

ПОЛОЖЕНИЕ
об обработке и защите персональных данных
в Организации

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение разработано в соответствии с законодательством Российской Федерации о персональных данных (далее по тексту - ПДн) и определяет политику Организации (далее по тексту – Оператор) в отношении обработки и защиты ПДн.

1.2. В настоящем Положении используются следующие термины:

персональные данные (ПДн) - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту ПДн);

обработка ПДн - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с ПДн, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн;

автоматизированная обработка ПДн – обработка ПДн с помощью средств вычислительной техники;

распространение ПДн - действия, направленные на раскрытие ПДн неопределенному кругу лиц; предоставление ПДн - действия, направленные на раскрытие ПДн определенному лицу или определенному кругу лиц;

блокирование ПДн - временное прекращение обработки ПДн (за исключением случаев, если обработка необходима для уточнения ПДн);

уничтожение ПДн - действия, в результате которых становится невозможным восстановить содержание ПДн в ИСПДн и/или в результате которых уничтожаются материальные носители ПДн;

обезличивание ПДн - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность ПДн конкретному субъекту ПДн;

информационная система персональных данных (ИСПДн) - совокупность содержащихся в базах данных ПДн и обеспечивающих их обработку информационных технологий и технических средств;

трансграничная передача ПДн - передача ПДн на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

1.3. Настоящее Положение определяет:

- порядок и условия обработки ПДн Оператором, включая порядок передачи ПДн третьим лицам, особенности автоматизированной и неавтоматизированной обработки ПДн, порядок доступа к ПДн, порядок организации внутреннего контроля и ответственность за нарушения при обработке ПДн,
- процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных,
- цели обработки ПДн,
- категории субъектов, персональные данные которых обрабатываются.
- содержание обрабатываемых ПДн для каждой цели обработки ПДн,
- сроки обработки и хранения обрабатываемых ПДн,
- порядок уничтожения ПДн при достижении целей обработки или при наступлении иных законных оснований.

1.4. Действие настоящего Положения распространяется на все процессы по сбору, систематизации, накоплению, хранению, уточнению, использованию, распространению (в том числе передачу), обезличиванию, блокированию, уничтожению ПДн, осуществляемых с использованием средств автоматизации и без их использования.

1.5. Настоящее Положение вступает в силу с момента его утверждения Директором "Организации"

(далее по тексту - Руководитель Оператора) и действует бессрочно, до замены его новым Положением.

1.6. Все изменения в Положение вносятся соответствующим Приказом.

2. ЦЕЛИ И ЗАДАЧИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Обработка ПДн должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка ПДн, несовместимая с целями сбора ПДн.

2.2. Не допускается объединение баз данных, содержащих ПДн, обработка которых осуществляется в целях, не совместимых между собой.

2.3. Обработке подлежат только ПДн, которые отвечают целям их обработки.

2.4. Содержание и объем обрабатываемых ПДн должны соответствовать заявленным целям обработки. Обрабатываемые ПДн не должны быть избыточными по отношению к заявленным целям их обработки.

2.5. Получение персональных данных может осуществляться как путем представления их самими субъектами персональных данных, так и путем получения их из иных источников.

2.6. Персональные данные следует получать у самого субъекта персональных данных. 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. Оператор должен сообщить субъекту персональных данных о целях, предполагаемых источниках и способах получения персональных данных, а так же о характере подлежащих получению персональных данных и последствиях отказа субъекта дать письменное согласие на их получение.

2.7. Обработка ПДн субъектов может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, при наличии договорных отношений между субъектами ПДн и Оператором, при обращении субъектов к Оператору с обращениями, заявлениями и жалобами, а также за оказанием услуг, предоставляемых Оператором, и в иных случаях, связанных с осуществлением Оператором его деятельности.

2.8. Оператор не имеет права получать и обрабатывать персональные данные субъекта о его политических, религиозных и иных убеждениях и частной жизни.

2.9. Оператор не имеет права получать и обрабатывать персональные данные субъекта о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом.

2.10. Основными целями обработки ПДн являются:

- 2.10.1. исполнение договорных обязательств;
- 2.10.2. предоставление услуг;
- 2.10.3. рассмотрение обращений граждан.

3. СОДЕРЖАНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОБРАБАТЫВАЕМЫХ ОПЕРАТОРОМ

3.1. В "Организации" обрабатываются ПДн следующих субъектов ПДн:

- физических лиц (потребителей услуг Оператора);
- индивидуальных предпринимателей - контрагентов Оператора;
- иных физических лиц, ПДн которых обрабатываются у Оператора.

