ПОЛИТИКА АО «АСТОН КОНСАЛТИНГ» В ОТНОШЕНИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ОРГАНИЗАЦИИ ПРОВЕДЕНИЯ ЛАБОРАТОРНЫХ ИССЛЕДОВАНИЙ.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Термины и определения

1.1.1. «Персональные данные (ПДн)» — любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

1.1.2. «Оператор 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.

1.1.3. «Обработка персональных данных» — любое действие (операция) или совокупность действий (операций) с персональными данными, совершаемых с использованием средств автоматизации или без их использования. Обработка персональных данных включает в себя, в том числе: сбор; запись; систематизацию; накопление; хранение; уточнение (обновление, изменение); извлечение; использование; передачу (распространение, предоставление, доступ); обезличивание; блокирование; удаление; уничтожение.

1.1.4. «Автоматизированная обработка персональных данных» — обработка персональных данных с помощью средств вычислительной техники.

1.1.5. «Распространение персональных данных» — действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

1.1.6. «Предоставление персональных данных» — действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

1.1.7. «Блокирование персональных данных» — временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

1.1.8. «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.

1.1.9. «Обезличивание персональных данных» — действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

1.1.10. «Информационная система персональных данных (ИСПДн)» — совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

1.1.11. «Доступ к информации» — возможность получения информации и ее использования.

1.1.12. «Информационные технологии» — процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

1.1.13. «Несанкционированный доступ (несанкционированные действия)» — доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

1.1.14. «Носитель информации (носитель персональных данных)» — материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

1.1.15. «Правила разграничения доступа» — совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

1.1.16. «Субъект доступа» — лицо или процесс, действия которого регламентируются правилами разграничения доступа.

1.1.17. «Субъект персональных данных», «субъект» — физическое лицо, к которому относятся персональные данные.
1.1.18. «Технические средства информационной системы персональных данных» — технические средства, осуществляющие обработку ПДн (средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т. п.), средства защиты информации).
1.1.19. «Средство защиты информации» — техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.
1.1.20. «База данных» — представленная в объективной форме совокупность самостоятельных материалов, систематизированных таким образом, чтобы эти материалы могли быть найдены и обработаны с помощью электронной вычислительной машины (ЭВМ).
1.1.21. «Юридические последствия» — случаи возникновения, изменения или прекращения правоотношений, затрагивающие права, свободы и законные интересы граждан.

1.2. Назначение политики

1.2.1. В процессе ведения своей деятельности Акционерное общество «Астон Консалтинг» (далее – «**Оператор**», «**Организация**») обрабатывает персональные данные физических лиц — субъектов персональных данных. Оператор считает важнейшими задачами обеспечение законности и справедливости при обработке персональных данных, соблюдение их конфиденциальности и обеспечение их безопасности, безопасности процессов при их обработке.
1.2.2. Настоящий документ определяет политику Оператора в отношении обработки и защиты персональных данных (далее – «**Политика**») при реализации проекта по организации проведения лабораторных исследований, с целью защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну. Настоящий документ является общедоступным документом, определяющим политику Оператора в отношении обработки персональных данных и содержащий сведения о реализуемых требованиях к защите персональных данных.
1.2.3. Настоящая Политика действует в отношении персональных данных, которые Оператор может получить в рамках проекта по организации проведения лабораторных исследований. Политика разработана в соответствии с нормами п. 2 ст. 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – «**Закон**»). Оператор обрабатывает персональные данные в строгом соответствии с Законом. Кроме того, Оператор соблюдает обязанности и требования, установленные законодательством Российской Федерации, в том числе, и в тех случаях, которые прямо не оговорены в настоящей Политике.
1.2.4. Настоящая Политика применима ко всем случаям обработки персональных данных Оператором или от имени Оператора, вне зависимости от того, производится она вручную или автоматизировано.
1.2. Действующая Политика размещена на странице по адресу: https://raregenome.aston-health.com/
1.3. Организация обеспечивает неограниченный доступ к настоящей Политике, к сведениям о реализуемых требованиях к защите персональных данных.

2. СОСТАВ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Персональные данные, полученные при реализации проекта по организации проведения лабораторных исследований – информация о пациентах, их законных представителях и прочая информация, получаемая и обрабатываемая Организацией при в соответствии с нормами действующего законодательства РФ и целями деятельности Общества.

