

**Положение  
об обработке и защите персональных данных  
Владельца Сайта <http://esparma-gmbh.ru/>**

**ГОРОД МОСКВА**

**2021г.**

## 1. Общие положения

1.1. Настоящее Положение об обработке персональных данных Владельца Сайта <http://esparma-gmbh.ru/> (далее - Положение) является локальным нормативным актом и разработано в соответствии с действующим законодательством Российской Федерации. Положение определяет порядок, условия обработки и защиты персональных данных, устанавливает процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений, связанных с обработкой персональных данных.

1.2. Целью настоящего Положения является обеспечение защиты прав граждан при обработке их персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

1.3. Настоящее Положение разработано в соответствии с:

- Конституцией Российской Федерации;
- Гражданским кодексом Российской Федерации;
- Федеральным законом от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – ФЗ «О персональных данных»);
- Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 01.11.2012 г. №1119;
- Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденным Постановлением Правительства РФ от 15.09.2008г. №687;
- иными нормативно-правовыми актами.

1.4. Настоящее Положение вступает в силу с момента его утверждения и действует бессрочно, до замены его новым Положением. Владелец Сайта оставляет за собой право внесения любых изменений в настоящее Положение в любое время без и предварительного уведомления.

1.5. Настоящее положение должно быть доведено до сведения всех работников Представительства.

1.6. Пользователь Сайта передает персональные данные Владельцу Сайта всякий раз, когда он указывает их на Сайте, отправляет Владельцу Сайта по электронной почте или сообщает лично. Передавая Владельцу Сайта свои персональные данные, Пользователь Сайта соглашается с условиями, приведенными в настоящем Положении. В соответствии с действующим законодательством и настоящим Положением о защите персональных данных, Пользователь Сайта может в любое время их изменить, обновить или попросить об удалении.

1.7. Обработка организована Владельцем Сайта на принципах:

- а) обработка персональных данных осуществляется на законной и справедливой основе;
- б) обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;
- в) не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;
- г) обработке подлежат только персональные данные, которые отвечают целям их обработки;
- д) содержание и объем обрабатываемых персональных данных соответствуют заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки;
- е) при обработке персональных данных обеспечена точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Представительство принимает необходимые меры либо обеспечивать их

принятие по удалению или уточнению неполных или неточных данных;

- ж) хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

#### 1.8. Способы обработки персональных данных:

- а) с использованием средств автоматизации;
- б) без использования средств автоматизации.

#### 1.9. В настоящем Положении используются следующие основные понятия:

- 1) **персональные данные** — любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных).

К персональным данным могут относиться:

- а) сведения, содержащиеся в документе, удостоверяющем личность субъекта персональных данных (фамилия, имя, отчество, дата и место рождения, адрес регистрации, семейное положение и др.);
  - б) информация, содержащаяся в страховом свидетельстве государственного пенсионного страхования;
  - в) сведения об образовании, квалификации или наличии специальных знаний или подготовки;
  - г) информация медицинского характера в случаях, предусмотренных законодательством;
  - д) сведения о семейном положении субъекта персональных данных, его социальном, имущественном положении;
  - е) информация о членах семьи субъекта персональных данных;
  - ж) информация о месте жительства, почтовый адрес, телефон работника, а также членов его семьи;
  - з) иная информация, относящаяся к прямо или косвенно определенному или определяемому субъекту персональных данных.
- 2) **информация** – сведения (сообщения, данные) независимо от формы их представления;
- 3) **субъект персональных данных** - Пользователь Сайта, доступного по ссылке <http://esparma-gmbh.ru/>, а также все сервисы и сайты Представительства фирмы «Эспарма ГмбХ» (Германия) г. Москва (уже существующие и создаваемые в будущем).
- 4) **Владелец Сайт** - Представительство фирмы «Эспарма Гмбх» (Германия), г. Москва (Номер записи об аккредитации 20150000123)
- 5) **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;
- 6) **распространение персональных данных** - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;
- 7) **предоставление персональных данных** - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;
- 8) **блокирование персональных данных** - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);
- 9) **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;

- 10) **обезличивание персональных данных** - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;
- 11) **неавтоматизированная обработка персональных данных** – обработка персональных данных без использования средств автоматизации;
- 12) **автоматизированная обработка персональных данных** - обработка персональных данных с помощью средств вычислительной техники;
- 13) **информационная система персональных данных** - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;
- 14) **технические средства** - средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных, средства защиты информации, применяемые в информационных системах.

## **2. Порядок и условия обработки персональных данных**

2.1. Обработка персональных данных осуществляется Владелцем Сайта в следующих случаях, предусмотренных ФЗ «О персональных данных», в частности:

- 1) обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;
- 2) обработка персональных данных необходима для достижения целей, предусмотренных Пользовательским Соглашением;
- 3) обработка персональных данных осуществляется в статистических целях, при условии обязательного обезличивания персональных данных.

2.2. Получение персональных данных осуществляется Владелцем Сайта у каждого субъекта персональных данных, либо у его представителя, имеющего соответствующие полномочия, путем формирования соответствующего запроса на Сайте;

2.3. Владелец Сайта вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных.

2.4. Владелец Сайта обязан не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

### **2.5. Согласие на обработку персональных данных**

2.5.1. Субъект персональных данных дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку персональных данных должно быть конкретным, информированным и сознательным. Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем.

