

Положение обработки ПДН

1. Общие положения

1.1. Настоящее Положение об обработке и защите персональных данных (далее - Положение) определяет порядок сбора, хранения, передачи и любого другого использования персональных данных в ООО «SOUL CLINIC» (далее – Оператор) в соответствии с законодательством Российской Федерации.

1.2. Цель разработки Положения - определение порядка обработки персональных данных работников и иных субъектов персональных данных, персональные данные которых подлежат обработке, на основании полномочий Оператора; обеспечение защиты прав и свобод человека и гражданина, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну, а также установление ответственности должностных лиц, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

1.3. Действие Положения распространяется на все персональные данные субъектов, обрабатываемые Оператором с применением средств автоматизации и без применения таких средств.

1.4. Настоящее Положение является локальным актом Оператора и вступает в силу с момента его утверждения руководителем и действует бессрочно, до замены его новым Положением.

1.5. Все изменения в Положение вносятся приказом директора.

1.6. Все работники Оператора должны быть ознакомлены с настоящим Положением под роспись.

1.7. Мероприятия по обеспечению безопасности персональных данных являются составной частью деятельности Оператора.

1.8. Основными нормативными правовыми актами, регулирующие отношения, связанные с обработкой персональных данных Оператором являются:

- Конституция Российской Федерации;
- Гражданский кодекс;
- Трудовой кодекс;
- Кодекс об Административных правонарушениях;

- Федеральный закон от 27.07.2006г. № 149-ФЗ "Об информации, информационных технологиях и о защите информации";
- Федеральный закон Российской Федерации от 27 июля 2006г. № 152-ФЗ "О персональных данных";
- Федеральный закон от 04.05.2011 N 99-ФЗ "О лицензировании отдельных видов деятельности";
- Федеральный закон от 28.03.1998 № 53-ФЗ "О воинской обязанности и военной службе";
- Постановление Правительства Российской Федерации от 01 ноября 2012 г. № 1119 г. Москва "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных";
- Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации";
- Приказ ФСТЭК России от 18.02.2013 № 21 "Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных";
- Приказ ФСБ России от 10.07.2014 N 378 "Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности";
- другие нормативные правовые акты, регламентирующие достижение целей, предусмотренных Уставом Оператора.

2. Основные понятия

В настоящем Положении используются следующие основные понятия:

- Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

- Оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;
- 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;
- Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники;
- Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;
- Предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;
- Блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);
- 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;
- Обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;
- Информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;
- Трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

3. Персональные данные субъектов

Оператор осуществляет обработку персональных данных в соответствии с Уставом, целями обработки персональных данных определенными в Политике обработки персональных данных Оператора, в целях выполнения возложенных законодательством Российской Федерации на Оператора функций, полномочий и обязанностей.

Состав обрабатываемых персональных данных для каждой категории субъектов утверждается Приказом директора.

4. Сбор персональных данных

4.1. Все персональные данные субъектов следует получать у них самих. Если персональные данные возможно получить только у третьей стороны, то субъект должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Должностное лицо Оператора должно сообщить о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа субъекта дать письменное согласие на их получение.

4.2. Субъект предоставляет должностному лицу Оператора достоверные сведения о себе. Должностное лицо проверяет достоверность сведений, сверяя данные, предоставленные субъектом, с имеющимися у субъекта документами.

4.3. Оператор не имеет права получать и обрабатывать персональные данные сотрудников и прочих физических лиц об их расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, интимной жизни, сведений о состоянии здоровья, за исключением случаев, предусмотренных законодательством.

4.4. В соответствии с Трудовым Кодексом РФ и федеральными законами, регламентирующими вопросы обязательного предоставления Оператором информации в органы власти и фонды (ИФНС, ПФР, ФСС, военкоматы и т.п.) определен перечень персональных данных, которые субъект персональных данных обязан представить оператору в связи с осуществлением трудовой деятельности.