2.2. **Состав персональных данных Пациентов:**

2.2.1. фамилия, имя и отчество;

2.2.2. паспортные данные или данные иного документа, удостоверяющего личность;

2.2.3. пол;

2.2.4. гражданство;

2.2.5. дата, месяц, год рождения;

2.2.6. адреса и дата регистрации по месту жительства (места пребывания);

2.2.7. контактный номер телефона;

2.2.8. контактный адрес электронной почты;

2.2.9. специальная категория персональных данных, включая: анамнез, диагноз, виды оказанной помощи, проведение лекарственной и иной терапии, результаты лабораторных и инструментальных исследований, иные медицинские данные, необходимые для целей обработки.

2.2.10. иные сведения, необходимые для достижения целей обработки персональных данных в соответствии с условиями настоящей Политики.

2.3. **Состав персональных данных Представителей Пациентов:**

2.3.1. фамилия, имя и отчество;

2.3.2. паспортные данные или данные иного документа, удостоверяющего личность;

2.3.3. адрес регистрации по месту жительства;

2.3.4. подтверждение представительства.

2.4. **Состав персональных данных медицинских специалистов:**

2.5. фамилия, имя и отчество;

2.6. место и адрес работы;

2.7. должность, специальность.

2.7.1. контактный номер телефона;

2.7.2. контактный адрес электронной почты.

3. ЦЕЛИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Обработка ПДн осуществляется исключительно в целях ведения хозяйственной деятельности, определенной Уставом Организации с соблюдением законодательства РФ.

3.2. Персональные данные Пациентов, Представителей Пациентов и медицинских специалистов обрабатываются Оператором для достижения следующей цели:

3.2.1. реализация проекта диагностики Пациентов, включающего организацию проведения лабораторных исследований, направленных на выявление и/или мониторинг течения болезни, формирование и анализ статистических данных, ведения базы данных лиц, которые прошли диагностику.

4. УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Лица, допущенные к обработке ПДн, в обязательном порядке знакомятся с настоящей Политикой, другими организационно-распорядительными документами Организации, касающиеся обработки персональных данных и принимают обязательство о неразглашении информации, содержащей персональные данные, в установленном порядке.

4.2. В целях организации обработки и обеспечения безопасности ПДн в Организации:
- назначается уполномоченное лицо, ответственное за организацию обработки ПДн. Допускается поручение указанных функций стороннему лицу, привлекаемому на основании заключенного договора.

4.3. Лицо, ответственное за организацию обработки ПДн в Организации, получает указания непосредственно от руководителя Организации и подотчетно ему.

4.4. Организация предоставляет лицу, ответственному за организацию обработки ПДн, сведения об обработке ПДн в Организации, необходимые в соответствии с требованиями законодательства в области ПДн.

4.5. В Организации формируется и поддерживается в актуальном состоянии перечень ПДн, обрабатываемых Оператором. Данный перечень составляется на основании сведений, предоставляемых руководителями подразделений, осуществляющих обработку ПДн.

4.6. В перечне ПДн определяются все цели, для достижения которых осуществляется обработка ПДн. Заявляемые цели обработки ПДн должны быть законны.

4.7. При определении правовых оснований обработки ПДн определяются реквизиты федерального закона, а также подзаконных актов, и (или) иных актов органов государственной власти, и (или) иных документов, на основании которых осуществляется обработка ПДн.

4.8. Обработка ПДн без определенного и законного основания не допускается.

4.9. На основании определенных целей обработки ПДн, способов обработки и создаваемых в процессе такой обработки различных видов документов устанавливаются сроки такой обработки ПДн, в том числе сроки хранения ПДн.

4.10. При использовании документов, содержащих ПДн, в различных целях, определение сроков обработки (в том числе хранения) таких документов устанавливается в соответствии с максимальным применимым сроком.

4.11. Для всех целей обработки и соответствующих наборов ПДн определяется необходимость получения согласия субъекта ПДн в случаях, установленных законодательством РФ. Решение о необходимости получения согласия субъекта принимается в соответствии с положениями законодательства РФ.

4.12. На основании принятого решения составляется типовая форма получения согласий субъектов ПДн на обработку их ПДн или основание, определяющее возможность обработки ПДн без получения согласия.

4.13. Согласие может быть получено в письменной форме, в форме электронного документа, признаваемого в соответствии с законодательством РФ равнозначным письменному согласию, содержащему собственноручную подпись субъекта ПДн, или иной форме, обеспечивающей возможность подтверждения получения согласия.

4.14. В случаях, определенных законодательством РФ, согласие на обработку ПДн должно быть получено только в письменной форме. Равнозначным содержащему собственноручную подпись субъекта ПДн согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью.

4.15. В случае получения согласия от законного представителя субъекта ПДн или представителей субъекта ПДн они обязаны представить документы, подтверждающие их полномочия.

4.16. Для удобства субъектов, а также контроля учета требований законодательства, допускается включение согласия в типовые формы (бланки) материальных носителей ПДн и в договоры с субъектами ПДн.