2.5.2. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных. В случае отзыва субъектом персональных данных согласия на обработку персональных данных Владелец Сайта не вправе продолжить обработку персональных данных без согласия субъекта персональных данных.

2.5.3. Субъект персональных данных выражает свое согласие на обработку персональных данных путем выставления отметки в поле «Я ознакомлен и согласен с «Условия сбора и обработки персональных данных» на запрос соответствующего ресурса Сайта о согласии Пользователя на обработку персональных данных.

2.5.4. Субъект персональных данных имеет право не давать своего согласия на обработку персональных данных. При этом Владелец Сайта вправе ограничить / отказать Пользователю доступ и возможность использования определенных ресурсов и сервисов Сайта.

### **3. Способы обработки персональных данных**

3.1. Владелец Сайта осуществляет автоматизированную обработку персональных данных.

3.2. Владелец Сайта не осуществляет извлечение персональных данных, содержащихся в информационной системе, перенос и фиксацию персональных данных на материальные носители, а также осуществления таких действий с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных при непосредственном участии человека.

3.3. Автоматизированная обработка персональных данных осуществляется с использованием средств вычислительной техники в электронных таблицах, базах данных и компьютерных программах, собирающих и обрабатывающих статистические данные.

3.4. При автоматизированной обработке должно быть обеспечено:

- a. проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;
- b. своевременное обнаружение фактов несанкционированного доступа к персональным данным;
- c. недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;
- d. возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- e. постоянный контроль над обеспечением уровня защищенности персональных данных.

3.5. Обеспечение безопасности персональных данных при их обработке в информационной системе осуществляется Владельцем Сайта.

### **4. Права и обязанности субъекта персональных данных**

#### **4.1. Субъект персональных данных вправе:**

4.1.1. Получать информацию, касающуюся обработки его персональных данных, в том числе содержащей:

- 1) подтверждение факта обработки персональных данных Владельцем Сайта;
- 2) правовые основания и цели обработки персональных данных;
- 3) цели и применяемые Владельцем Сайта способы обработки персональных данных;
- 4) наименование и место нахождения Владельца Сайта, сведения о лицах, которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные;
- 5) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок не предусмотрен федеральным законом;
- 6) сроки обработки персональных данных, в том числе сроки их хранения;
- 7) порядок осуществления субъектом персональных данных прав, предусмотренных ФЗ «О персональных данных»;
- 8) информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- 9) иные сведения, предусмотренные ФЗ «О персональных данных» и другими федеральными законами.

4.1.2. Получать разъяснения по вопросам обработки принадлежащих ему персональных данных, сформировав соответствующий запрос в форме обратной связи на Сайте, либо направив соответствующий письменный запрос по адресу местонахождения Владельца Сайта.

Указанная информация должна быть представлена субъекту персональных данных Владелец Сайта в доступной форме, и в ней не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

Данная информация предоставляется субъекту персональных данных или его представителю Владелец Сайта при обращении либо при получении запроса субъекта персональных данных или его представителя.

Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами, в том числе, если доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц.

4.1.3. Отозвать в любой момент и без объяснения причин свое согласие на обработку персональных данных и / или согласие на передачу персональный данных третьим лицам, сформировав запрос об отзыве согласия на обработку персональных данных и / или согласие на передачу персональный данных третьим лицам в форме обратной связи на Сайте, либо направив соответствующий письменный запрос по адресу местонахождения Владельца Сайта;

4.1.4. Потребовать в любой момент и без объяснения причин удаления персональных данных в форме обратной связи на Сайте, либо направив соответствующий письменный запрос по адресу местонахождения Владельца Сайта;

## **4.2. Субъект персональных данных обязан:**

4.2.1. Передавать Владельцу Сайта достоверные персональные данные. Субъект персональных данных самостоятельно несет ответственность за достоверность предоставленных данных. Владелец Сайта имеет право по своему усмотрению заблокировать, либо удалить учетную запись Пользователя и отказать Пользователю в использовании сервисов Сайта в случае, если у Владельца есть основания полагать, что предоставленные Пользователем персональные заведомо ложны и недостоверны.

## **5. Обязанности Владельца Сайта**

### **5.1. Владелец Сайта обязан:**

5.1.1. При сборе персональных данных предоставить субъекту персональных данных по его просьбе информацию, предусмотренную подпунктом 4.1.1. настоящего Положения;

5.1.2. Разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные, включая, но не ограничиваясь, ограничением доступа и / или возможностью использовать определенные ресурсы и сервисы Сайта;

5.1.3. Сообщить субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя в течение тридцати дней с даты получения запроса.

5.1.4. В случае выявления неправомерной обработки персональных данных либо по запросу субъекта персональных данных осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование.

В случае выявления неточных персональных данных при обращении субъекта персональных данных, осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

5.1.5. В случае подтверждения факта неточности персональных данных, на основании сведений, представленных субъектом персональных данных уточнить персональные данные либо обеспечить их уточнение.

5.1.6. В случае выявления неправомерной обработки персональных данных прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных.

5.1.7. В случае достижения цели обработки персональных данных прекратить обработку персональных данных или обеспечить ее прекращение и уничтожить персональные данные или обеспечить их уничтожение.

