ПРИЛОЖЕНИЕ № 6
к приказу директора
ООО МЦ «РевмаМед»
от ___.___.2021 №____

# ПОЛОЖЕНИЕ
# об обработке персональных данных

г. Сыктывкар
2021

**Оглавление**

## 1. Основные понятия и определения

Для целей настоящего Положения об обработке персональных данных (далее – Положение), обрабатываемых в ООО МЦ «РевмаМед» (далее − Общество) используются следующие основные понятия и определения:

1.1. **персональные данные (далее – ПДн)** − любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных);

1.2. **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;

1.3. **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;

1.4. **автоматизированная обработка персональных данных** – обработка персональных данных с помощью средств вычислительной техники;

1.5. **распространение персональных данных** − действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

1.6. **предоставление персональных данных** – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

1.7. **блокирование персональных данных** – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

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;

1.9. **обезличивание персональных данных** – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

1.10. **информационная система персональных данных (далее – ИСПДн)** – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

1.11. **конфиденциальность персональных данных** – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их раскрытия третьим лицам и распространения без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом;

1.12. **документированная информация** – зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель;

1.13. **средство защиты информации** – техническое, программное, программно-

техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации;

1.14. **субъект персональных данных** – физическое лицо, которое прямо или косвенно определено или определяемо с помощью персональных данных;

1.15. **информационные технологии** – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;

1.16. **контролируемая зона** – это пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание посетителей, а также транспортных, технических и иных материальных средств.

## 2. Общие положения

2.1. Настоящее Положение разработано в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», постановлением Правительства от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», постановлением Правительства от 15.09.2008 № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

2.2. Цели разработки Положения:

- определение принципов и порядка обработки ПДн субъектов ПДн в Обществе;
- обеспечение защиты прав и свобод субъектов ПДн Общества при обработке их ПДн, а также установление ответственности лиц, обрабатывающих ПДн, за невыполнение требований норм, регулирующих обработку и защиту ПДн.

2.3. Объем обрабатываемых ПДн, категории субъектов, ПДн которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований определяются Перечнем персональных данных, обрабатываемых в ООО МЦ «РевмаМед» (далее – Перечень), Перечнем информационных систем персональных данных и Политикой в отношении обработки персональных данных (далее – Политика).

2.4. В Обществе обрабатываются ПДн следующих категорий физических лиц (субъектов ПДн):

- работников (в т.ч. уволенных работников);
- близких родственников работников;
- соискателей на вакантные должности;
- клиентов (физических лиц, индивидуальных предпринимателей);
- контрагентов/поставщиков (индивидуальных предпринимателей, представителей юридических лиц);
- пациентов.

2.5. Общество обрабатывает следующие категории ПДн:

2.5.1. Работников (в т.ч. уволенных работников): фамилия, имя, отчество; место рождения; год, месяц и дата рождения; пол; адрес и дата регистрации; адрес места жительства; гражданство; контактные данные (номер телефона); паспортные данные (серия, номер, кем и когда выдан) или данные иного документа, удостоверяющего личность; сведения об идентификационном номере налогоплательщика; сведения о номере и серии страхового

свидетельства государственного пенсионного страхования; трудовой стаж (места работы, должности, период работы, причины увольнения); сведения о трудовой книжке (серия, номер, дата выдачи, записи в ней); справка с основного места работы; сведения о временной нетрудоспособности; должность; структурное подразделение; сведения о приеме на работу, перемещении по должностям, увольнении; сведения о повышении квалификации, переподготовке или аттестации (серия, номер, дата выдачи документа о повышении квалификации, переподготовке или аттестации, наименование и местоположение образовательного учреждения); сведения о трудовом договоре (содержание и реквизиты); сведения о командировках, отпусках; табельный номер; семейное положение; тарифная ставка (оклад); надбавка; данные о начисленных суммах (заработной платы, материальной помощи, премии и иных); тип и сумма налогового вычета; статус налогоплательщика; данные о суммах удержаний и перечислений из заработной платы работника согласно его заявлению или исполнительному листу; сведения о сумме выплат и иных вознаграждений и страховом стаже застрахованного лица; уровень образования; наименование образовательного учреждения; сведения о документах, подтверждающих образование (наименование, номер, дата выдачи); специальность; квалификация; ученая степень; ученое звание; номер и дата выдачи удостоверения о дополнительном образовании; сведения о воинском учете; медицинская книжка; сведения о нахождении в отпуске по беременности и родам, уходу за ребенком.

2.5.2. Близких родственников работников: фамилия, имя, отчество; год, месяц, дата рождения; степень родства; сведения из свидетельства о рождении.