4.17. Оператор организовывает хранение в течение установленных сроков обработки ПДн полученных согласий субъектов на обработку их ПДн или соответствующих свидетельств наличия оснований, при которых такое согласие не требуется.

4.18. Согласие на обработку ПДн может быть отозвано субъектом ПДн путем направления обращения Оператору.

4.19. Оператор уведомляет уполномоченный орган по защите прав субъектов ПДн о своем намерении осуществлять обработку ПДн.

4.20. Уведомление готовится лицом, ответственным за организацию обработки ПДн в Организации, в соответствии с рекомендованной формой, устанавливаемой уполномоченным органом по защите прав субъектов ПДн, подписывается руководителем Организации и направляется в виде документа на бумажном носителе или в форме электронного документа.

4.21. В случае изменения сведений, а также в случае прекращения обработки ПДн Оператор обязан уведомить об этом уполномоченный орган по защите прав субъектов ПДн.

4.22. В случае изменения сведений, содержащихся в уведомлении об обработке ПДн, структурное подразделение Организации, являющееся инициатором таких изменений в обработке ПДн, готовит изменения в уведомление и передает такие изменения лицу, ответственному за организацию обработки ПДн. Дальнейшие действия по подготовке изменений в уведомление для передачи в уполномоченный орган по защите прав субъектов ПДн осуществляются аналогично действиям при первоначальной подаче уведомления.

5. ДЕЙСТВИЯ (ОПЕРАЦИИ) С ПЕРСОНАЛЬНЫМИ ДАННЫМИ

5.1. **Сбор персональных данных**

5.1.1. В Организации применяются следующие способы получения ПДн от субъектов ПДн:
заполнение субъектом ПДн (либо его законным представителем) соответствующих форм (в том числе для заключения договора) или заполнение их законным представителем;

5.1.2. Обращение на горячую линию Оператора № 8 (800) 301-06-51 для ввода данных после получения согласия Субъекта.

5.1.2. В том случае если предоставление ПДн является обязательным в соответствии с законодательством РФ, необходимо разъяснить субъекту ПДн юридические последствия отказа предоставить его ПДн.

5.1.3. Организация освобождается от обязанности предоставить субъекту ПДн сведения, в случаях, если:

- субъект ПДн уведомлен об осуществлении обработки его ПДн Оператором;
- ПДн получены Организацией на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн;
- обработка ПДн, разрешенных субъектом персональных данных для распространения, осуществляется с соблюдением запретов и условий, предусмотренных статьей 10.1 Закона о персональных данных;
- предоставление субъекту ПДн сведений нарушает права и законные интересы третьих лиц.

5.1.4. Оператор осуществляет обработку ПДн для статистических или иных исследовательских целей, если при этом не нарушаются права и законные интересы субъекта персональных данных.

5.2. **Систематизация, накопление, уточнение и использование персональных данных**

5.2.1. Систематизация, накопление, уточнение, использование ПДн могут осуществляться любыми законными способами в соответствии с правилами, инструкциями, руководствами, регламентами и иными документами, определяющими технологический процесс обработки информации.

5.2.2. Уточнение ПДн должно производиться только на основании законно полученной в установленном порядке информации.

5.2.3. Решение об уточнении ПДн субъекта ПДн принимается лицом, ответственным за организацию обработки ПДн в Организации.

5.2.4. Использование ПДн должно осуществляться исключительно в заявленных целях. Использование ПДн в заранее не определенных и не оформленных установленным образом целях не допускается.

5.3. **Запись и извлечение персональных данных**

5.3.1. Запись ПДн в ИСПДн Организации может осуществляться с любых носителей информации или из других ИСПДн.

5.3.2. Извлечение ПДн из ИСПДн может осуществляться с целью:

- вывода ПДн на бумажный или иной носитель информации, не предназначенный для его обработки средствами вычислительной техники;
- вывода ПДн на носители информации, предназначенные для их обработки средствами вычислительной техники.

5.3.3. Извлечение ПДн допускается только на машинные носители, зарегистрированные и учтенные в установленном в Организации порядке.

5.4. **Передача персональных данных**

5.4.1. Перед осуществлением передачи ПДн проверяется основание на осуществление такой передачи и наличие согласия на передачу ПДн в согласии субъекта ПДн на обработку ПДн или наличие иных законных оснований.

5.4.2. Передача ПДн осуществляется лицами в соответствии с их обязанностями.

5.4.3. Передача носителей ПДн осуществляется лично или с использованием курьерской службы, соблюдающей необходимые требования по защите ПДн.

5.4.4. Передача ПДн по информационным каналам осуществляется с использованием защищенных каналов связи или с использованием средств криптографической защиты информации.