4.5. В случае отказа субъекта предоставить свои персональные данные, Оператор не сможет на законных основаниях осуществлять возложенные на него законодательством Российской Федерации обязанности, что приведет к тому, что субъект персональных данных не сможет быть принят на работу.

5. Порядок обработки персональных данных

5.1 Персональные данные обрабатываются лицами согласно Перечня должностей, допущенных к обработке персональных данных, утвержденного директором.

5.2 Допуск к работе с персональными данными осуществляется только после дачи работником обязательства о неразглашении конфиденциальной информации, в том числе персональных данных, ознакомления под роспись с Политикой обработки персональных данных, локальными актами Оператора по вопросам обработки и защиты персональных данных.

5.3 Работники, осуществляющие обработку персональных данных, получают доступ к персональным данным в объеме, минимально необходимом для выполнения должностных и функциональных обязанностей и в форме определенной Перечнем должностей, допущенных к обработке персональных данных.

5.4 Для осуществления обработки персональных данных без использования средств автоматизации используются типовые формы документов, утвержденные органами государственной власти, государственными внебюджетными фондами, локальными актами Оператора. Документы, содержащие персональные данные предоставляемые в военкоматы, по запросам правоохранительных органов, органов государственной власти и местного самоуправления на основании законных оснований оформляются в свободной форме с указанием персональных данных в объеме, не превышающем законные требования.

5.5 Хранение персональных данных должно осуществляться не дольше чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, иным нормативным правовым документом или договором, стороной которого, является субъект персональных данных. Места хранения материальных носителей персональных данных определяются Приказами об утверждении мест хранения.

5.6 Хранение персональных данных в электронном виде осуществляется на серверах и автоматизированных рабочих местах лиц, допущенных к обработке персональных данных определенных Перечнем мест хранения персональных данных в информационной системе персональных данных.

5.7 По достижению целей обработки персональных данных Оператор осуществляет хранение персональных данных в соответствие со сроками хранения, утвержденными номенклатурой дел в части не противоречащей требованиям нормативных актов Российской Федерации.

5.8 Персональные данные содержащиеся в базах данных в электронном виде – до окончания срока, определенного федеральными законами и номенклатурой дел (дела оперативного хранения – менее 10 лет). По окончании данного срока персональные данные должны быть перенесены на архивное хранение.

5.9 Допускается хранение копий баз данных с персональными данными в электронном архиве в течение срока хранения и в объеме соответствующих архивных документов.

5.10 Руководитель и сотрудники Оператора (операторы) при обработке персональных данных сотрудника должны соблюдать следующие общие требования:

- обработка персональных данных может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, для достижения целей обработки персональных данных Оператора, достижения целей, предусмотренных Уставом и Политикой обработки персональных данных Оператора, на основании согласия на обработку персональных данных данного субъектом;
- при определении объема и содержания обрабатываемых персональных данных оператор должен руководствоваться Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным законом «О персональных данных» от 27.07.2006 № 152-ФЗ и иными федеральными законами.
- при принятии решений, затрагивающих интересы субъекта, Оператор, как оператор, не имеет права основываться на персональных данных субъекта, полученных исключительно в результате их автоматизированной обработки или электронного получения.
- защита персональных данных субъекта от неправомерного их использования или утраты обеспечивается Оператором за счет своих средств в порядке, установленном федеральным законом.
- работники и их представители должны быть ознакомлены под роспись с документами Оператора, устанавливающими порядок обработки персональных данных, а также об их правах и обязанностях в этой области.
- во всех случаях отказ субъекта от своих прав на сохранение и защиту персональных данных недействителен.

6. Передача персональных данных

При передаче персональных данных субъекта Оператор должен соблюдать следующие требования:

6.1 При передаче персональных данных Оператор предупреждает лиц, получающих персональные данные субъекта, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требует от этих лиц

подтверждения того, что это правило соблюдено. Лица, получившие персональные данные субъекта, обязаны соблюдать режим конфиденциальности. Данное положение не распространяется на обмен персональными данными субъектов в порядке, установленном федеральными законами.