5.1.8. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных прекратить их обработку или обеспечить прекращение такой обработки и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные или обеспечить их уничтожение. ,

5.1.9. В случае отсутствия возможности уничтожения персональных данных, Владелец Сайта осуществляет блокирование таких персональных данных или обеспечивает их блокирование.

5.1.10. Назначить лицо, ответственное за организацию обработки персональных данных, которое обязано:

- 1) осуществлять внутренний контроль за соблюдением Владельцем Сайта законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;
- 2) доводить до сведения работников Владельца Сайта положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;
- 3) организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль над приемом и обработкой таких обращений и запросов.

5.1.11. Принимать необходимые правовые, организационные и технические меры по обеспечению безопасности персональных данных.

5.1.12. Осуществлять внутренний контроль и (или) аудит соответствия обработки персональных данных ФЗ «О персональных данных» и принятым в соответствии с ним локальным нормативным актам.

## **6. Особенности обработки персональных данных Владельцем Сайта**

6.1. При обработке персональных данных работников Владелец Сайта обязуется:

- 1) осуществлять обработку персональных данных Пользователя Сайта исключительно в целях, указанных в Пользовательском Соглашении;
- 2) при определении объема и содержания обрабатываемых персональных данных Пользователя Сайта ограничиваться исключительно данными, необходимыми для достижения целей, указанных в Пользовательском Соглашении;

6.2. При передаче персональных данных Владелец Сайта должен соблюдать следующие требования:

- 1) не сообщать персональные данные Пользователя Сайта третьей стороне без выраженного согласия Пользователя Сайта;
- 2) не сообщать персональные данные Пользователя Сайта в коммерческих целях без его согласия;
- 3) осуществлять передачу персональных данных Пользователя Сайта в пределах организации в соответствии с настоящим Положением.

## **7. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных**

7.1. В случае неисполнения/ненадлежащего исполнения требований настоящего Положения к применяются меры ответственности, предусмотренные законодательством Российской Федерации и нормативными актами Владельца Сайта.

**Приложения:**

- 1) Согласие на обработку персональных данных и передачу персональных данных третьему лицу на 1 л. (форма);
- 2) Положение об обеспечении безопасности персональных данных при их обработке в Представительстве фирмы «Эспарма ГмбХ» (Германия) г. Москва на 10 л.
- 3) Обязательство о неразглашении персональных данных на 1 л. (форма)



## СОГЛАСИЕ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ И ИХ ПЕРЕДАЧУ ТРЕТЬЕЙ СТОРОНЕ

Я, \_\_\_\_\_, \_\_\_\_\_ года рождения,  
зарегистрированный (ая) по адресу: \_\_\_\_\_

\_\_\_\_\_,  
Адрес электронной почты \_\_\_\_\_  
в соответствии со статьей 9 Федерального закона от 27.07.2006 г. №152-ФЗ «О персональных данных» даю согласие Владельцу Сайта <http://esparma-gmbh.ru/> на автоматизированную, а также без использования средств автоматизации обработку, включая сбор, систематизацию, накопление, хранение, уточнение, обновление, изменение, использование, распространение, передачу третьим лицам (распространение, предоставление, доступ) в том числе трансграничную, обезличивание, блокирование, удаление, уничтожение моих персональных данных (в том числе фамилии, имени, отчества; даты и места рождения; образования; профессии; доходов; адреса места жительства и фактического проживания; номера телефона (домашний, мобильный); адреса электронной почты; в целях:

- предусмотренных Пользовательским Соглашением;
- обеспечения соблюдения законов и иных нормативных правовых актов.

Также я даю согласие на:

- включение в общедоступные источники персональных данных следующих персональных данных: фамилии, имени, отчества, даты рождения;
- на предоставление третьей стороне моих персональных данных для целей, предусмотренных Пользовательским соглашением:
- формирования статистического отчета о посещении Сайта, использования ресурсов и сервисов Сайта;
- Иных целей, предусмотренных Пользовательским Соглашением;

Я соглашаюсь получать от Представительства фирмы «Эспарма ГмбХ» (Германия) г. Москва на электронный адрес, указанный мною выше информационные и/или рекламные электронные и/или голосовые сообщения.

Настоящее согласие действует с настоящего дня до дня его отзыва в форме, предусмотренной п.п.4.1.3. Положением об обработке и защите персональных данных.

\_\_\_\_\_/\_\_\_\_\_  
(подпись) (Ф.И.О. указывается полностью)  
«\_\_\_» \_\_\_\_\_ 201\_\_ г.

к Положению об обработке  
и защите персональных данных  
Владельца Сайта  
г. Москва  
От «\_\_\_» \_\_\_\_\_ 2020г.

**Положение  
об обеспечении безопасности персональных данных при их обработке в  
Владельцем Сайта**

**1. Общие положения**

1.1. Настоящее Положение об обеспечении безопасности персональных данных при их обработке Владельцем Сайта <http://esparma-gmbh.ru/> (далее – Положение) определяет меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

1.2. Целью настоящего Положения является обеспечение защиты прав граждан при обработке их персональных данных.