5.4.5. Передача ПДн должна осуществляться на основании:

- договора с третьим лицом, в адрес которого осуществляется передача ПДн;
- основанного на законодательстве РФ запроса, полученного от третьего лица, в адрес которого осуществляется передача ПДн;
- исполнения возложенных законодательством РФ на Организацию функций, полномочий и обязанностей.

5.4.6. Передача ПДн без согласия соответствующего субъекта ПДн или без иных законных оснований запрещается.

5.4.7. Оператор не осуществляет распространение ПДн субъекта.

5.4.8. Трансграничная передача ПДн Оператором не осуществляется.

5.5. **Поручение обработки персональных данных другому лицу**

5.5.1. Организация вправе поручить обработку ПДн другому лицу:

- с согласия субъекта ПДн;
- без согласия субъекта ПДн, если такая передача предусмотрена законодательством РФ.

5.5.2. Лицо, осуществляющее обработку ПДн по поручению Организации, обязано соблюдать правила обработки и требования по защите ПДн, предусмотренные поручением в соответствии с требованиями законодательства РФ. В поручении Организации:

- должен быть определен перечень действий (операций) с ПДн, которые будут совершаться лицом, осуществляющим обработку ПДн;
- должны быть определены цели обработки ПДн;
- должна быть установлена обязанность такого лица соблюдать конфиденциальность ПДн;
- должна быть установлена обязанность такого лица обеспечивать безопасность ПДн при их обработке и принимать необходимые меры, направленные на обеспечение выполнения обязанностей, предусмотренных Законом о персональных данных;

- должна быть установлена обязанность по запросу Оператора в течение срока действия поручения, в том числе до обработки ПДн, предоставлять документы и иную информацию, подтверждающие принятие мер и соблюдение в целях исполнения поручения Оператора требований по обеспечению безопасности ПДн, установленных Законом о персональных данных;
- должны быть указаны требования к защите обрабатываемых ПДн, в том числе требование об уведомлении Оператора о случаях, предусмотренных частью 3.1 статьи 21 Закона о персональных данных;
- должна быть установлена ответственность такого лица перед Организацией, в случаях нарушений установленных требований и законодательства РФ в области ПДн;
- при необходимости получения согласий на обработку ПДн от субъектов ПДн, должен быть определен порядок сбора согласий субъектов ПДн.

5.5.3. Поручением Организации может являться договор, содержащий указанную выше информацию.

5.5.4. Ответственность перед субъектом ПДн за обеспечение безопасности его ПДн всегда несет Организация.

5.5.5. Все указанные выше требования являются актуальными в соответствующем применении в случае поручения другим лицом обработки ПДн Организации.

5.6. **Хранение персональных данных**

5.6.1. ПДн хранятся в соответствии со сроками и условиями хранения, определенными для конкретных ПДн в соответствии с необходимостью их обработки в согласии субъекта на обработку таких ПДн и локальных актах Оператора.

5.6.2. Хранение ПДн субъектов ПДн в Организации осуществляется как без использования средств автоматизации (на бумажных и магнитных носителях), так и при помощи таковых в базах данных ИСПДн.

5.6.3. Хранение ПДн в Организации допускается в форме документов - зафиксированной на бумажном носителе информации (содержащей ПДн) с реквизитами, позволяющими ее идентифицировать и определить субъекта ПДн.

5.6.4. Хранение ПДн осуществляется на определенных для этой роли носителях, в соответствии с требованиями по обеспечению безопасности ПДн, в защищенном месте и под контролем ответственных лиц.

5.6.5. При использовании сменных машинных носителей информации для записи и хранения ПДн они подлежат обязательному учету в журнале учета сменных машинных носителей. На все сменные носители ПДн должны быть нанесены соответствующие реквизиты.

5.6.6. Хранение ПДн в Организации осуществляется в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен федеральным законом и (или) договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн.

5.6.7. Оператор обеспечивает раздельное хранение ПДн обрабатываемых в различных целях путем реализации организационных и технических мер.

5.6.8. Оператор обеспечивает запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации.

5.7. **Блокирование персональных данных**

5.7.1. Блокированием ПДн называется временное прекращение обработки ПДн (за исключением случаев, если обработка необходима для уточнения ПДн).

5.7.2. Возможность блокирования ПДн конкретного субъекта ПДн должна обеспечиваться во всех ИСПДн Организации. В качестве блокирования может использоваться блокирование прав доступа к конкретным ИСПДн или полям данных, содержащих блокируемые ПДн.

