Редакция от «28» апреля 2021 г.

Утверждена приказом № 5 от 28 апреля 2021 г.

для сайта https://elotmarket.ru/

**Политика**

ИП Сомова В.В. в отношении обработки и защиты

персональных данных

(политика конфиденциальности)

Политика в отношении обработки персональных данных (далее – Политика) определяет правила и порядок обработки персональных данных (ПД) различных субъектов ПД в ИП Сомов В.В. (далее – Предприятие). Политика определяет обработку ПД в информационных системах (ИС) обработки персональных данных и в не автоматизированном виде.

Настоящая Политика разработана в соответствии с:

- Конституцией Российской Федерации;

- Трудовым кодексом Российской Федерации;

- Федеральным законом от 27 июля 2006 года №152-ФЗ «О персональных данных»;

- Федеральным законом от 27 июля 2006 года №149-ФЗ «Об информации, информационных технологиях и защите информации»;

- Постановлением Правительства Российской Федерации от 1 ноября 2012 года №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

- Постановлением Правительства Российской Федерации от 15 сентября 2008 года №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

- Приказом ФСТЭК России от 18 февраля 2013 года №21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

- Специальными требованиями и рекомендациями по технической защите конфиденциальной информации (СТР-К) ФСТЭК России.

1. **Основные понятия и определения**
   1. **Автоматизированная обработка персональных данных** – обработка персональных данных с помощью средств вычислительной техники.
   2. **Блокирование персональных данных** – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).
   3. **Защищаемая информация** – информация, определённая перечнем защищаемой информации (Приложение 1 к Приказу «Об обработке персональных данных»)
   4. **Информационная система персональных данных** (ИСПДн) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.
   5. **Обезличивание персональных данных** – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.
   6. **Обработка персональных данных** – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.
   7. **Оператор** – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно, или совместно с другими лицами организующее и (или) осуществляющее обработку персональных данных, а также определяющее цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.
   8. **Персональные данные** (ПД) – любая информация, относящаяся к прямо или косвенно определённому или определяемому физическому лицу (субъекту персональных данных).
   9. **Предоставление персональных данных** – действия, направленные на раскрытие персональных данных определённому лицу или определённому кругу лиц.
   10. **Роскомнадзор** – Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор), которая является федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, в том числе электронных, и массовых коммуникаций, информационных технологий и связи, функции по контролю и надзору за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных, а также функции по организации деятельности радиочастотной службы. Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций является уполномоченным федеральным органом исполнительной власти по защите прав субъектов персональных данных.
   11. **Система защиты персональных данных**– совокупность программных, аппаратных и технических средств защиты информации, используемых для обеспечения информационной безопасности информационных систем.
   12. **Сотрудник, ответственный за организацию обработки персональных данных**– сотрудник ИП Сомов В.В., назначенный ответственным за организацию обработки и обеспечение защиты ПД на Предприятии.
   13. **Угрозы безопасности персональных данных** – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных.
   14. **Уничтожение персональных данных** – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.
   15. **Уровень защищённости** – под уровнем защищённости персональных данных понимается комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.
   16. **Участник эЛот** – физическое лицо (в том числе, представитель физического лица, индивидуальный предприниматель, представитель индивидуального предпринимателя, руководитель или иной уполномоченный представитель юридического лица), находящееся в договорных отношениях с ИП Сомов В.В. либо представляющий интересы лица, находящегося в договорных отношениях с ИП Сомов В.В., и предоставившее свои ПД для обработки в добровольном порядке.
   17. **Иное лицо -** физическое лицо, не являющееся сотрудником Предприятия или участником электронной торговой площадки эЛот, однако являющееся стороной, выгодоприобретателем или поручителем в договоре с Предприятием; выполняющее подрядные работы по заказу Предприятия или оказывающее услуги Предприятию и другие лица, участвующие в хозяйственной деятельности Предприятия. А также представители таких лиц и прочие лица, передающие свои ПД Предприятию на основании согласия на обработку ПД.
2. **Цели обработки персональных данных**
   1. Основание и цели обработки ПД на предприятии устанавливаются в соответствии с типом субъекта:
      1. Сотрудники – на основании согласия субъекта на обработку ПД и для достижения следующих целей:
         1. обеспечение соблюдения законов и иных нормативных правовых актов, содействия сотрудникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности сотрудников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества предприятия;
         2. исполнение договорных отношений с сотрудником.
      2. Участники эЛот – на основании согласия субъекта на обработку ПД и для достижения следующих целей:
         1. обеспечение соблюдения законов и иных нормативно-правовых актов;
         2. обеспечение функционирования электронной площадки эЛот;
         3. исполнение договорных отношений между ИП Сомов В.В. и субъектом ПД.
      3. Иные лица – на основании согласия субъекта на обработку ПД или ином законном основании и для достижения следующих целей:
         1. обеспечение соблюдения законов и иных нормативно-правовых актов;
         2. исполнение договорных отношений между субъектом ПД и Предприятием;
         3. осуществление прав и законных интересов Предприятия или третьих лиц для достижения общественно значимых целей.
   2. Персональные данные субъекта могут обрабатываться только для достижения целей установленных в пункте 2.1 для конкретного типа субъектов ПД.
   3. Субъект предоставляет ПД в объёме, необходимом для достижения целей.
   4. Субъект даёт согласие Предприятию на обработку своих ПД:
      1. Сотрудники – при подписании трудового договора. Далее согласие хранится вместе с трудовым договором сотрудника.
      2. Участники эЛот – при регистрации на площадке и присоединении к регламенту эЛот. Хранение производится в электронном виде в базе данных эЛот.
      3. Иные лица – при установлении договорных отношений, либо в другой законной форме. Согласие хранится вместе с документами, относящимися к хозяйственной деятельности Предприятия и Лица.
   5. Согласие субъекта должно содержать следующие сведения:
      1. фамилию, имя, отчество, дата, место рождения и адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
      2. наименование и адрес оператора, получающего согласие субъекта персональных данных;
      3. цель обработки персональных данных;
      4. перечень персональных данных, на обработку которых даётся согласие субъекта персональных данных;
      5. перечень действий с персональными данными, на совершение которых даётся согласие, общее описание используемых оператором способов обработки персональных данных;
      6. срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;
      7. подпись субъекта персональных данных.