1.3. Настоящее Положение разработано в соответствии с:

- Федеральным законом от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – ФЗ «О персональных данных»);
- Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 01.11.2012 г. №1119;

1.4. Настоящее Положение вступает в силу с момента его утверждения и действует бессрочно, до замены его новым Положением. Владелец Сайта оставляет за собой право внесения любых изменений в настоящее Положение в любое время без предварительного уведомления.

**2. Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных.**

2.1. Владелец Сайта при обработке персональных данных принимает необходимые правовые, организационные и технические меры и обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

**2.2. Обеспечение Владельцем Сайта безопасности персональных данных достигается, в частности:**

2.2.1. Определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

2.2.2 Применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, предусмотренных настоящим Положением, в том числе:

- а) организацией режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого

- проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;
- б) обеспечение сохранности носителей персональных данных;
  - в) обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;
  - г) восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
  - д) закреплением перечня должностей, допущенных к обработке персональных данных, путем издания соответствующего приказа с указанием полного и ограниченного доступа к персональным данным, а также с указанием перечня действий, который осуществляется с персональными данными в рамках своей трудовой функции;
  - е) установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными;
  - ж) контролем над обеспечением безопасности персональных данных и уровня защищенности информационных систем персональных данных.

### 3. Определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

3.1. Под угрозами безопасности персональных данных Владелец Сайта определил 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.

Поскольку Владелец Сайта не обрабатывает биометрические и специальные персональные данные для Владельца Сайта актуальны угрозы, не связанные с наличием недокументированных возможностей в системном и прикладном программном обеспечении, то в организации устанавливается 3 тип угрозы безопасности.

Определение опасности угроз безопасности персональных данных проведено экспертным методом на основе опроса экспертов (специалистов в области защиты информации) с учетом результатов обследования информационных систем.

Актуальность угрозы в соответствии с Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных определяется с учетом оценок вероятности ее реализации и опасности. Результаты приведены ниже.

№ п/п	Форма реализации угрозы	Интерпретация реализуемости угрозы	Опасность угрозы	Актуальность угрозы
1. Утечки по техническим каналам				
1.1.	Утечка акустической информации	низкая	средняя	неактуальная
1.2.	Утечка видовой информации:			
1.2.1.	со средств отображения индивидуального пользования	низкая	средняя	неактуальная
1.2.2.	со средств коллективного отображения	низкая	средняя	неактуальная
1.2.3.	с печатных документов	низкая	средняя	неактуальная
1.3.	Утечка информации за счет побочных электромагнитных излучений информативных сигналов от технических средств	низкая	средняя	неактуальная
1.4.	Утечка информации за счет наводок информативного сигнала, обрабатываемого техническими средствами, на цепи электропитания и	низкая	средняя	неактуальная

	линии связи, выходящие за пределы контролируемой зоны			
1.5.	Утечка информации за счет радиозлучений или электрических сигналов от электронных устройств перехвата информации, подключенных к каналам связи или техническим средствам обработки информации	средняя	средняя	неактуальная
2.	Несанкционированный доступ к информации			
2.1.	Угрозы уничтожения, хищения, модификации технических средств ИСПДн (Информационная система персональных данных), носителей информации путем физического доступа к элементам ИСПДн:			
2.1.1.	кража ПК	низкая	средняя	неактуальная
2.1.2.	кража носителей информации	средняя	высокая	актуальная
2.1.3.	кража ключей и атрибутов доступа	низкая	средняя	неактуальная
2.1.4.	нарушение функционирования телекоммуникационных каналов, технических средств ИСПДн	низкая	низкая	неактуальная
2.1.5.	внедрение аппаратных закладок в технические средства ИСПДн	средняя	средняя	актуальная
2.1.6.	несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) технических средств ИСПДн	низкая	средняя	неактуальная
2.2.	Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программноматематических воздействий):			
2.2.1.	воздействие вредоносных программ	низкая	средняя	неактуальная
2.2.2.	недекларированные возможности общесистемного и прикладного ПО	низкая	средняя	неактуальная
2.2.3.	ошибки в общесистемном и прикладном ПО	низкая	средняя	неактуальная
2.2.4.	установка ПО не связанного с исполнением служебных обязанностей	средняя	высокая	актуальная
2.3.	Неумышленные деструктивные действия персонала:			
2.3.1.	утрата ключей и атрибутов доступа	низкая	средняя	неактуальная
2.3.2.	непреднамеренная модификация (уничтожение) информации сотрудниками	средняя	средняя	актуальная
2.3.3.	непреднамеренное отключение средств защиты	средняя	средняя	актуальная
2.3.4.	вывод из строя аппаратно-программных средств вследствие ошибочных действий	средняя	средняя	актуальная
2.4.	Умышленные деструктивные действия персонала:			
2.4.1.	произвольное копирование баз данных	низкая	высокая	актуальная
2.4.2.	накопление данных пользователем информационной системы	средняя	высокая	актуальная
2.4.3.	злонамеренное разрушение (искажение) информации	средняя	высокая	актуальная
2.4.4.	злонамеренное блокирование данных	низкая	средняя	актуальная
2.4.5.	фальсификация данных	средняя	высокая	актуальная
2.4.6.	несанкционированный доступ персонала информационной системы (далее - ИС) к ресурсам	средняя	средняя	актуальная
2.4.7.	компрометация аутентификатора	высокая	средняя	актуальная
2.4.8.	компрометация ключа СКЗИ (средство криптографической защиты информации)	средняя	высокая	актуальная
2.4.9.	нарушение функционирования средства защиты	низкая	высокая	актуальная
2.4.10.	произвольное создание точек входа в систему за счет неправомерных действий	высокая	средняя	неактуальная
2.5.	Угрозы несанкционированного доступа по каналам связи:			

