

УТВЕРЖДЕНО

Приказом Генерального директора

ООО «СТК РЕШЕНИЕ» от «20» мая 2025 г. № 7

ПРАВИЛА ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

ООО «СТК РЕШЕНИЕ»

1. Общие положения

1.1. Настоящие Правила обработки персональных данных (далее — «Правила») разработаны в соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее — «152-ФЗ») в действующей редакции, Постановления Правительства Российской Федерации от 15.09.2008 № 687, Постановления Правительства Российской Федерации от 01.11.2012 № 1119, приказа Роскомнадзора, приказов ФСТЭК и ФСБ России в области защиты информации, а также с учётом требований Регламента (ЕС) 2016/679 (GDPR) и иных применимых нормативных актов.

1.2. Правила определяют политику Общества с ограниченной ответственностью «СТК РЕШЕНИЕ» (далее — «Оператор», «Компания») в отношении обработки персональных данных (далее — «ПДн»), устанавливают порядок и условия их обработки и защиты, а также права и обязанности Оператора и субъектов ПДн.

1.3. Правила обязательны для исполнения всеми работниками Оператора, а также лицами, привлекаемыми Оператором к обработке ПДн на основании договоров (поручений).

1.4. Правила публикуются в свободном доступе на сайте m.karpov@stk-solution.ru в исполнение обязанности Оператора, предусмотренной ч. 2 ст. 18.1 152-ФЗ.

2. Основные понятия

- «Персональные данные (ПДн)» — любая информация, относящаяся прямо или косвенно к определённому или определяемому физическому лицу.
- «Оператор» — ООО «СТК РЕШЕНИЕ», самостоятельно или совместно с другими лицами организующее и/или осуществляющее обработку ПДн, а также определяющее цели обработки, состав и действия с ПДн.
- «Субъект ПДн» — физическое лицо, чьи персональные данные обрабатываются Оператором.
- «Обработка ПДн» — любое действие или совокупность действий с ПДн: сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (предоставление, доступ), обезличивание, блокирование, удаление, уничтожение.
- «Автоматизированная обработка» — обработка ПДн с помощью средств вычислительной техники.
- «Распространение ПДн» — действия, направленные на раскрытие ПДн неопределённому кругу лиц.

- «Предоставление ПДн» — действия, направленные на раскрытие ПДн определённому лицу или определённому кругу лиц.
- «Блокирование ПДн» — временное прекращение обработки ПДн (за исключением случаев, если обработка необходима для уточнения ПДн).
- «Уничтожение ПДн» — действия, в результате которых становится невозможным восстановить содержание ПДн в информационной системе и/или уничтожаются их материальные носители.
- «Обезличивание ПДн» — действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность ПДн конкретному субъекту.
- «Информационная система персональных данных (ИСПДн)» — совокупность содержащихся в базах данных ПДн и обеспечивающих их обработку информационных технологий и технических средств.
- «Специальные категории ПДн» — данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни (ст. 10 152-ФЗ).
- «Биометрические ПДн» — сведения, характеризующие физиологические и биологические особенности человека, позволяющие установить его личность (ст. 11 152-ФЗ).
- «Утечка ПДн» — неправомерная передача, предоставление, распространение или доступ к ПДн вследствие нарушения требований к защите.

3. Принципы и условия обработки ПДн

3.1. Принципы обработки (ст. 5 152-ФЗ):

- обработка на законной и справедливой основе;
- обработка ограничивается достижением конкретных, заранее определённых и законных целей; не допускается обработка ПДн, несовместимая с целями их сбора;
- не допускается объединение баз данных, обработка которых осуществляется в целях, несовместимых между собой;
- обработке подлежат только ПДн, соответствующие целям обработки;
- содержание и объём ПДн соответствуют заявленным целям обработки; не допускается избыточность ПДн;
- при обработке обеспечиваются точность ПДн, их достаточность, актуальность;
- хранение ПДн осуществляется в форме, позволяющей определить субъекта, не дольше, чем этого требуют цели обработки.