6.2 Передавать персональные данные субъектов их законным представителям в порядке, установленном федеральными законами, и ограничивать эту информацию только теми персональными данными субъекта, которые необходимы для выполнения указанными представителями их функции.

6.3 Передача персональных данных третьим лицам может осуществляться с согласия субъекта персональных данных или в случаях, предусмотренных федеральными законами, Политикой обработки персональных данных, Уставом Оператора.

6.4 Передача персональных данных работников осуществляется исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, получении образования и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

6.5 Передача персональных данных третьим лицам в целях оказания услуг осуществляется в соответствии с Политикой обработки персональных данных и заключенными договорами.

6.6 Передача персональных данных в иные учреждения, организации, государственные и муниципальные органы осуществляется только с письменного указания руководителя.

6.7 Перечень организаций, передачу персональных данных которым осуществляется на регулярной основе в соответствии с заключенными договорами утверждается Приказом руководителя.

7. Мероприятия по обеспечению безопасности персональных данных

7.1 Общие положения

Лицо, ответственное по организации обработки персональных данных назначается Приказом руководителя.

Для разработки и осуществления мероприятий по обеспечению безопасности персональных данных при их обработке, руководитель назначается лицо, ответственное за обеспечение безопасности персональных данных.

Лица, ответственные за организацию обработки и обеспечение безопасности персональных данных, в своей деятельности руководствуется нормативными документами в области обработки персональных данных, должностными инструкциями и локальными актами Оператора.

Разработка и осуществление мероприятий по обеспечению безопасности персональных данных может осуществляться также сторонними организациями на договорной основе, имеющими лицензии на право проведения соответствующих работ.

Мероприятия по защите персональных данных осуществляются в соответствии с внутренним планом.

Организация режима обеспечения физической безопасности должна обеспечивать сохранность носителей персональных данных, технических средств обработки персональных данных и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

Лица, осуществляющие обработку персональных данных обязаны соблюдать требования Инструкции по обеспечению безопасности персональных данных.

7.2 Мероприятия по обеспечению безопасности персональных данных при обработке в информационных системах персональных данных

7.2.1. Общие требования

Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, включающей организационные, правовые и технические меры, в том числе средства защиты информации и используемые в информационной системе информационные технологии.

При обработке персональных данных в информационных системах Оператора должно быть обеспечено:

- проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации.
- своевременное обнаружение фактов несанкционированного доступа к персональным данным.

- недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование.

- возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

- контроль над обеспечением уровня защищенности персональных данных при их обработке в информационной системе.

7.2.2. Перечень мероприятий по обеспечению безопасности персональных данных обрабатываемых в информационных системах персональных данных

Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах включают в себя:

- определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз.

- разработку на основе модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем.

- проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации.

- установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией.

- обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними.

- учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;

- учет машинных носителей персональных данных

- учет лиц, допущенных к работе с персональными данными в информационной системе.

- контроль над соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией.

- разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных при их обработке в информационной системе, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений.

7.2.3. Определение уровня защищенности персональных данных при их обработке в информационной системе

При обработке в информационной системе персональные данные подлежат обязательному определению уровня защищенности.

Для проведения определения уровня защищенности персональных данных при их обработке в информационной системе Оператора приказом Руководителя Оператора назначается комиссия.

Результаты определения уровня защищенности персональных данных оформляются соответствующим актом.

7.3. Мероприятия по обеспечению безопасности персональных данных при их обработке без использования средств автоматизации

7.3.1. Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и определен перечень лиц, осуществляющих обработку персональных данных, либо имеющих к ним доступ.

7.3.2. Необходимо обеспечивать отдельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

8.3.3. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключаящие несанкционированный к ним доступ.

7.3.4. Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных данных (далее - материальные носители), в специальных разделах или на полях форм (бланков).