2.5.1.	перехват передаваемой информации за пределами контролируемой зоны	низкая	средняя	неактуальная
2.5.2.	перехват в пределах контролируемой зоны внешними нарушителями	низкая	средняя	неактуальная
2.5.3.	перехват в пределах контролируемой зоны внутренними нарушителями	средняя	высокая	актуальная
2.5.4.	угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.	средняя	средняя	актуальная
2.5.5.	угрозы выявления паролей по сети	средняя	средняя	актуальная
2.5.6.	угрозы навязывание ложного маршрута сети	средняя	средняя	актуальная
2.5.7.	угрозы подмены доверенного объекта в сети	средняя	средняя	актуальная
2.5.8.	угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях	средняя	средняя	актуальная
2.5.9.	угрозы типа «Отказ в обслуживании»	средняя	средняя	актуальная
2.5.10.	угрозы удаленного запуска приложений	средняя	средняя	актуальная
2.5.11.	угрозы внедрения по сети вредоносных программ	средняя	высокая	актуальная
2.5.12.	вторжение в ИСПД по информационно-телекоммуникационным сетям	средняя	высокая	актуальная
2.5.13.	искажение в каналах передачи	низкая	средняя	неактуальная
3	Угрозы стихийного характера			
3.1.	Нарушение электроснабжения:			
3.1.1.	внешнего	низкая	средняя	неактуальная
3.1.2.	объектового	низкая	средняя	неактуальная
3.1.3.	Стихийное бедствие, катастрофа	низкая	средняя	неактуальная

#### **4. Применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.**

4.1. Владелец Сайта установил 4-ый уровень защищенности персональных данных при их обработке в информационных системах.

Владелец Сайта использует следующие информационные системы для обработки персональных данных:

№	Наименование системы	Подразделение организации	Тип базы данных	Доступ в интернет	Объем данных
1.					
3.					
4.	Файлы Microsoft Word, Microsoft Excel	Бухгалтерия, офис-менеджер, отдел маркетинга	Разрозненные файлы	Нет	1000 – 100000

4.2. Для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных класса 4 система защиты персональных данных Владельца Сайта включает:

- а) организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;
- б) обеспечение сохранности носителей персональных данных;
- в) управление доступом;
- г) регистрацию и учет;
- д) обеспечение целостности персональных данных;
- е) антивирусную защиту;
- ж) предотвращение и обнаружение вторжений.

4.3. Помещение, где осуществляется размещение сервера, содержащего персональные данные, находится в закрытом состоянии - на замке, с доступом только у работников, отвечающих за его работоспособность.

4.4. Режим безопасности помещений также в организации обеспечивается ограничением круга лиц, имеющих право доступа в помещения без сопровождения, определение мест хранения ключей от помещений, опечатывание помещения в нерабочее время.

4.5. Система управления доступом в информационных системах реализована в информационных системах персональных данных Владельца Системы и позволяет разграничивать доступ пользователей к отдельным объектам системы и отдельным группам персональных данных.

4.6. Пользователи информационных систем персональных данных объединены в группы, обладающие определенными ролями в процессе обработки данных. Роли определяют, какими правами доступа обладают пользователи информационных систем персональных данных.

4.7. Аутентификация пользователя при доступе к информационным системам персональных данных осуществляется с помощью уникального идентификатора пользователя (логина) и пароля. Пароль имеет цифробуквенную структуру, т.е. состоит одновременно из цифр и букв в русской или латинской раскладке клавиатуры. Пароль не может быть короче 6 символов. Пароли доступа в операционную систему у пользователей Представительства меняются регулярно.

4.8. Ответственным за неразглашение логина и пароля назначается пользователь информационной системы персональных данных.

4.9. Смену пароля пользователя доступа к корпоративным ресурсам компании, в том числе доступ к сети компании, почтовым сервисам, к серверу хранения информации, осуществляют сам пользователь. Оповещение о смене пароля направляется пользователю автоматически за 3 календарных дня до истечения срока действия пароля.

4.10. В случае, если создалась угроза компрометации пароля пользователя к корпоративным ресурсам или паролей информационных систем персональных данных, пользователь обязан незамедлительно обратиться к специалисту отвечающего за работу программных систем Представительства для внеплановой смены паролей.

4.11. Физический доступ посторонних лиц к рабочим местам пользователей информационных систем персональных данных запрещен, за исключением сотрудников, осуществляющих обслуживание информационных систем в присутствии пользователя. Автоматическая блокировка пользовательского интерфейса операционной системы осуществляется по истечению заданного времени бездействия.

4.12. Хранение централизованных баз данных информационных систем персональных данных осуществляется на основных серверах Представительства, расположенных в специально выделенном, закрытом помещении (серверной) с ограниченным доступом. Доступ в серверную имеют только работники осуществляющих обслуживание программных систем. Сетевой доступ к базам данных информационных систем персональных данных разграничен по правам доступа ролей пользователей, ведущих обработку персональных данных.