5.7.3. Блокирование ПДн в Организации осуществляется:
- в случае выявления неправомерной обработки ПДн при обращении субъекта ПДн или его представителя либо по запросу субъекта ПДн или его представителя, либо уполномоченного органа по защите прав субъектов ПДн с момента такого обращения или получения указанного запроса на период проверки;
- в случае отсутствия возможности уничтожения ПДн в установленные сроки до их уничтожения.

5.7.4. После устранения выявленной неправомерной обработки ПДн Организация осуществляет снятие блокирования ПДн.

5.7.5. Решение о блокировании и снятии блокирования ПДн субъекта ПДн принимается ответственным лицом за организацию обработки ПДн в Организации.

5.8. **Обезличивание персональных данных**

5.8.1. Обезличивание ПДн может быть проведено с целью ведения статистических данных, снижения ущерба от разглашения защищаемых ПДн, снижения требуемого уровня защищенности ПДн и по достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено законодательством РФ.

5.8.2. Способы обезличивания при условии дальнейшей обработки ПДн:
- введение идентификаторов - метод реализуется путем замены части ПДн, позволяющих идентифицировать субъекта их идентификаторами и созданием справочника соответствия;
- изменение состава и семантики - метод реализуется путем обобщения, изменения значений атрибутов ПДн или удаления части сведений, позволяющих идентифицировать субъекта;
- декомпозиция - метод состоит в разделении множества атрибутов ПДн на несколько подмножеств и создании таблиц, устанавливающих связи между подмножествами с последующим раздельным хранением записей, соответствующим подмножествам этих атрибутов;
- перемешивание - метод заключается в перестановке отдельных значений или групп значений атрибутов ПДн между собой;
- автоматическое обезличивание ПДн с использованием соответствующего программного обеспечения, обеспечивающего надлежащую защиту ПДн от несанкционированного доступа или обратного обезличивания (деобезличивания).

5.8.3. Возможно объединение различных методов обезличивания в одну процедуру.

5.8.4. Допускается производить обезличивание ПДн при обработке без использования средств автоматизации способом, исключающим дальнейшую обработку этих ПДн с сохранением возможности обработки иных данных, зафиксированных на бумажном носителе (удаление, вымарывание).

5.8.5. При использовании в Организации процедуры обезличивания ПДн должны храниться отдельно от обезличенных данных. При использовании обезличенных данных следует:
- организовать раздельное хранение обезличенных данных и дополнительной информации о выбранном методе реализации процедуры обезличивания и параметрах процедуры обезличивания;
- обеспечивать конфиденциальность данной дополнительной информации при хранении и передаче.

5.8.6. Действия, связанные с внесением изменений и дополнений в состав обезличенных данных, а также запросов на обработку данных следует регистрировать в журналах учета. В случае если обезличивание ПДн и иные действия с ПДн осуществляется автоматически, данные сведения в журнале учета не отражаются.

5.9. **Удаление и уничтожение персональных данных**

5.9.1. ПДн подлежат уничтожению в следующих случаях:
- истечение установленного срока хранения и обработки ПДн;

- по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом;
- в случае если сохранение ПДн более не требуется для целей обработки ПДн;
- ПДн являются незаконно полученными или не являются необходимыми для заявленной цели обработки;
- в случае выявления неправомерной обработки ПДн, если обеспечить правомерность обработки ПДн невозможно;
- в случае отзыва субъектом ПДн согласия на обработку его ПДн, если отсутствуют иные основания для обработки данных ПДн.

5.9.2. При уничтожении ПДн необходимо:
- убедиться в необходимости уничтожения ПДн;
- убедиться в том, что уничтожаются те ПДн, которые предназначены для уничтожения;
- уничтожить ПДн подходящим способом;
- осуществить уведомление соответствующих лиц о факте уничтожения, в случае необходимости.

5.9.3. При уничтожении ПДн могут применяться следующие способы:
- измельчение в бумагорезательной (бумагоуничтожительной) машине — для бумажных документов;
- тщательное вымарывание (с проверкой тщательности вымарывания) — для сохранения возможности обработки иных данных, зафиксированных на бумажном носителе, содержавшем ПДн;
- измельчение в специальной бумагорезательной (бумагоуничтожительной) машине или физическое уничтожение (разрушение) носителей информации - для носителей информации на оптических дисках;
- физическое уничтожение частей носителей информации — разрушение или сильная деформация - для носителей информации на жестком магнитном диске (уничтожению подлежат внутренние диски и микросхемы); SSD-дисках, USB- и Flash-носителях (уничтожению подлежат модули и микросхемы долговременной памяти);
- стирание с помощью средств уничтожения информации — для записей в базах данных и отдельных документов на машинном носителе;
- иные методы, в результате которых становится невозможным восстановление ПДн.