3.2. Данный перечень может пересматриваться по мере необходимости.

3.3. К персональным данным субъектов ПДн, обрабатываемых Оператором для достижения предусмотренных Уставом Оператора целей деятельности по оказанию медицинских услуг (исполнение договорных обязательств, предоставление услуг, рассмотрение обращений граждан, реализация прав участников "Организации" и др.), относятся:

- фамилия, имя, отчество;
- пол;
- число, месяц, год рождения;
- вид документа, удостоверяющего личность;
- адрес регистрации по месту жительства;
- номер контактного телефона или сведения о других способах связи;
- сведения о состоянии здоровья, а также состояния здоровья ближайших родственников;
- реквизиты полиса ДМС;
- факты предыдущих обращений за медицинской помощью и их результаты.иные персональные данные, необходимые для достижения целей, предусмотренных пунктами 2.12.3. - 2.12.6. настоящего Положения

4. ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ. ПОРЯДОК ДОСТУПА В ПОМЕЩЕНИЯ, В КОТОРЫХ ОБРАБАТЫВАЮТСЯ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

4.1. Сотрудники Оператора, которые в силу выполняемых должностных обязанностей постоянно работают с ПДн, получают доступ к необходимым категориям ПДн на срок выполнения ими соответствующих должностных обязанностей на основании Перечня лиц, допущенных к работе с ПДн, который утверждается Руководителем Оператора.

4.2. Список лиц, имеющих доступ к ПДн для информационной системы, должен поддерживаться в актуальном состоянии.

4.3. Оператором установлен разрешительный порядок доступа к ПДн. Сотрудникам Оператора предоставляется доступ к работе с ПДн исключительно в пределах и объеме, необходимых для выполнения ими своих должностных обязанностей на основании решения Руководителя.

4.4. В случае, если сотруднику сторонней организации необходим доступ к ПДн Оператора, то необходимо, чтобы в договоре со сторонней организацией были прописаны условия конфиденциальности ПДн и обязанность сторонней организации и ее сотрудников по соблюдению требований текущего законодательства в области защиты ПДн (поручение Оператора). Кроме того, в случае доступа к ПДн лиц, не являющихся сотрудниками Оператора, должно быть получено согласие субъектов ПДн на предоставление их ПДн третьим лицам. Указанное согласие не требуется, если ПДн предоставляются в целях исполнения гражданско-правового договора, заключенного Оператором с субъектом ПДн.

4.6. Доступ сотрудника Оператора к ПДн прекращается с даты, прекращения трудовых отношений, либо даты изменения должностных обязанностей сотрудника и/или исключения сотрудника из списка лиц, имеющих право доступа к ПДн.

4.7. Оператор вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных. Лицо, осуществляющее обработку персональных данных по поручению Оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные настоящим Положением и действующим законодательством. В случае, если Оператор поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет Оператор. Лицо, осуществляющее обработку персональных данных по поручению Оператора, несет ответственность перед Оператором.

4.8. Запрещается оставлять материальные носители ПДн без присмотра в незапертых помещениях, в которых осуществляется обработка персональных данных.

4.9. Сотрудники, постоянно работающие в помещениях, в которых осуществляется обработка ПДн, должны быть допущены к работе с соответствующими видами персональных данных Руководителем Оператора.

4.10. В служебных помещениях Оператора применяются административные, технические, физические и процедурные меры, направленные для защиты ПДн от нецелевого использования,

несанкционированного доступа, раскрытия, потери, изменения и уничтожения обрабатываемых ПДн. К указанным мерам относятся:

- физические меры защиты: двери, снабженные замками, сейфы и безопасное уничтожение носителей, содержащих ПДн;
- технические меры защиты: применение антивирусных программ, программ защиты, установление паролей на персональных компьютерах;
- организационные меры защиты: обучение и ознакомление с принципами безопасности и конфиденциальности, доведение до сотрудников, допущенных к обработке ПДн, важности защиты персональных данных и способов обеспечения защиты.

5. ПРОЦЕДУРЫ, НАПРАВЛЕННЫЕ НА ВЫЯВЛЕНИЕ И ПРЕДОТВРАЩЕНИЕ НАРУШЕНИЙ ЗАКОНОДАТЕЛЬСТВА В СФЕРЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. Оператор обязан принимать необходимые правовые, организационные, технические и другие меры для обеспечения безопасности ПДн.