4.13. Система регистрации и учета реализована в информационных системах персональных данных Представительства программы 1С в виде электронных журналов учета действий пользователя, в которых регистрируются подлежащие учету действия пользователя: дата и время доступа пользователя к информационной системе персональных данных, тип объекта информационной системы, к которому был осуществлен доступ, вид действия, которое было произведено с объектом информационной системы.

4.14. Обеспечение целостности персональных данных при обработке в информационных системах персональных данных достигается применением процедуры автоматического многократно дублированного резервного копирования персональных данных с возможностью их быстрого восстановления в случае их изменения, повреждения, блокирования или уничтожения вследствие технологической аварии или несанкционированного доступа.

4.15. Резервное копирование персональных данных осуществляется автоматически в конце каждого дня.

4.16. Резервные копии персональных данных дублируются на основных серверах Владельца Сайта. Резервные копии персональных данных хранятся в виде электронных архивов в течение длительного времени, что позволяет в случае необходимости восстановить их с разной степенью актуальности. Файловый и сетевой доступ к резервным копиям персональных данных ограничен работниками, обслуживающими программные системы, оборудование организации, ответственными за резервное копирование и безопасность персональных данных при их автоматизированной обработке.

4.17. Работник, ответственный за резервное копирование персональных данных, имеет право в течение рабочего дня создавать резервные копии персональных данных по своему усмотрению в целях предотвращения их изменения, повреждения или уничтожения.

4.18. Антивирусная защита персональных данных обеспечена применением антивирусного программного комплекса на всех компьютерах Представительства. Обновление антивирусных баз осуществляется ежедневно в автоматическом режиме.

4.19. Предотвращение вторжений в электронно-вычислительную сеть Владельца Сайта и информационные системы персональных данных обеспечено следующими мерами:

- а) разграничение доступа пользователей к компьютерам с использованием логина и пароля;
- б) разграничение доступа пользователей к объектам информационных систем согласно ролям пользователей;
- в) автоматическая блокировка неиспользуемых длительное время операционных систем;
- г) использование специально оборудованного, закрытого помещения с ограниченным доступом для содержания серверов Представительства и хранения резервных копий персональных и технологических данных;
- д) использование брандмауэров на персональных компьютерах пользователей и серверах Представительства;
- е) регулярный мониторинг уязвимостей используемого программного обеспечения работниками, ответственными за безопасность персональных данных при их автоматизированной обработке, и обновление его в случае обнаружения критических уязвимостей;
- ж) регулярное резервное копирование системной технологической информации: файлов конфигурации, журналов регистрации, базы данных контроллеров домена, веб-сервера организации и прочей технологической информации.

## **6. Осуществление контроля над обеспечением безопасности персональных данных.**

6.1. Контроль за принимаемыми мерами по обеспечению безопасности персональных данных при обработке их в информационных системах персональных данных Владельца Сайта осуществляют работники, ответственные за безопасность персональных данных при их автоматизированной обработке.

6.2. Работники, ответственные за безопасность персональных данных при их автоматизированной обработке, обеспечивают:

- а) проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным;
- б) своевременное обнаружение фактов несанкционированного доступа к персональным данным или же их изменения, повреждения, блокировки или уничтожения;
- в) осуществление режима разграничения доступа пользователей к информационным системам персональных данных;
- г) осуществление контроля над плановой сменой паролей пользователей Владельца Сайта;
- д) недопущение воздействий на технические средства автоматизированной обработки персональных данных, в результате которых может быть нарушено их функционирование;
- е) поддержание в работоспособном состоянии и своевременное обновление технических и программных средств автоматизированной обработки персональных данных;
- ж) возможность незамедлительного восстановления персональных данных из резервных копий в случаях их изменения, повреждения, блокировки или уничтожения вследствие технологических неисправностей или несанкционированного доступа;
- з) контроль над осуществлением регулярного резервного копирования персональных данных;
- и) формирование и поддержание в актуальном состоянии перечней информационных систем персональных данных, используемых для обработки персональных данных;
- к) проведение инструктажа работников по безопасности персональных данных при их обработке на персональных компьютерах.

## **7. Права и обязанности работников, осуществляющих обработку персональных данных на автоматизированных рабочих местах.**

### **7.1. Работник, осуществляющий обработку персональных данных, обязан:**

- а) знать и выполнять требования действующих нормативных актов организации в сфере обработки персональных данных;
- б) знать и соблюдать установленные требования по условиям и порядку обработки персональных данных, учету, обеспечению безопасности персональных данных;
- в) соблюдать требования правил создания и использования паролей доступа к информационным системам персональных данных, в частности, обеспечивать: неразглашение своего индивидуального логина и пароля, в том числе в письменном виде в качестве записок-напоминаний, пометок и т.п, своевременную плановую смену пароля или внеплановую в случае угрозы его разглашения;
- г) обеспечивать недопущение за свое рабочее место посторонних лиц, а также работников, не имеющих доступ к обработке персональных данных на его рабочем месте;
- д) экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на нем информацией посторонними лицами;
- е) блокировать операционную систему своего рабочего персонального компьютера, ноутбука при его покидании путем нажатия комбинации Ctrl+Alt+Del и выбора опции «Блокировать компьютер»;
- ж) незамедлительно извещать работников, ответственных за безопасность персональных данных при их автоматизированной обработке, в случае выявленных фактов изменения, повреждения, блокирования или уничтожения персональных данных.