5.9.4. При уничтожении ПДн необходимо учитывать их наличие в архивных базах данных и производить уничтожение во всех копиях базы данных, если иное не установлено действующим законодательством РФ.

5.9.5. При необходимости уничтожения части ПДн допускается уничтожать бумажный носитель одним из указанных в настоящей Политике способов, с предварительным копированием сведений, не подлежащих уничтожению, способом, исключающим одновременное копирование ПДн, подлежащих уничтожению.

5.9.6. Уничтожение ПДн производится лицами, обрабатывающими ПДн в соответствующей ИСПДн, в которой производится уничтожение ПДн, в присутствии лица, ответственного за организацию обработки ПДн в Организации.

5.9.7. Подтверждение уничтожения ПДн осуществляется Оператором в соответствии с требованиями, установленными уполномоченным органом по защите прав субъектов персональных данных. В том числе, по факту уничтожения ПДн составляется акт уничтожения ПДн, который подписывается лицами, производившими уничтожение, заверяется лицом, ответственным за организацию обработки ПДн в Организации, присутствовавшим при уничтожении и осуществляется выгрузка из журнала регистрации событий в ИСПДн (при автоматизированной обработки ПДн).

5.9.8. Хранение актов уничтожения ПДн и выгрузки из журнала регистрации событий в ИСПДн осуществляется в течение 3 лет, если иное не установлено нормативно-правовыми актами РФ.

5.10. **Доступ уполномоченных лиц к персональным данным**

5.10.1. Уполномоченным лицам предоставляются права доступа к персональным данным в объеме, необходимом для выполнения их обязанностей, в целях выполнения данных обязанностей и только на период действия указанной необходимости.

5.10.2. Список уполномоченных лиц, имеющих доступ к персональным данным, определяется в порядке, предусмотренным внутренними документами Организации. Перечень подразделений и уполномоченных лиц, допущенных к обработке ПДн, разрабатывается и пересматривается по мере необходимости (изменение организационно-штатной структуры, введение новых должностей и т.п.) на основании заявок начальников структурных подразделений. Доступ к персональным данным лиц, не имеющих надлежащим образом оформленного допуска, запрещается.

5.10.3. Уполномоченные лица получают права доступа к персональным данным после:

- ознакомления и изучения требований настоящей Политики и иных внутренних организационно-распорядительных документов Организатора в части, их касающейся;
- прохождения инструктажа о соблюдении порядка обработки ПДн;
- ознакомления с видами ответственности за нарушение (невыполнение) норм законодательства РФ в сфере обработки и защиты ПДн;
- принятия обязательства о неразглашении информации, содержащей персональные данные. Процедура предоставления доступа к персональным данным, обрабатываемым в ИСПДн, осуществляется в соответствии с установленным порядком путем подачи заявки на доступ к ИСПДн. Предоставление доступа к ПДн и их обработка уполномоченными лицами осуществляется в пределах контролируемой зоны в помещениях, предназначенных для обработки персональных данных.

6. ИНФОРМАЦИОННЫЕ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. В документах Организации определяется перечень информационных систем персональных данных (ИСПДн) и их основные характеристики, включая:

- наименование информационной системы ПДн;
- назначение информационной системы ПДн;
- параметры, характеризующие информационную систему ПДн.

6.2. **Наименование информационной системы персональных данных.**

6.2.1. С целью идентификации каждой информационной системы ПДн в Организации ей присваивается наименование, которое должно отражать основное назначение данной информационной системы либо наименование программных средств обработки ПДн в данной информационной системе.

6.3. **Назначение информационной системы персональных данных.**

6.3.1. Назначение ИСПДн определяется в соответствии с сервисами, реализуемыми ИСПДн, внутренними задачами или с определенными требованиями, предъявляемыми действующим законодательством РФ.

6.4. **Параметры, характеризующие информационную систему персональных данных.**

6.4.1. Для каждой ИСПДн Организации определяет параметры, характеризующие такую ИСПДн, в том числе:

- наименование информационной системы ПДн;
- назначение информационной системы ПДн;
- цель обработки ПДн в ИСПДн;

- перечень ПДн о субъекте ПДн, обрабатываемых в ИСПДн;
- места обработки ПДн, используемые носители и компоненты ИСПДн;
- пользователи ИСПДн и их права доступа;
- прочие характеристики.

6.5. **Требования к уполномоченным лицам, осуществляющим доступ к персональным данным или их обработку.**

6.5.1. Организация осуществляет ознакомление уполномоченных лиц, осуществляющих обработку ПДн или осуществляющих доступ к ним, с положениями законодательства РФ о ПДн (в том числе с требованиями к защите ПДн), локальными актами Организации по вопросам обработки ПДн, включая настоящую Политику.