7.3.5. При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

7.3.6. Лица, осуществляющие обработку персональных данных без использования средств автоматизации (в том числе работники Оператора или лица, осуществляющие такую обработку по договору с Оператором), должны быть проинформированы о факте обработки ими персональных данных, обработка которых осуществляется без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки;

7.3.7. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовая форма), должны соблюдаться следующие условия:

а) типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, имя (наименование) и адрес Оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки персональных данных;

б) типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации, - при необходимости получения письменного согласия на обработку персональных данных;

в) типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;

г) типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

7.3.8. При ведении журналов, содержащих персональные данные, необходимые для однократного пропуска субъекта персональных данных на территорию

Оператора, или в иных аналогичных целях, должны соблюдаться следующие условия:

а) необходимость ведения такого журнала должна быть предусмотрена локальными актами оператора, содержащим сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, способы фиксации и состав информации, запрашиваемой у субъектов персональных данных, перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала, сроки обработки персональных данных, а также сведения о порядке пропуска субъекта персональных данных на территорию Оператора, без подтверждения подлинности персональных данных, сообщенных субъектом персональных данных;

б) копирование содержащейся в таких журналах (реестрах, книгах) информации не допускается;

в) персональные данные каждого субъекта персональных данных могут заноситься в такой журнал (книгу, реестр) не более одного раза в каждом случае пропуска субъекта персональных данных на территорию Оператора.

7.3.9. При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению отдельной обработки персональных данных, в частности:

а) при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;

б) при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

7.3.10. Уничтожение или обезличивание части 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).

8.3.11. Правила, предусмотренные пунктами 8.3.9, 8.3.10 настоящего Положения, применяются также в случае, если необходимо обеспечить отдельную обработку зафиксированных на одном материальном носителе персональных данных и информации, не являющейся персональными данными.

8.3.12. Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

8. Уничтожение персональных данных

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. В результате уничтожения персональных данных становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и уничтожаются материальные носители персональных данных.

Уничтожение персональных данных субъекта осуществляется комиссией. Документальной фиксации уничтожения персональных данных субъекта является оформлением акта уничтожения персональных данных по утвержденной форме.

Уничтожение бумажных носителей персональных данных осуществляется путем сожжения, либо измельчения в бумаго-уничтожающей машине.

При необходимости уничтожения части персональных данных, уничтожается материальный носитель с предварительным копированием сведений, не подлежащих уничтожению, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению.

Уничтожение машинных носителей информации производится следующим путем:

- оптические диски и дискеты – путем оплавления в бесформенную массу;
- флеш накопители – путем ударно-механического повреждения основной платы, на которой располагается флеш память;

- накопитель на жестком магнитном диске – путем ударно-механического повреждения исключения возможности восстановления информации в лабораторных условиях.

Для уничтожения информации с машинных носителей информации могут использоваться программные методы гарантированного удаления информации, в которых используются основные алгоритмы гарантированного удаления данных.

Персональные данные, хранящиеся в электронных базах данных, уничтожаются путем удаления персональных данных конкретного субъекта из баз данных. В случае невозможности произвести удаление персональных данных из базы данных применяется обезличивание персональных данных для обеспечения невозможности определить принадлежность персональных данных конкретному субъекту без дополнительных сведений.

9. Контроль и надзор за выполнением требований настоящего Положения

Контроль и надзор за выполнением требований настоящего Положения осуществляется в соответствии с ежегодным Планом внутренних проверок состояния защиты персональных данных, утверждаемым директором.

Контроль заключается в проверке выполнения требований нормативных документов по защите информации, а также в оценке обоснованности и эффективности, принятых мер. Он может проводиться ответственным за организацию обработки персональных данных, или на договорной основе сторонними организациями, имеющими лицензии на деятельность по технической защите конфиденциальной информации.

10. Финансирование мероприятий по обеспечению безопасности персональных данных

Финансирование мероприятий производится из средств Оператора.

11. Ответственность за нарушение требований настоящего положения

Лица, виновные в нарушении требований настоящего Положения, несут гражданскую, уголовную, административную, дисциплинарную и иную ответственность, предусмотренную законодательством Российской Федерации.