### **7.2. Работнику, осуществляющему обработку персональных данных, запрещается:**

- а) разглашать персональные данные третьим лицам;
- б) копировать персональные данные на внешние носители либо общедоступные сетевые ресурсы без разрешения своего непосредственного руководителя;
- в) самостоятельно вмешиваться в функционирование аппаратных и программных составляющих своего персонального компьютера, ноутбука, устанавливать программы, драйверы, GSM-модемы, подключать мобильные устройства и тому подобное оборудование;



- г) несанкционированно, без разрешения своего непосредственного руководителя и консультации с работниками, ответственными за безопасность персональных данных при их автоматизированной обработке, открывать общий доступ к папкам на своем компьютере, ноутбуке;
- д) отключать или блокировать средства защиты информации такие, как антивирусная программа и сетевой брандмауэр;
- е) хранить и обрабатывать на своем компьютере, ноутбуке информацию личного характера и прочую информацию, не имеющую непосредственного отношения к должностным обязанностям работника;
- ж) привлекать посторонних лиц для производства ремонта или настройки своего компьютера, ноутбука, корпоративного мобильного телефона, планшетного компьютера при наличии.

7.3. Работник, осуществляющий обработку персональных данных на персональном компьютере, имеет право получать инструктаж по безопасности персональных данных у работников, ответственных за безопасность персональных данных при их автоматизированной обработке, а также обращаться к ним по иным вопросам в целях обеспечения безопасности персональных данных.

## **8. Правила уничтожения носителей, содержащих персональные данные**

8.1. Уничтожение носителей, содержащих персональные данные субъектов персональных данных, должно соответствовать следующим правилам:

- быть конфиденциальным, исключая возможность последующего восстановления;
- оформляться юридически, в частности, актом о выделении документов, содержащих персональные данные субъектов персональных данных, к уничтожению и актом об уничтожении носителей, содержащих персональные данные субъектов персональных данных;
- должно проводиться комиссией по уничтожению персональных данных;
- уничтожение должно касаться только тех носителей, содержащих персональные данные субъектов персональных данных, которые подлежат уничтожению в связи с истечением срока хранения, достижением цели обработки указанных персональных данных либо утратой необходимости в их достижении, не допуская случайного или преднамеренного уничтожения актуальных носителей.

## **9. Порядок уничтожения носителей, содержащих персональные данные**

9.1. Персональные данные субъектов персональных данных хранятся не дольше, чем этого требуют цели их обработки, и подлежат уничтожению по истечении срока хранения, достижении целей обработки или в случае утраты необходимости в их достижении.

9.2. Носители, содержащие персональные данные субъектов персональных данных, уничтожаются в специально отведенном для этих целей помещении комиссией по уничтожению персональных данных, утвержденной приказом Главы представительства (далее – Комиссия).

9.3. Носители, содержащие персональные данные субъектов персональных данных, уничтожаются Комиссией в срок, не превышающий 30 дней с даты истечения срока хранения, достижения цели обработки персональных данных либо утраты необходимости в их достижении.

9.4. Комиссия производит отбор бумажных носителей персональных данных, подлежащих уничтожению, с указанием оснований для уничтожения.

9.5. На все отобранные к уничтожению документы составляется акт о выделении документов, содержащих персональные данные субъектов персональных данных, к уничтожению.

9.6. В актах о выделении документов, содержащих персональные данные субъектов персональных данных, к уничтожению и актах об уничтожении носителей, содержащих персональные данные субъектов персональных данных, исправления не допускаются.

9.7. Комиссия проверяет наличие всех документов, включенных в акт о выделении носителей, содержащих персональные данные субъектов персональных данных, к уничтожению.

9.8. По окончании сверки акт о выделении документов, содержащих персональные данные субъектов персональных данных, к уничтожению подписывается всеми членами Комиссии и утверждается проректором по направлению.

9.9. Носители, содержащие персональные данные субъектов персональных данных, отобранные для уничтожения и включенные в акт, после проверки их Комиссией передаются ответственному за уничтожение документов в помещение бухгалтерии.

9.10. Уничтожение носителей, содержащих персональные данные субъектов персональных данных, производится после утверждения акта в присутствии всех членов Комиссии, которые несут персональную ответственность за правильность и полноту уничтожения перечисленных в акте носителей.

9.11. Уничтожение персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

9.12. Уничтожение носителей, содержащих персональные данные, осуществляется в следующем порядке:

– уничтожение персональных данных, содержащихся на бумажных носителях, осуществляется путем измельчения на мелкие части, исключающие возможность последующего восстановления информации. Измельчение осуществляется с использованием shreddera (уничтожителя документов), установленного в помещении бухгалтерии, либо документы передаются на переработку (утилизацию) организациям, собирающим вторсырье (пункты приема макулатуры);

– уничтожение персональных данных, содержащихся на машиночитаемых носителях, осуществляется путем нанесения им неустраняемого физического повреждения, исключающего возможность их использования, а также восстановления данных. Вышеуказанное достигается путем деформирования, нарушения единой целостности носителя;

– подлежащие уничтожению файлы с персональными данными субъектов персональных данных, расположенные на жестком диске, удаляются средствами операционной системы компьютера с последующим «очищением корзины»;

– в случае допустимости повторного использования носителя CD-RW, DVD-RW применяется программное удаление («затирание») содержимого диска путем его форматирования с последующей записью новой информации на данный носитель.