5.2. При обработке ПДн в информационных системах 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 ПДн;
- недопущение воздействия на технические средства автоматизированной обработки ПДн, в результате которого может быть нарушено их функционирование;
- возможность незамедлительного восстановления ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- постоянный контроль над обеспечением уровня защищенности ПДн.

5.3. Оператором используются технические средства и программное оборудование для обработки и защиты ПДн.

5.4. Оператором ведется журнал учета и хранения съемных носителей информации.

5.5. Все лица, допущенные к работе с ПДн, а также связанные с эксплуатацией и техническим сопровождением ИСПДн должны быть под роспись ознакомлены с требованиями настоящего Положения, а также должны подписать Обязательство об обеспечении конфиденциальности персональных данных сотрудниками Оператора.

5.6. Обработка ПДн без использования средств автоматизации (далее - неавтоматизированная обработка ПДн) может осуществляться в виде документов на бумажных носителях и в электронном виде (файлы, базы данных) на электронных носителях информации.

5.7. При неавтоматизированной обработке ПДн должно быть обеспечено:

- осуществление обработки ПДн таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ;
- раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях;
- соблюдение условий, обеспечивающих сохранность персональных данных и исключающих несанкционированный к ним доступ, при хранении материальных носителей.

5.8. Документы и внешние электронные носители информации, содержащие ПДн, должны храниться в служебных помещениях в надежно запираемых и опечатываемых шкафах (сейфах). При этом должны быть созданы надлежащие условия, обеспечивающие их сохранность.

5.9. Сотрудники обязаны незамедлительно сообщать Руководителю Оператора об утрате или недостатке носителей информации, составляющей ПДн, а также о причинах и условиях возможной

утечки ПДн. В случае попытки посторонних лиц получить от сотрудника ПДн, обрабатываемых Оператором, незамедлительно известить об этом Руководителя Оператора.

6. СОГЛАСИЕ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. Субъект ПДн принимает решение о предоставлении своих ПДн и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку ПДн должно быть конкретным, информированным и сознательным. Согласие на обработку ПДн может быть дано субъектом ПДн или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено законодательством РФ. В случае получения согласия на обработку ПДн от представителя субъекта ПДн полномочия данного представителя на дачу согласия от имени субъекта ПДн проверяются Оператором.

6.2. Получение письменного согласия на обработку ПДн осуществляется сотрудником Оператора, при получении ПДн от субъекта ПДн, путем оформления письменного согласия по форме, установленной Оператором.

7. ПРАВА СУБЪЕКТА В ОТНОШЕНИИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОБРАБАТЫВАЕМЫХ ОПЕРАТОРОМ

7.1. Субъект ПДн имеет право на получение информации, касающейся обработки его ПДн, в том числе содержащей:

- подтверждение факта обработки ПДн Оператором;
- правовые основания и цели обработки ПДн;
- цели и применяемые Оператором способы обработки ПДн;
- наименование и место нахождения Оператора, сведения о лицах (за исключением сотрудников Оператора), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с Оператором или на основании федерального закона;
- обрабатываемые ПДн, относящиеся к соответствующему субъекту ПДн, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- сроки обработки ПДн, в том числе сроки их хранения;
- порядок осуществления субъектом ПДн прав, предусмотренных Федеральным законом «О персональных данных»;
- информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению оператора, если обработка поручена или будет поручена такому лицу;
- иные сведения, предусмотренные Федеральным законом «О персональных данных» или другими федеральными законами.

7.2. Запрос субъекта персональных данных должен содержать сведения позволяющие провести его идентификацию:

- фамилию, имя, отчество субъекта ПДн или его представителя;
- номер основного документа, удостоверяющего личность субъекта ПДн или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе;
- сведения, подтверждающие участие субъекта ПДн в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки ПДн Оператором;
- подпись субъекта ПДн или его представителя.

Запрос может быть направлен электронной почтой и подписан электронной подписью в соответствии с законодательством Российской Федерации.

7.3. При обращении либо при получении запроса субъекта ПДн или его представителя Оператор должен предоставить сведения в доступной форме и в них не должны содержаться ПДн, относящиеся к другим субъектам ПДн, за исключением случаев, если имеются законные основания для раскрытия таких ПДн. Оператор обязан предоставить информацию по запросу субъекта ПДн или его представителя в порядке, предусмотренном Федеральным законом «О персональных данных».

7.4. Субъект ПДн вправе требовать от Оператора уточнения его ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

7.5. Возможность ознакомления с ПДн предоставляется на безвозмездной основе лицом ответственным за обработку ПДн.