6.5.2. Обязанности и ответственность работников и других уполномоченных лиц Организации по обработке и защите ПДн определяются в настоящей Политике и иных документах Организации.

7. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ

7.1.1. 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, в специальных разделах или на полях форм (бланков).

7.1.2. 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 для каждой категории персональных данных должен использоваться отдельный материальный носитель.

7.1.3. При использовании типовых форм документов, характер которых предполагает или допускает включение в них персональных данных, должны соблюдаться следующие условия:

- типовая форма и (или) связанные с ней документы (инструкции по заполнению и т.п.) должны содержать сведения о цели обработки данных, 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 и общее описание способов их обработки Оператором;
- типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных (если такое согласие необходимо по законодательству);
- 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;
- типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, обрабатываемых для достижения несовместимых целей.

7.1.4. 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 и установить перечень лиц, осуществляющих обработку персональных данных (имеющих к ним доступ). Перечень мест хранения материальных носителей персональных данных утверждается локальным актом Оператора.

7.1.5. Лица, осуществляющие обработку персональных данных, должны быть проинформированы о факте обработки ими персональных данных, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами и локальными актами Оператора.

8. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

8.1. Обеспечение безопасности персональных данных при их обработке

8.1.1. В соответствии с требованиями действующего законодательства о ПДн, при обработке ПДн Организация обязана принимать необходимые организационные и технические меры для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения ПДн, а также от иных неправомерных действий.

8.1.2. Безопасность ПДн достигается путем исключения несанкционированного, в том числе случайного, доступа к ПДн, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение ПДн, а также иных несанкционированных действий.

8.1.3. Защита ПДн, обрабатываемых в Организации, осуществляется в соответствии с установленным порядком организации и проведения работ по защите персональных данных.

8.1.4. Работы по обеспечению безопасности ПДн при их обработке в ИСПДн являются неотъемлемой частью работ по созданию информационных систем.

8.2. Режим ограниченного доступа к персональным данным

8.2.1. С целью реализации требований законодательства РФ по обеспечению безопасности ПДн в Организации вводится режим ограниченного доступа к ПДн.

8.2.2. Создание режима ограниченного доступа к персональным данным включает в себя:

- создание и уточнение перечня информационных систем персональных данных;
- создание порядка организации и проведения работ по защите персональных данных;
- создание и уточнение перечня помещений, предназначенных для обработки персональных данных;
- создание и уточнение перечня лиц, которым разрешен доступ к ПДн;
- разработку, оформление и уточнение перечня информационных ресурсов, содержащих ПДн (мест расположения баз данных или иных документов и массивов, содержащих ПДн);
- дополнение договоров с контрагентами вопросами обязательств по обеспечению безопасности передаваемых им ПДн;
- внесение изменений в инструкции и иные внутренние документы, предусматривающие регулирование отношений по использованию ПДн;
- при прекращении их полномочий уполномоченных лиц, передаче (возврате) имеющихся в их распоряжении бумажных носителей информации, содержащих ПДн;
- документирование и реализация разрешительной системы доступа (матриц доступа) к информационным (программным) ресурсам в информационных системах ПДн Организации;
- разработка инструкций для уполномоченных лиц по вопросам обеспечения безопасности ПДн.

8.2.3. Организация и контроль за выполнением указанных мероприятий возлагается на лица, ответственные за организацию обработки и защиты ПДн в Организации. Разрабатываемые документы подлежат утверждению руководителем Организации.

8.3. **Система защиты персональных данных**

8.3.1. Безопасность ПДн при их обработке в информационных системах Организации обеспечивается с помощью системы защиты ПДн, включающей организационные меры и средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки ПДн), а также используемые информационные технологии.

8.4. **Средства защиты информации**

8.4.1. Технические и программные средства обработки ПДн должны удовлетворять устанавливаемым в соответствии с законодательством РФ требованиям, обеспечивающим защиту информации.

8.4.2. Эксплуатация средств защиты информации должна осуществляться строго в соответствии с эксплуатационной документацией на такие средства. Лица, эксплуатирующие средства защиты информации, должны быть ознакомлены с такой документацией.

8.5. **Требования к помещениям, в которых производится обработка персональных данных**

8.5.1. Размещение информационных систем, специальное оборудование и охрана помещений, в которых ведется работа с персональными данными, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей ПДн и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

9. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ПРАВИЛ ОБРАБОТКИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

9.1. Лица, виновные в нарушении норм, регулирующих обработку и защиту ПДн, несут дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством РФ.

9.2. Лица, имеющие доступ к ПДн, несут персональную ответственность за несанкционированное распространение ПДн, а также за соблюдение установленного в Организации порядка обеспечения безопасности в отношении ПДн.