3.2. Условия обработки (ст. 6 152-ФЗ)

Обработка ПДн осуществляется при наличии хотя бы одного из следующих условий:

- согласие субъекта ПДн (в случаях, требующих такого согласия — оформленное в порядке ст. 9 152-ФЗ);
- обработка необходима для достижения целей, предусмотренных международным договором РФ или законом;

- обработка необходима для исполнения договора, стороной или выгодоприобретателем которого является субъект;
- обработка необходима для защиты жизни, здоровья или иных жизненно важных интересов;
- обработка необходима для осуществления прав и законных интересов Оператора или третьих лиц при условии, что не нарушаются права и свободы субъекта;
- обработка осуществляется в статистических или иных исследовательских целях при условии обязательного обезличивания.

3.3. Обработка специальных категорий ПДн (ст. 10 152-ФЗ)

Оператор не осуществляет обработку специальных категорий ПДн на постоянной основе. В случае разовой обработки (например, если субъект указывает в обращении сведения о состоянии здоровья) такая обработка допускается при наличии письменного согласия субъекта и осуществляется в минимально необходимом объёме.

3.4. Биометрические ПДн

Оператор не осуществляет обработку биометрических ПДн на сайте m.karpov@stk-solution.ru.

3.5. Согласие на обработку ПДн

3.5.1. Согласие субъекта на обработку ПДн оформляется в порядке, установленном ст. 9 152-ФЗ в редакции Федерального закона от 24.06.2025 № 156-ФЗ. С 01.09.2025 согласие оформляется отдельным документом от иных подписываемых субъектом документов.

3.5.2. Применяется следующее правило разделения согласий:

- отдельное согласие на обработку ПДн в общих целях;
- отдельное согласие на получение рекламно-информационных рассылок (e-mail, SMS, push);
- отдельное согласие на телефонные коммуникации и запись разговоров;
- отдельное согласие на передачу ПДн третьим лицам (Партнёрам, Портфельным компаниям);
- отдельное согласие на трансграничную передачу;
- отдельное согласие на использование в маркетинговых материалах;
- отдельное согласие на обработку cookies и иных идентификаторов;
- отдельное согласие на обработку специальных категорий ПДн (если применимо).

3.5.3. Согласия фиксируются с указанием даты, времени, IP-адреса, версии документа Политики/Соглашения; хранятся в течение всего срока обработки и дополнительно 3 года после её прекращения.

4. Категории субъектов и обрабатываемые данные

4.1. Оператор обрабатывает ПДн следующих категорий субъектов:

- посетители Сайта (анонимные и идентифицированные);
- заявители (физические лица, направляющие обращения, заявки, запросы);

- подписчики на рассылку;
- клиенты и контрагенты — физические лица, индивидуальные предприниматели; представители юридических лиц;
- соискатели вакансий;
- работники Оператора и лица, работающие по гражданско-правовым договорам;
- представители Партнёров и Портфельных компаний;
- спикеры, эксперты, авторы контента.

4.2. Перечень обрабатываемых ПДн и сроки их хранения приведены в Приложении к настоящим Правилам и в Политике конфиденциальности.

5. Порядок и условия обработки

5.1. Сбор

5.1.1. Сбор ПДн граждан Российской Федерации, в том числе через информационно-телекоммуникационную сеть «Интернет», осуществляется Оператором с использованием баз данных, находящихся на территории Российской Федерации (ч. 5 ст. 18 152-ФЗ в редакции ФЗ от 28.02.2025 № 23-ФЗ).

5.1.2. Для целей локализации Оператор использует инфраструктуру российских облачных провайдеров (Yandex.Cloud, VK Cloud, Selectel или эквивалентных) с подтверждённым размещением серверов на территории РФ.