8. ПРАВА И ОБЯЗАННОСТИ ОПЕРАТОРА ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

8.1. Оператор вправе:

8.1.1. Поручить обработку ПДн другому лицу с согласия субъекта ПДн, если иное не предусмотрено законодательством РФ, на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, либо путем принятия государственным или муниципальным органом соответствующего акта.

8.1.2. В случае отзыва субъектом ПДн согласия на обработку ПДн, продолжить обработку ПДн без согласия субъекта ПДн при наличии оснований, указанных в законодательстве РФ.

8.1.3. Отказать субъекту ПДн в выполнении повторного запроса сведений, не соответствующего условиям, предусмотренным законодательством РФ. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на Операторе.

8.1.4. Самостоятельно определять состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей Оператора, предусмотренных законодательством РФ.

8.2. Оператор обязан:

8.2.1. Оператор до начала обработки ПДн обязан уведомить уполномоченный орган по защите прав субъектов ПДн о своем намерении осуществлять обработку ПДн, за исключением случаев, предусмотренных законодательством РФ.

8.2.2. При получении доступа к ПДн не раскрывать третьим лицам и не распространять ПДн без согласия субъекта ПДн, если иное не предусмотрено законодательством РФ.

8.2.3. При сборе ПДн, предоставить субъекту ПДн по его просьбе информацию, предусмотренную законодательством РФ.

Если предоставление ПДн Оператору для субъекта ПДн является обязательным в соответствии с Федеральным законом «О персональных данных», Оператор обязан разъяснить субъекту ПДн юридические последствия отказа предоставить его ПДн.

8.2.4. Если ПДн получены не от субъекта ПДн, Оператор, за исключением случаев, предусмотренных законодательством РФ, до начала обработки таких ПДн обязан предоставить субъекту ПДн следующую информацию:

- наименование и адрес Оператора или его представителя;
- цель обработки ПДн и ее правовое основание;
- предполагаемые пользователи ПДн;
- установленные Федеральным законом «О персональных данных» права субъекта ПДн;
- источник получения ПДн.

- 8.2.5. Принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей Оператора, предусмотренных законодательством РФ.
- 8.2.6. Опубликовать на сайте Оператора настоящее Положение, определяющее политику Оператора в отношении обработки ПДн.
- 8.2.7. Представить документы и локальные акты, предусмотренные законодательством РФ, и/или иным образом подтвердить принятие мер, необходимых и достаточных для обеспечения выполнения обязанностей Оператора, по запросу уполномоченного органа по защите прав субъектов ПДн.
- 8.2.8. При обработке ПДн принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн.
- 8.2.9. Сообщить в порядке, предусмотренном законодательством РФ, субъекту ПДн или его представителю безвозмездно информацию о наличии ПДн, относящихся к соответствующему субъекту ПДн, а также предоставить возможность ознакомления с этими ПДн при обращении субъекта ПДн или его представителя либо в течение тридцати дней с даты получения запроса субъекта ПДн или его представителя.
- 8.2.10. В случае отказа в предоставлении информации о наличии ПДн о соответствующем субъекте ПДн или ПДн субъекту ПДн или его представителю при их обращении либо при получении запроса субъекта ПДн или его представителя оператор обязан дать в письменной форме мотивированный ответ, содержащий ссылку на положение законодательства РФ, являющееся основанием для такого отказа, в срок, не превышающий тридцати дней со дня обращения субъекта ПДн или его представителя либо с даты получения запроса субъекта ПДн или его представителя.
- 8.2.11. В срок, не превышающий семи рабочих дней со дня предоставления субъектом ПДн или его представителем сведений, подтверждающих, что ПДн являются неполными, неточными или неактуальными, Оператор обязан внести в них необходимые изменения. В срок, не превышающий семи рабочих дней со дня представления субъектом ПДн или его представителем сведений, подтверждающих, что такие ПДн являются незаконно полученными или не являются необходимыми для заявленной цели обработки, оператор обязан уничтожить такие ПДн. Оператор обязан уведомить субъекта ПДн или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым ПДн этого субъекта были переданы.
- 8.2.12. Сообщить в уполномоченный орган по защите прав субъектов ПДн по запросу этого органа необходимую информацию в течение тридцати дней с даты получения такого запроса.
- 8.2.13. В случае выявления неправомерной обработки ПДн, осуществляемой Оператором или лицом, действующим по поручению Оператора, Оператор в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку ПДн или обеспечить прекращение неправомерной обработки ПДн лицом, действующим по поручению Оператора. В случае если обеспечить правомерность обработки ПДн невозможно, Оператор в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки ПДн, обязан уничтожить такие ПДн или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении ПДн Оператор обязан уведомить субъекта ПДн или его представителя, а в случае, если обращение субъекта ПДн или его представителя либо запрос уполномоченного органа по защите прав субъектов ПДн были направлены уполномоченным органом по защите прав субъектов ПДн, также указанный орган.
- 8.2.14. В случае достижения цели обработки ПДн Оператор обязан прекратить обработку ПДн или обеспечить ее прекращение (если обработка ПДн осуществляется другим лицом, действующим по поручению Оператора) и уничтожить ПДн или обеспечить их уничтожение (если обработка ПДн осуществляется другим лицом, действующим по поручению Оператора) в срок, не превышающий тридцати дней с даты достижения цели обработки ПДн, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем, по которому является субъект ПДн,