9.3. Руководитель подразделения, разрешающий доступ лиц к ПДн, несет персональную ответственность за:

- данное разрешение;
- выполнение возложенных на него функций по организации обработки и защите ПДн, обрабатываемых подразделением.

9.4. Каждое лицо, получающее для работы носитель информации, содержащий ПДн, несет персональную ответственность за сохранность данного носителя.

9.5. Лица, в обязанность которых входит обработка ПДн, обязаны обеспечить каждому субъекту ПДн возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законодательством РФ. Неправомерный отказ в предоставлении собранных в установленном порядке документов, либо несвоевременное предоставление таких документов или иной информации в случаях, предусмотренных законом, либо предоставление неполной или заведомо ложной информации, либо иные нарушения законодательства в области ПДн - влекут за собой ответственность, предусмотренную действующим законодательством.

10. ОБЯЗАННОСТИ ОПЕРАТОРА ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

10.1. Организация при обработке персональных данных выполняет свои обязанности как оператор персональных данных, предусмотренные Законом и указанные в настоящей Политике.

10.2. В целях обеспечения прав и свобод человека и гражданина Организация и его представители при обработке персональных данных обязаны соблюдать следующие общие требования:

10.2.1. принимать необходимые правовые, организационные и технические меры или 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

10.2.2. обрабатывать персональные данные только законными способами и на законных основаниях;

10.2.3. ограничивать обработку персональных данных при достижении заранее определенных и законных целей;

10.2.4. обрабатывать только те персональные данные, которые отвечают целям обработки;

10.2.5. обеспечивать соответствие содержания и объема обрабатываемых персональных данных целям обработки, не допускать избыточности обрабатываемых персональных данных по отношению к заявленным целям обработки;

10.2.6. обеспечивать точность персональных данных, их достаточность и актуальность по отношению к целям обработки персональных данных;

10.2.7. осуществлять хранения персональных данных в форме, позволяющей определить субъекта персональных данных, но не дольше, чем этого требуют цели обработки персональных данных, если иной срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект 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;

10.2.8. сообщать в порядке, предусмотренном законодательством РФ, субъекту персональных данных или его представителю информацию о наличии и составе 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 либо в течение тридцати дней с даты получения запроса субъекта персональных данных или его представителя;

10.2.9. если предоставление персональных данных является обязательным в соответствии с федеральным законом, разъяснять субъекту персональных данных юридические последствия отказа предоставить его персональные данные;

10.2.10. при сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети «Интернет», обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации.

10.2.11. В случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных, оператор обязан с момента выявления такого инцидента оператором, уполномоченным органом по защите прав субъектов персональных данных или иным заинтересованным лицом уведомить уполномоченный орган по защите прав субъектов персональных данных:

1) в течение двадцати четырех часов о произошедшем инциденте, о предполагаемых причинах, повлекших нарушение прав субъектов персональных данных, и предполагаемом вреде, нанесенном правам субъектов персональных данных, о принятых мерах по устранению последствий соответствующего инцидента, а также предоставить сведения о лице, уполномоченном оператором на взаимодействие с уполномоченным органом по защите прав субъектов персональных данных, по вопросам, связанным с выявленным инцидентом;

2) в течение семидесяти двух часов о результатах внутреннего расследования выявленного инцидента, а также предоставить сведения о лицах, действия которых стали причиной выявленного инцидента (при наличии).

11. ПРАВА СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ.

11.1. Организация при обработке персональных данных обеспечивает необходимые условия для беспрепятственной реализации Субъектом персональных данных своих прав.

11.2. На свободный доступ и беспрепятственную возможность ознакомления с настоящей Политикой.

11.3. Субъект персональных данных имеет право на доступ к своим персональным данным.

11.4. Субъект персональных данных имеет требовать исключения или исправления неверных или неполных персональных данных;

11.5. Субъект персональных данных имеет право на получение сведений, указанных в части 7 статьи 14 Закона о персональных данных. Право субъекта персональных данных на доступ к своим персональным данным ограничивается в случаях, предусмотренных Законом о персональных данных.

11.6. Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

11.7. Субъект персональных данных обладает иными правами, предусмотренными Законом.

12. КОНФИДЕНЦИАЛЬНОСТЬ.

12.1. Оператор принимает все необходимые меры для сохранности конфиденциальности ПДн в том числе в ИСПДн Оператора, при необходимости заключает соглашения о конфиденциальности с лицами, получающими доступ к ПДн субъекта на законных основаниях.

12.2. Организация и ее представители, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия Субъекта персональных данных, если иное не предусмотрено федеральными законами.