, правовое основание и цель передачи, категории и перечень данных, категории субъектов, перечень иностранных государств, в которые планируется передача, и дата проведения оценки соблюдения получателем конфиденциальности и безопасности.

Перед подачей уведомления оператор обязан получить от органов власти иностранного государства или от иностранных получателей сведения о принимаемых ими мерах по защите данных и об условиях прекращения обработки, а также сведения о правовом регулировании в области персональных данных в соответствующем государстве, если оно не обеспечивает адекватную защиту прав субъектов. Эти сведения оператор обязан предоставить Роскомнадзору по его запросу.

Закон различает государства, обеспечивающие адекватную защиту прав субъектов персональных данных, и государства, которые её не обеспечивают. Перечень государств, обеспечивающих адекватную защиту, утверждается уполномоченным органом. Для передачи в государства, не входящие в этот перечень, действует более строгий порядок: по общему правилу передача может начинаться только после истечения установленного срока рассмотрения уведомления, если Роскомнадзор не принял решения о запрете или ограничении. Для государств с адекватной защитой передача, как правило, может осуществляться с момента направления уведомления.

Роскомнадзор вправе принять решение о запрете или об ограничении трансграничной передачи в целях защиты нравственности, здоровья, прав и законных интересов граждан, а также по иным основаниям, установленным законом. Решения могут приниматься и по инициативе других уполномоченных органов. В случае такого решения оператор обязан обеспечить уничтожение данных, ранее переданных получателю.

С практической точки зрения важно, что под трансграничную передачу могут подпадать не только очевидные случаи, например отправка базы данных зарубежному партнёру, но и использование иностранных облачных сервисов, почтовых сервисов, мессенджеров и систем аналитики, серверы которых находятся за пределами России. Поэтому организациям рекомендуется проводить ревизию используемых сервисов и оценивать, не происходит ли при их использовании передача данных за рубеж.

Обязанности при утечке персональных данных

С 1 сентября 2022 года в законе закреплены специальные обязанности оператора на случай инцидентов. В случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлёкшей нарушение прав субъектов, оператор обязан уведомить Роскомнадзор.

Уведомление направляется в два этапа. В течение двадцати четырёх часов с момента выявления инцидента оператор сообщает о произошедшем инциденте, о предполагаемых причинах, повлёкших нарушение прав субъектов, и предполагаемом вреде, о принятых мерах по устранению последствий, а

также предоставляет сведения о лице, уполномоченном взаимодействовать с Роскомнадзором по вопросам, связанным с инцидентом. В течение семидесяти двух часов оператор сообщает о результатах внутреннего расследования выявленного инцидента, а также предоставляет сведения о лицах, действия которых стали его причиной, при наличии таких сведений.

Инцидент может быть выявлен самим оператором, а также Роскомнадзором или иным заинтересованным лицом, которое сообщило о нём. Поэтому важно, чтобы у оператора был налаженный порядок приёма таких сообщений и реагирования на них. Кроме того, при утечке оператор обязан устранить допущенное нарушение и принять меры к недопущению подобных инцидентов в будущем.

Информирование об инцидентах осуществляется в том числе через государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак, с которой оператор обязан взаимодействовать в установленном порядке. В последние годы законодатель значительно усилил ответственность именно за утечки, что сделало своевременное реагирование и уведомление одним из ключевых элементов соблюдения закона.

Роскомнадзор, реестр операторов и уведомление об обработке

Уполномоченным органом по защите прав субъектов персональных данных является Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций, то есть Роскомнадзор. Он обеспечивает контроль и надзор за соответствием обработки требованиям закона, рассматривает обращения субъектов, ведёт реестр операторов.

Оператор до начала обработки персональных данных обязан уведомить Роскомнадзор о своём намерении осуществлять обработку. Закон предусматривает ограниченный перечень случаев, когда такое уведомление не требуется. После изменений, вступивших в силу в 2022 году, этот перечень был сокращён, и обязанность уведомления распространилась на большее число операторов. Уведомление можно направить в бумажной или электронной форме.