## Условия обработки персональных данных

* 1. На Предприятии осуществляется автоматизированная и неавтоматизированная обработка ПД субъектов.
  2. Срок хранения ПД, в том числе заявлений о согласии на обработку установлен в зависимости от типа Субъекта:
     1. Сотрудники: 75 лет согласно строке 666 Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения, утверждённого Приказом Министерства культуры Российской Федерации от 25 августа 2010 года №558 и других нормативно-правовых актов РФ.
     2. Участники эЛот: 10 лет с даты последнего подписанного с помощью электронной подписи и (или) отправленного посредством эЛот документа, согласно п. 2.1.10 приказа Минэкономразвития РФ от 15.02.2010 №54 и других нормативно-правовых актов РФ.
     3. Иные лица: если иное не установлено договором, то 5 лет согласно п. 436, 455, 456 Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения, утверждённого Приказом Министерства культуры Российской Федерации от 25 августа 2010 года №558.
  3. Любые действия с ПД субъекта без письменного его согласия или любого другого основания, установленного Федеральным законом №152-ФЗ «О персональных данных», а также пунктом 2.1 настоящей Политики, запрещены.
  4. Сбор специальных категорий ПД субъектов, в том числе информации об их расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, интимной жизни Предприятием не производится.
  5. Сотрудники Предприятия, допущенные к обработке ПД, проходят инструктаж и соблюдают нормы законодательства в области защиты ПД и локальных нормативно-правовых актов Предприятия. Сотрудники, не прошедшие инструктаж, к обработке ПД не допускаются.
  6. В случае выявления недостоверных ПД или неправомерных действий с ними при обращении или по запросу субъекта, Предприятие обязано осуществить блокирование ПД в соответствии с действующим законодательством.
  7. В случае подтверждения факта неточности персональных данных Предприятие на основании сведений, представленных субъектом, его представителем, либо уполномоченным органом по защите прав субъектов ПД, или иных необходимых документов, обязано уточнить ПД в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.
  8. В случае достижения цели обработки ПД или окончания срока обработки Предприятие обязано прекратить обработку ПД в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено законодательством. Уничтожение производится под контролем ответственного за организацию обработки ПД.Об уничтожении составляется акт.
  9. В случае отзыва субъектом согласия на обработку его ПД, Предприятие обязано прекратить их обработку в случае, если сохранение ПД более не требуется для целей обработки ПД и не противоречит законодательству. Предприятие обязано уничтожить ПД в срок, не превышающий тридцати дней с даты поступления указанного отзыва.