иным соглашением между Оператором и субъектом ПДн либо если Оператор не вправе осуществлять обработку ПДн без согласия субъекта ПДн на основаниях, предусмотренных законодательством РФ.

8.2.15. В случае отзыва субъектом ПДн согласия на обработку его ПДн, прекратить их обработку или обеспечить прекращение такой обработки (если обработка ПДн осуществляется другим лицом, действующим по поручению Оператора) и в случае, если сохранение ПДн более не требуется для целей обработки ПДн, уничтожить ПДн или обеспечить их уничтожение (если обработка ПДн осуществляется другим лицом, действующим по поручению Оператора) в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, иным соглашением между оператором и субъектом ПДн либо если Оператор не вправе осуществлять обработку ПДн без согласия субъекта ПДн на основаниях, предусмотренных законодательством РФ.

8.2.16. Назначить лицо, ответственное за организацию обработки ПДн.

9. ПОРЯДОК ОБРАБОТКИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

9.1. Обеспечение конфиденциальности ПДн, обрабатываемых Оператором, является обязательным требованием для всех лиц, которым ПДн стали известны.

9.2. Сотрудники Оператора, осуществляющие оформление документов, обязаны получать в установленных случаях согласие субъектов ПДн на обработку.

9.3. В случае нарушения установленного порядка обработки ПДн сотрудники Оператора несут ответственность в соответствии с разделом 10 настоящего Положения.

9.4. ПДн субъектов на бумажных носителях, обрабатываемые Оператором, хранятся в отделах (на рабочих местах сотрудников), имеющих допуск к обработке соответствующих ПДн. Носители ПДн не должны оставаться без присмотра. При оставлении рабочего места, сотрудники, осуществляющие обработку ПДн должны, убирать носители в сейф, запираемый шкаф или иным образом ограничивать несанкционированный доступ к носителям. При утере или порче ПДн осуществляется по возможности их восстановление.

9.5. Места хранения документов, содержащих ПДн, и лица, ответственные за обеспечение защиты носителей ПДн, определяются соответствующим Приказом Руководителя Оператора об утверждении мест хранения материальных носителей персональных данных.

ПДн субъектов ПДн, обрабатываемых Оператором (договоры, акты, соглашения, анкеты, копии паспортов, иные подобные документы, содержащие ПДн субъектов ПДн, носители информации (флеш-карты, CD-диски, и т.п.), хранятся в соответствующих отделах (подразделениях) Оператора, осуществляющих обработку ПДн, в запираемых шкафах (сейфах) и в персональных компьютерах, оборудованных системой защиты от несанкционированного доступа.

9.6. При неавтоматизированной обработке различных категорий ПДн должен использоваться отдельный материальный носитель для каждой категории ПДн.

9.7. При неавтоматизированной обработке ПДн на бумажных носителях:

- не допускается фиксация на одном бумажном носителе ПДн, цели обработки которых заведомо несовместимы;
- ПДн должны обособляться от иной информации, в частности путем фиксации их на отдельных бумажных носителях, в специальных разделах или на полях форм (бланков).

9.8. Хранение ПДн должно осуществляться в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн.

9.9. Под уничтожением обработанных ПДн понимаются действия, в результате которых невозможно восстановить содержание ПДн в ИСПДн или в результате которых уничтожаются материальные носители ПДн.

9.10. Обрабатываемые ПДн подлежат уничтожению либо обезличиванию по достижении целей

обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено действующим законодательством.

9.11. Уничтожение обработанных ПДн производится комиссией по уничтожению документов с составлением соответствующего Акта об уничтожении.

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

9.13. Уточнение ПДн 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 ПДн.