В уведомлении указываются, в частности, наименование и адрес оператора, цель обработки, категории данных и категории субъектов, правовое основание, перечень действий и способы обработки, описание мер по обеспечению безопасности, сведения об ответственном за организацию обработки, дата начала обработки, срок или условие её прекращения, сведения о наличии или отсутствии трансграничной передачи, сведения о месте нахождения базы данных. При изменении сведений оператор обязан уведомить Роскомнадзор об изменениях в установленный срок.

Реестр операторов является общедоступным. Это позволяет любому человеку проверить, уведомила ли организация надзорный орган об обработке и какие сведения о своей деятельности заявила. Сведения реестра не заменяют политику оператора, но дополняют её.

Полномочия Роскомнадзора включают право запрашивать у операторов информацию, требовать уточнения, блокирования или уничтожения недостоверных или незаконно полученных данных, принимать меры по приостановлению или прекращению обработки, осуществляемой с нарушением закона, обращаться в суд с исковыми заявлениями в защиту прав субъектов, направлять материалы в органы прокуратуры и иные правоохранительные органы, а также составлять протоколы об административных правонарушениях.

Ответственность за нарушения

Законодательство предусматривает несколько видов ответственности за нарушения в сфере персональных данных: гражданско-правовую, дисциплинарную, административную и уголовную.

Гражданско-правовая ответственность выражается прежде всего в обязанности возместить убытки и моральный вред. Закон прямо устанавливает, что моральный вред, причинённый субъекту вследствие нарушения его прав, нарушения правил обработки, а также требований к защите персональных данных, подлежит возмещению. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесённых субъектом убытков.

Дисциплинарная и материальная ответственность применяется к работникам, нарушившим правила обработки данных. Например, разглашение охраняемой законом тайны, ставшей известной работнику в связи с исполнением им трудовых обязанностей, в том числе разглашение персональных данных другого работника, Трудовой кодекс относит к основаниям для расторжения трудового договора по инициативе работодателя.

Административная ответственность установлена Кодексом Российской Федерации об административных правонарушениях. Основная статья посвящена нарушению законодательства в области персональных данных и содержит отдельные составы: обработка в случаях, не предусмотренных законом, или несовместимая с целями сбора; обработка без согласия в письменной форме, когда оно требуется; невыполнение обязанности опубликовать политику; непредоставление субъекту информации; невыполнение требований об уточнении, блокировании или уничтожении данных; необеспечение сохранности при неавтоматизированной обработке; невыполнение обязанности по локализации. Отдельно предусмотрена ответственность за непредставление уведомлений в Роскомнадзор.

В 2024 году в КоАП были внесены существенные изменения, вступившие в силу в 2025 году. Были установлены специальные составы за действия или бездействие оператора, повлёкшие неправомерную передачу персональных данных (утечку), с размером штрафа, зависящим от масштаба утечки — количества затронутых субъектов или записей, — а также повышенные санкции за повторные нарушения, в том числе оборотные штрафы, исчисляемые от выручки. Отдельный состав предусмотрен за неуведомление или несвоевременное уведомление Роскомнадзора об утечке. Конкретные размеры штрафов зависят от состава правонарушения, субъекта ответственности (гражданин, должностное лицо, индивидуальный предприниматель, юридическое лицо) и обстоятельств дела, поэтому для оценки рисков в каждой конкретной ситуации необходимо обращаться к действующей редакции кодекса.

Уголовная ответственность предусмотрена Уголовным кодексом Российской Федерации. Давно существует состав о нарушении неприкосновенности частной жизни — незаконном собирании или распространении сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия. Наказание ужесточается, если деяние совершено лицом с использованием своего служебного положения. Кроме того, ответственность может наступать за неправомерный доступ к компьютерной информации и другие преступления в сфере компьютерной информации.

В конце 2024 года в Уголовный кодекс была введена отдельная норма об ответственности за незаконные использование и (или) передачу, сбор и (или) хранение компьютерной информации, содержащей персональные данные, а также за создание и обеспечение функционирования информационных ресурсов, предназначенных для незаконного хранения и распространения такой

информации. Это было сделано в ответ на рост числа утечек и торговли базами данных. Квалифицирующие признаки связаны, в частности, с использованием специальных категорий или биометрических данных, с трансграничной передачей, с корыстной заинтересованностью, с использованием служебного положения и с совершением деяния группой лиц.