## **10. Порядок сдачи макулатуры**

10.1. Документы по истечении срока хранения, достижении целей обработки или в случае утраты необходимости в их достижении подлежат уничтожению путем сдачи организациям, собирающим вторсырье (пункты приема макулатуры).

10.2. Выделенные документы по акту о выделении документов, содержащих персональные данные субъектов персональных данных, к уничтожению передаются к уничтожению в упакованном виде.

10.3. Документы, подлежащие вывозу, не должны содержать бумагу и картон, не пригодные для переработки; бумагу и картон, покрытые полиэтиленом и другими полимерными пленками; материал, выделяющий ядовитые и токсичные вещества.

10.4. Документы, подлежащие вывозу, не должны содержать:

– тряпье, веревку, шпагат из лубяных волокон и полимеров;

– металлические и деревянные изделия, кусочки стекла и керамики, камень, уголь, слюду, целлофан, целлулоид, полимерные материалы в виде изделий (пленок, гранул), пенопласт, искусственную и натуральную кожу, клеенку, битум, парафин, остатки химических и минеральных веществ и красок;

– влажность документов, подлежащая вывозу, должна быть не более 10 процентов.

10.5. Сдача оформляется приемо-сдаточными накладными, данные которых (дата сдачи, номер накладной, вес сданной макулатуры) указываются в акте о выделении документов, содержащих персональные данные субъектов персональных данных, к уничтожению.

10.6. Погрузка и вывоз документов осуществляются под контролем лица, ответственного за обеспечение сохранности документов структурного подразделения.

10.7. Отобранные к уничтожению документы перед сдачей на переработку в качестве макулатуры должны в обязательном порядке измельчаться до степени, исключающей возможность прочтения текста.

## **11. Порядок оформления документов об уничтожении персональных данных**

11.1. Об уничтожении носителей, содержащих персональные данные, Комиссия составляет и подписывает акт об уничтожении носителей, содержащих персональные данные субъектов персональных данных, который утверждается Главой представительства.

11.2. Акт об уничтожении носителей, содержащих персональные данные субъектов персональных данных, составляется по установленной форме.

В акте указываются:

- дата, место и время уничтожения;
- должности, фамилии, инициалы членов Комиссии;
- вид и количество уничтожаемых носителей, содержащих персональные данные субъектов персональных данных;
- основание для уничтожения;
- способ уничтожения.

11.3. Факт уничтожения носителей, содержащих персональные данные субъектов персональных данных, фиксируется в журнале учета документов, переданных на уничтожение. Данный документ является документом конфиденциального характера и вместе с актами хранится в помещении бухгалтерии в течение одного года. По истечении срока хранения акт о выделении документов, содержащих персональные данные субъектов персональных данных к уничтожению и акт об уничтожении носителей, содержащих персональные данные субъектов персональных данных, передаются в архив Представительства на хранение.

**ФОРМА**

**Обязательство  
о неразглашении персональных данных**

Я, \_\_\_\_\_, «\_\_\_» \_\_\_\_\_ года рождения,  
паспорт: № \_\_\_\_\_, выдан \_\_\_\_\_

зарегистрирован по адресу: \_\_\_\_\_,

понимаю, что получаю доступ к персональным данным работников Представительства фирмы «Эспарма ГмбХ» (Германия) г. Москва. Я также понимаю, что во время исполнения своих обязанностей я занимаюсь сбором, обработкой и хранением персональных данных работников.

Я понимаю, что разглашение такого рода информации может нанести ущерб работникам организации, как прямой, так и косвенный.

В связи с этим даю обязательство при работе (сборе, обработке и хранении) с персональными данными сотрудника соблюдать все описанные в Положении о персональных данных требования.

Я подтверждаю, что не имею права разглашать сведения о (об):

- анкетных и биографических данных;
- образовании;
- трудовом и общем стаже;
- составе семьи;
- паспортных данных;
- воинском учете;
- заработной плате работника;
- социальных льготах;
- специальности;
- занимаемой должности;
- наличии судимостей;
- адресе места жительства, домашнем телефоне;
- месте работы или учебы членов семьи и родственников;
- содержании трудового договора;
- составе декларируемых сведений о наличии материальных ценностей;
- содержании декларации, подаваемой в налоговую инспекцию;
- подлинниках и копиях приказов по личному составу;
- личных делах и трудовых книжках сотрудников;
- делах, содержащих материалы по повышению квалификации и переподготовке сотрудников, их аттестации, служебным расследованиям;
- копиях отчетов, направляемых в органы статистики;
- сведений о доходах, в том числе доходах с предыдущих мест работы.

Я предупрежден(а) о том, что в случае разглашения мной сведений, касающихся персональных данных работника, или их утраты я несу ответственность в соответствии со ст. 90 ТК РФ.

С Положением о порядке обработки персональных данных работников Представительства фирмы «Эспарма ГмбХ» (Германия) г. Москва и гарантиях их защиты ознакомлен(а).

\_\_\_\_\_  
(должность)  
«\_\_\_» \_\_\_\_\_ 201\_\_ г.

\_\_\_\_\_  
(подпись)      ФИО