## Ответственный за организацию обработки ПД

* 1. ИП Сомов В.В. назначает сотрудника, ответственного за организацию обработки ПД и ответственного за реагирование на обращения сотрудников по вопросам ПД.
  2. Сотрудник, ответственный за организацию обработки ПД обязан:
     1. осуществлять внутренний контроль за соблюдением Предприятием и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;
     2. доводить до сведения работников ИП Сомов В.В. положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, внутренних требований к защите персональных данных;
     3. проводить инструктаж по вопросам ПД;
     4. координировать работы по защите ПД.
  3. Сотрудник, ответственный за реагирование на обращения субъектов по вопросам ПД обязан:
     1. организовывать приём и обработку обращений и запросов субъектов или их представителей и (или) осуществлять контроль за приёмом и обработкой таких обращений и запросов;
     2. вести журнал учёта запросов и ответов на запросы по вопросам ПД и инцидентов, связанных с ПД субъектов.

## Права субъекта

* 1. Субъект имеет право:
     1. на получение информации, касающейся обработки его ПД, в том числе содержащей:

- подтверждение факта обработки персональных данных;

- правовые основания и цели обработки ПД;

- цели и применяемые способы обработки ПД;

- наименование и адрес Предприятия, сведения о лицах, которые имеют доступ к ПД и условия передачи ПД;

- срок обработки ПД, в том числе срок их хранения;

- информацию о трансграничной передаче данных;

- иные сведения, предусмотренные Федеральным законом № 152-ФЗ «О персональных данных» или другими федеральными законами.

* + 1. на отзыв данного ранее согласия на обработку ПД, в соответствии с Федеральным законом №152-ФЗ «О персональных данных».
  1. Сведения должны быть предоставлены субъекту в доступной форме, и в них не должны содержаться ПД, относящиеся к другим субъектам.
  2. Если субъект ПД считает, что оператор осуществляет обработку его ПД с нарушением требований действующего законодательства или иным образом нарушает его права и свободы, субъект ПД вправе обжаловать действия или бездействие оператора в РКН или в судебном порядке.

## Порядок запроса сведений субъектом ПД

* 1. Сведения, запрашиваемые субъектом, предоставляются ему или его представителю при получении запроса, оформленного в соответствии с Федеральным законом №152-ФЗ «О персональных данных». Запрос должен содержать обязательные поля:
     1. фамилию, имя, отчество заявителя;
     2. реквизиты основного документа, удостоверяющего личность;
     3. сведения, подтверждающие факт отношений субъекта и ИП Сомов В.В. (номер договора, дату заключения договора, срок работы, договор или копию договора), либо сведения, иным способом подтверждающие факт обработки ПД Предприятием;
     4. личную подпись субъекта либо его представителя и дату составления запроса.

Полномочия представителя должны быть оформлены в соответствии с действующим законодательством Российской Федерации.

* 1. Оформленный запрос предоставляется сотруднику, ответственному за реагирование на обращение субъектов по вопросам ПД.
  2. Ответственный за реагирование на обращения субъектов по вопросам ПД проверяет представленный запрос и готовит запрашиваемую субъектом информацию в виде ответного письма за подписью руководителя Предприятия или его заместителя в срок не более 30 дней, в другом случае, в течение указанного срока, готовит мотивированный законодательством отказ.
  3. Субъект вправе обратиться повторно на Предприятие или направить повторный запрос в целях получения запрошенных сведений, и ознакомления с такими ПД не ранее чем через 30 дней после первоначального запроса или по факту получения ответа на первоначальное обращение, в том числе, если запрошенные сведения, а также обрабатываемые ПД были предоставлены для ознакомления субъекту не в полном объёме. Повторный запрос должен содержать обоснование направления повторного запроса.
  4. Предприятие вправе отказать субъекту в выполнении повторного запроса, в случае несоответствия перечисленным выше условиям.
  5. Право субъекта на доступ к его ПД, обрабатываемым Предприятием, может быть ограничено в соответствии с федеральными законами.