Подзаконные акты и требования к защите

Законы задают общие правила, а конкретные технические и организационные требования содержатся в подзаконных актах. Ключевую роль среди них играют постановления Правительства Российской Федерации и нормативные акты федеральных органов исполнительной власти, прежде всего ФСТЭК России и ФСБ России, а также акты самого Роскомнадзора.

Постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119 утверждены требования к защите персональных данных при их обработке в информационных системах персональных данных. Этот документ вводит понятие уровней защищённости. Уровень определяется с учётом категорий обрабатываемых данных (специальные, биометрические, общедоступные, иные), их принадлежности (работники оператора или иные лица), количества субъектов и типа актуальных угроз. Для каждого уровня установлен набор обязательных мер.

Отдельное постановление Правительства, принятое в 2008 году, регулирует особенности обработки персональных данных, осуществляемой без использования средств автоматизации. Оно определяет требования к обособлению данных на материальных носителях, к типовым формам документов, к хранению носителей и к условиям доступа к ним. Это важно для организаций, которые работают с бумажными анкетами, журналами, копиями документов.

Ещё одно постановление Правительства утверждает перечень мер, направленных на обеспечение выполнения обязанностей, предусмотренных законом о персональных данных, для государственных и муниципальных органов. Для коммерческих организаций оно напрямую не применяется, но часто используется как ориентир.

ФСТЭК России — Федеральная служба по техническому и экспортному контролю — утверждает состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах. Соответствующий приказ ФСТЭК 2013 года № 21 перечисляет группы мер: идентификация и аутентификация, управление доступом, ограничение программной среды, защита машинных носителей, регистрация событий безопасности, антивирусная защита, обнаружение вторжений, контроль защищённости, обеспечение целостности и доступности, защита среды виртуализации, защита технических средств, защита информационной системы и её средств связи и передачи данных и другие. Для каждого уровня защищённости определён базовый набор мер, который оператор адаптирует и уточняет с учётом своей системы и актуальных угроз.

ФСБ России устанавливает требования в части использования средств криптографической защиты информации. Они применяются, если для нейтрализации актуальных угроз оператор использует шифрование. Кроме того, методические документы ФСТЭК описывают порядок определения угроз безопасности информации, на основе которого строится модель угроз — документ, лежащий в основе выбора мер защиты.

Роскомнадзор также издаёт нормативные акты, касающиеся его компетенции: о порядке и сроках уведомлений, о требованиях к подтверждению уничтожения персональных данных, о порядке взаимодействия при инцидентах, об оценке вреда, который может быть причинён субъектам. Кроме того, Роскомнадзор публикует разъяснения и рекомендации, например по составлению политики

обработки данных, которые не являются обязательными нормами, но отражают позицию надзорного органа.

Как всё это связано между собой

Законодательство о персональных данных образует многоуровневую систему. На верхнем уровне находится Конституция, которая закрепляет право на неприкосновенность частной жизни и запрет на использование сведений о частной жизни без согласия. Ниже — федеральные законы: закон о персональных данных как основной, закон об информации как общий, Трудовой кодекс как специальный для трудовых отношений, а также отраслевые законы, в которых встречаются нормы о данных, например о связи, о банках, об электронной подписи.

Ещё ниже находятся постановления Правительства и акты профильных ведомств, которые превращают общие требования закона в конкретные меры. Наконец, на уровне самой организации действуют её локальные документы: политика обработки персональных данных, положения, инструкции, приказы, формы согласий. Именно они показывают, как общие требования закона применяются в повседневной работе конкретного оператора.

Для человека из этой системы важны прежде всего несколько вещей: его данные можно обрабатывать только на законном основании и для понятных целей; он вправе знать, что с ними происходит; он может требовать исправления и, в предусмотренных случаях, уничтожения данных; он может отозвать согласие; и у него есть куда обратиться за защитой — к самому оператору, в Роскомнадзор и в суд.

Для организации эта система означает необходимость постоянной работы: инвентаризации данных и процессов, документирования целей и оснований, защиты информационных систем, обучения сотрудников, своевременных уведомлений надзорного органа и готовности к инцидентам. Законодательство продолжает развиваться, поэтому и документы оператора, и это справочное приложение периодически пересматриваются, а читать их всегда стоит в актуальной редакции.