9.14. Уничтожение носителей, содержащих ПДн, осуществляется в следующем порядке:

- ПДн на бумажных носителях уничтожаются путем использования shreddera (уничтожители документов), установленного в офисе Оператора.
- ПДн, размещенные в памяти персональных компьютеров уничтожаются путем удаления их из памяти персональных компьютеров.
- ПДн, размещенные на флеш-карте, CD-диске, ином носителе информации уничтожаются путем удаления файла с носителя, при необходимости путем нарушения работоспособности флеш-карты или CD-диска.

Уничтожение носителей ПДн производится комиссией по уничтожению документов с составлением соответствующего Акта об уничтожении.

9.15. Все помещения Оператора по окончании рабочего дня и отсутствия сотрудников, должны запираются, окна должны быть закрыты, должна быть включена сигнализация (при наличии).

9.16. Сетевое оборудование, серверы следует располагать в местах, недоступных для посторонних лиц (в специальных помещениях, шкафах, коробах).

9.17. Уборка помещений и обслуживание технических средств ИСПДн должна осуществляться под контролем ответственных за данные помещения и технические средства лиц с соблюдением мер, исключающих несанкционированный доступ к ПДн, носителям информации, программным и техническим средствам обработки, передачи и защиты информации ИСПДн.

9.18. Оператор должен осуществлять внутренний контроль процесса обработки ПДн в целях изучения и оценки фактического состояния защищенности ПДн, своевременного реагирования на нарушения установленного порядка их обработки, а также в целях совершенствования этого порядка и обеспечения его соблюдения.

9.19. Мероприятия по осуществлению внутреннего контроля обработки и обеспечения безопасности ПДн направлены на решение следующих задач:

обеспечение соблюдения сотрудниками Оператора требований настоящего Положения и нормативно-правовых актов, регулирующих сферу ПДн;

оценка компетентности персонала, задействованного в обработке ПДн,

обеспечение работоспособности и эффективности технических средств ИСПДн и средств защиты ПДн, их соответствия требованиям уполномоченных органов исполнительной власти по вопросам безопасности ПДн;

выявление нарушений установленного порядка обработки ПДн и своевременное предотвращение негативных последствий таких нарушений;

принятие корректирующих мер, направленных на устранение выявленных нарушений, как в порядке обработки ПДн, так и в работе технических средств ИСПДн;

разработка рекомендаций по совершенствованию порядка обработки и обеспечения безопасности ПДн по результатам контрольных мероприятий;

осуществление внутреннего контроля за исполнением рекомендаций и указаний по устранению нарушений.

9.20. Результаты мероприятий по внутреннему контролю оформляются актами и являются основанием для разработки рекомендаций по совершенствованию порядка обработки и обеспечения безопасности ПДн, по модернизации технических средств ИСПДн и средств защиты ПДн, по обучению и повышению компетентности сотрудников, допущенных к обработке ПДн.

10. СРОКИ ОБРАБОТКИ И ХРАНЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

10.1. Сроки обработки и хранения ПДн субъектов ПДн, обрабатываемых Оператором, определяются нормативными правовыми актами, регламентирующими порядок их сбора и обработки.

10.2. Срок хранения ПДн, внесенных в ИСПДн Оператора, должен соответствовать сроку хранения бумажных оригиналов.

11. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ НАСТОЯЩЕГО ПОЛОЖЕНИЯ

11.1. Руководитель Оператора несет ответственность за необеспечение конфиденциальности ПДн и несоблюдение прав и свобод субъектов ПДн в отношении их ПДн, в том числе прав на неприкосновенность частной жизни, личную и семейную тайну.

11.2. Сотрудники Оператора, допущенные к работе с персональными данными, несут персональную ответственность за несоблюдение требований по обработке и обеспечению безопасности ПДн, установленных настоящим Положением, в соответствии с законодательством Российской Федерации.

11.3. Сотрудник Оператора может быть привлечен к ответственности в случаях:
умышленного или неосторожного раскрытия ПДн;

утраты материальных носителей ПДн;

нарушения требований настоящего Положения и других нормативных документов Оператора в части вопросов доступа и работы с ПДн.

11.4. В случаях нарушения установленного порядка обработки и обеспечения безопасности ПДн, несанкционированного доступа к ПДн, раскрытия ПДн и нанесения Оператору, его сотрудникам, клиентам и контрагентам материального или иного ущерба виновные лица несут уголовную, гражданскую, административную, дисциплинарную и иную предусмотренную законодательством РФ ответственность.