# **Обеспечение безопасности ПД**

* 1. Безопасность ПД достигается путем исключения несанкционированного, в том числе случайного, доступа к ПД, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение ПД, а также иных несанкционированных действий, которые могут повлечь за собой изменение, блокирование, удаление, распространение и другие действия с ПД.
  2. Безопасность ПД при их обработке в ИС обеспечивается с помощью системы защиты ПД, включающей организационные меры и средства защиты информации, средства предотвращения несанкционированного доступа, технические средства защиты, а также используемые в информационной системе информационные технологии. Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям.

* 1. Обмен ПД при их обработке в информационных системах осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и путем применения технических средств.

* 1. Размещение информационных систем, режим доступа в помещения и системы видеонаблюдения, охрана и организационные меры обеспечивают сохранность носителей ПД и средств защиты информации, а также исключают возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

* 1. При обработке ПД в ИС должно быть обеспечено:

* + 1. проведение мероприятий, направленных на предотвращение несанкционированного доступа к ПД и (или) передачи их лицам, не имеющим права доступа к такой информации;

* + 1. своевременное обнаружение фактов несанкционированного доступа к ПД;

* + 1. недопущение воздействия на технические средства автоматизированной обработки ПД, в результате которого может быть нарушено их функционирование;

* + 1. возможность восстановления ПД, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

* + 1. контроль за обеспечением уровня защищенности ПД.

* 1. Мероприятия по обеспечению безопасности ПД при их обработке в ИС включают в себя:

* + 1. определение угроз безопасности ПД при их обработке, формирование на их основе модели угроз;

* + 1. разработку на основе модели угроз системы защиты ПД, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего уровня защищённости ИС;

* + 1. проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;

* + 1. установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;

* + 1. обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

* + 1. учёт применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей ПД;

* + 1. учёт лиц, допущенных к работе с ПД в ИС;

* + 1. расследование и выявление действий сотрудников, приводящих к нарушению конфиденциальности ПД или другим нарушениям, приводящим к снижению уровня защищённости ПД, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений.

* 1. Допуск сотрудников ИП Сомов В.В. к конкретным категориям ПД устанавливается перечнем, либо внутренним приказом по организации.
  2. Сотрудники, допущенные к обработке ПД, в соответствии с п. 7.7 несут ответственность за нарушения правил обработки ПД установленных действующим законодательством РФ и локальными нормативно-правовыми актами оператора.

# **Особенности неавтоматизированной обработки ПД**

* 1. Неавтоматизированная обработка ПД сотрудников в ИП Сомов В.В. заключается в работе с бумажными носителями информации, содержащими ПД субъектов.
  2. К бумажным носителям ПД относятся:
     1. кадровые документы;
     2. договоры, приложения к ним, в случае если они содержат ПД и позволяют идентифицировать субъекта;
     3. светокопии документов, удостоверяющих личность субъекта;
     4. другие бумажные носители, содержащие ПД субъектов.
  3. В ИП Сомов В.В. установлены следующие требования к хранению бумажных носителей ПД:
     1. срок хранения для бумажных носителей ПД, устанавливается пунктом 3.2 Политики;
     2. бумажные носители ПД хранятся в сейфах, за сохранность документов в сейфе назначен ответственный сотрудник;
     3. запрещается хранение бумажных носителей ПД в местах, доступных для ознакомления посторонними лицами;
     4. сотруднику, выполняющему обработку ПД с использованием бумажных носителей ПД, запрещается хранить их на своем рабочем месте.
  4. У ИП Сомов В.В. установлены следующие требования к уничтожению бумажных носителей ПД:
     1. уничтожение бумажных носителей ПД может проводиться при помощи технических средств (уничтожителей бумаги), путём разрезания вручную или вымарывания. При этом должна быть обеспечена невозможность восстановления ПД из остатков носителя;
     2. уничтожение бумажных носителей должно проходить в присутствии ответственного за организацию обработки ПД и должно оформляться актом.
  5. Не допускается фиксация на одном бумажном носителе ПД, цели обработки которых заведомо несовместимы. В случае обработки различных категорий ПД, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.
  6. Уточнение ПД при осуществлении их неавтоматизированной обработки у ИП Сомов В.В. производится путём обновления или изменения данных на бумажном носителе ПД, либо путём изготовления нового бумажного носителя ПД с уточнёнными ПД. Прежний носитель при этом уничтожается.
  7. При хранении бумажных носителей ПД должны соблюдаться условия, обеспечивающие сохранность ПД и исключающие несанкционированный к ним доступ.