5.2. Хранение

5.2.1. ПДн хранятся в форме, позволяющей определить субъекта, не дольше, чем этого требуют цели обработки. По достижении целей обработки ПДн уничтожаются или обезличиваются.

5.2.2. Хранение ПДн осуществляется на серверах в Российской Федерации; копии и архивы — в зашифрованном виде с разграничением доступа.

5.3. Уточнение

ПДн уточняются по запросу субъекта или при поступлении достоверных сведений об их неактуальности — в срок не более 15 рабочих дней.

5.4. Передача

5.4.1. Передача ПДн третьим лицам осуществляется в случаях, предусмотренных Политикой конфиденциальности, и только при наличии правового основания.

5.4.2. С Партнёрами, обрабатывающими ПДн по поручению Оператора, заключаются договоры в порядке ч. 3 ст. 6 152-ФЗ, содержащие, в частности:

- перечень действий с ПДн;
- цели обработки;
- обязанность соблюдать конфиденциальность и применять меры защиты;
- условия прекращения обработки и уничтожения данных по завершении договора.

5.5. Трансграничная передача

5.5.1. Трансграничная передача ПДн осуществляется только после направления уведомления в Роскомнадзор в порядке ст. 12 152-ФЗ.

5.5.2. До начала передачи в государства, не обеспечивающие адекватной защиты прав субъектов, Оператор ожидает результата рассмотрения уведомления Роскомнадзором (10 рабочих дней) и при отсутствии запрета приступает к передаче.

5.6. Обезличивание

Обезличивание применяется для целей статистики, продуктовой аналитики и архивирования. После обезличивания данные не подлежат восстановлению без использования дополнительной информации, хранящейся отдельно.

5.7. Блокирование и уничтожение

5.7.1. Блокирование осуществляется по требованию субъекта или Роскомнадзора, а также в случае выявления неправомерной обработки, до устранения нарушений.

5.7.2. Уничтожение ПДн производится в срок не более 30 дней после достижения целей обработки, отзыва согласия или возникновения иного основания для прекращения обработки. Уничтожение оформляется актом с указанием перечня уничтоженных носителей и применённого способа.

6. Меры по обеспечению безопасности

6.1. В соответствии со ст. 18.1, 19 152-ФЗ Оператор применяет следующие меры:

6.1.1. Организационные меры:

- назначение Ответственного за организацию обработки ПДн (ст. 22.1 152-ФЗ); сведения публикуются в Политике;
- утверждение и поддержание в актуальном состоянии настоящих Правил и иных локальных актов (Политика информационной безопасности, Положение об ИСПДн, Перечень обрабатываемых ПДн, Перечень должностей с доступом к ПДн, Инструкция по реагированию на инциденты);
- ознакомление работников с локальными актами под подпись;
- проведение внутреннего контроля и аудита соответствия не реже одного раза в год;
- оценку вреда, который может быть причинён субъектам ПДн в случае нарушения;
- определение угроз безопасности ПДн и модели угроз;
- установление уровня защищённости ПДн в ИСПДн в соответствии с ПП РФ № 1119.

6.1.2. Технические меры:

- применение средств защиты информации, прошедших процедуру оценки соответствия (сертификация ФСТЭК/ФСБ России для соответствующих уровней защищённости);
- разграничение прав доступа по принципу минимально необходимых привилегий (RBAC);

- двухфакторная аутентификация для административных учётных записей;
- шифрование каналов связи (TLS 1.2 и выше) и шифрование «при хранении» (at rest) для критичных хранилищ;
- резервное копирование и хранение копий в зашифрованном виде в географически разнесённых дата-центрах в РФ;
- регистрация и анализ событий безопасности (SIEM/логирование);
- использование межсетевых экранов, антивирусной защиты, систем обнаружения вторжений;
- регулярное обновление программного обеспечения, управление уязвимостями;
- обезличивание и псевдонимизация данных в средах разработки и тестирования.

6.1.3. Физические меры:

- размещение информационных систем в дата-центрах с соответствующим уровнем физической защиты;
- контроль доступа в помещения, где осуществляется обработка ПДн на бумажных носителях;
- организованное хранение и уничтожение бумажных носителей.

7. Реагирование на инциденты

7.1. При выявлении инцидента, связанного с возможной или фактической утечкой ПДн, Оператор:

- незамедлительно (но не позднее 24 часов с момента обнаружения) направляет уведомление в Роскомнадзор о факте инцидента (ч. 3.1 ст. 21 152-ФЗ); канал — Единая система взаимодействия Роскомнадзора;
- в течение 72 часов с момента обнаружения направляет уведомление о результатах внутреннего расследования;
- для субъектов ЕЭЗ/Великобритании, чьи права могут быть нарушены, уведомляет надзорный орган и субъектов в порядке Art. 33, 34 GDPR / UK GDPR;
- принимает меры по локализации инцидента, восстановлению защиты, минимизации последствий;
- проводит служебное расследование, оформляет акт, при необходимости привлекает экспертов;
- по результатам обновляет внутренние процессы и средства защиты.

8. Права субъектов ПДн и порядок их реализации

8.1. Полный перечень прав и порядок их реализации приведены в разделе 10 Политики конфиденциальности.

8.2. Запросы субъектов рассматриваются в следующие сроки:

- ответ на запрос о наличии и условиях обработки ПДн — 15 рабочих дней с момента получения запроса (с возможностью продления до 5 рабочих дней);
- уточнение, блокирование или уничтожение ПДн — 30 рабочих дней;

- ответ на запрос по GDPR — не более 1 месяца с момента получения, с возможностью продления до 3 месяцев в сложных случаях;
- ответ на запрос по CCPA — 45 дней с возможностью однократного продления.

8.3. Запросы направляются на адрес m.karpov@stk-solution.ru. Идентификация заявителя осуществляется по совокупности имеющихся у Оператора сведений; при сомнениях Оператор вправе запросить документ, удостоверяющий личность.

9. Ответственный за организацию обработки ПДн

9.1. В соответствии со ст. 22.1 152-ФЗ Оператор назначает Ответственного за организацию обработки ПДн (далее — «Ответственный»).

9.2. Ответственный:

- организует внутренний контроль соблюдения требований законодательства о ПДн;
- доводит до сведения работников Оператора положения законодательства и локальных актов;
- организует приём и обработку обращений и запросов субъектов ПДн;
- взаимодействует с Роскомнадзором и иными уполномоченными органами;
- координирует реагирование на инциденты;
- инициирует обновление локальных актов и обучения сотрудников.

9.3. Сведения об Ответственном (Ф.И.О., телефон, e-mail) указываются в Политике конфиденциальности.

10. Сроки хранения и порядок уничтожения

10.1. Конкретные сроки хранения определены в Политике конфиденциальности и в локальном «Перечне сроков хранения персональных данных».

10.2. Уничтожение ПДн оформляется актом с указанием:

- даты уничтожения;
- оснований уничтожения (достижение целей, отзыв согласия, истечение срока хранения и т. д.);
- перечня уничтоженных категорий ПДн и носителей;
- применённого способа уничтожения (физическое уничтожение носителя, многократная перезапись, криптографическое стирание и т. д.);
- Ф.И.О. и подписей лиц, осуществивших уничтожение.

10.3. По требованию субъекта Оператор предоставляет подтверждение уничтожения его ПДн.

11. Заключительные положения

11.1. Настоящие Правила утверждаются Генеральным директором Оператора и вступают в силу с даты утверждения.

11.2. Правила подлежат пересмотру по мере изменения законодательства, но не реже одного раза в год.

11.3. Действующая редакция Правил размещается на сайте <https://стк-решение.рф/>.

11.4. Контроль за соблюдением Правил возлагается на Ответственного за организацию обработки ПДн.

Редакция: «25» декабря 2025 г.