2.5.3. Соискателей на вакантные должности: фамилия, имя, отчество; год, месяц и дата рождения; место рождения; гражданство; адрес места жительства; контактные данные (номер телефона); трудовой стаж (места работы, должности, период работы); семейное положение; уровень образования; сведения о дополнительном образовании (курсы, переподготовка, стажировка); наименование образовательного учреждения; специальность; квалификация.

2.5.4. Клиентов (физических лиц, индивидуальных предпринимателей): фамилия, имя, отчество; полное наименование индивидуального предпринимателя; место рождения; год, месяц и дата рождения; адрес и дата регистрации; юридический адрес; пол; гражданство; контактные данные (номер телефона, email); паспортные данные (серия, номер, кем и когда выдан) или данные иного документа, удостоверяющего личность.

2.5.5. Контрагентов/поставщиков (индивидуальных предпринимателей, представителей юридических лиц): фамилия, имя, отчество; полное наименование индивидуального предпринимателя; адрес и дата регистрации; юридический адрес; контактные данные (телефон, эл.почта); паспортные данные (серия, номер, кем и когда выдан) или данные иного документа, удостоверяющего личность; сведения об идентификационном номере налогоплательщика; номер расчетного (лицевого) счета.

2.5.6. Пациентов: фамилия, имя, отчество; место рождения; год, месяц и дата рождения; адрес места жительства; пол; гражданство; контактные данные (номер телефона); паспортные данные (серия, номер, кем и когда выдан) или данные иного документа, удостоверяющего личность; сведения о номере и серии страхового свидетельства государственного пенсионного страхования; сведения из полисов обязательного (добровольного) медицинского страхования (серия, номер, дата); сведения с места работы (должность); сведения о временной нетрудоспособности; семейное положение; состав семьи; сведения о социальном статусе; сведения о социальных льготах; уровень

образования; жалобы; история болезни; сведения из медицинской карты; состояние здоровья; результаты исследования/анализов; диагнозы.

2.6. Категории ПДн, которые субъект может сделать общедоступными, описывается Перечнем и определяется в Согласии на обработку персональных данных субъектов ПДн.

2.7. Порядок ввода в действие и изменения Положения:

2.7.1. Пересмотр пунктов настоящего Положения, Перечня и Политики производится ответственным (лицом, комиссией) за организацию обработки ПДн по мере необходимости (при изменении организационно-штатной структуры; при изменении законодательства Российской Федерации о персональных данных; при изменении условий и порядка обработки персональных данных субъектов персональных данных Общества и т.п.), но не реже 1 (одного) раза в год.

2.7.2. Настоящее Положение вступает в силу с момента его утверждения приказом директора Общества и действует бессрочно, до замены его новым Положением.

2.8. Контроль соблюдения требований настоящего Положения и контроль принятых организационных и технических мер осуществляет ответственный за организацию обработки ПДн, назначенный приказом директора Общества (в случае его отсутствия – иным лицом, уполномоченным от имени Общества).

2.9. Все работники Общества, имеющие доступ к ПДн, должны быть ознакомлены с настоящим Положением под роспись.

## 3. Правовое основание обработки персональных данных

3.1. Необходимость обработки ПДн с использованием средств автоматизации, а также без использования таких средств обусловлена сложившейся практикой обработки документов, содержащих ПДн и рядом нормативно-правовых актов Российской Федерации.

3.2. Обработка ПДн в Обществе осуществляется, руководствуясь следующими нормативно-правовыми актами:

- Конституция Российской Федерации;
- Трудовой кодекс Российской Федерации;
- Гражданский кодекс Российской Федерации;
- Налоговый кодекс Российской Федерации;
- Федеральный закон от 22.10.2004 № 125-ФЗ «Об архивном деле в Российской Федерации»;
- Федеральный закон от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности»;
- Федеральный закон от 07.02.1992 № 2300-1 «О защите прав потребителей»;
- Федеральный закон от 28.03.1998 № 53-ФЗ «О воинской обязанности и военной службе»;
- Федеральный закон от 01.04.1996 № 27-ФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования»;
- Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи»;
- Федеральный закон от 06.12.2011 № 402-ФЗ «О бухгалтерском учете»;
- Федеральный закон от 28.12.2013 № 426-ФЗ «О специальной оценке условий труда»;
- Федеральный закон от 15.12.2001 № 167-ФЗ «Об обязательном пенсионном страховании в Российской Федерации»;

– Федеральный закон от 29.11.2010 № 326-ФЗ «Об обязательном медицинском страховании в Российской Федерации»;

– Федеральный закон от 25.07.2002 № 115-ФЗ «О правовом положении иностранных граждан в Российской Федерации»;

– Федеральный закон 25.12.2008 № 273-ФЗ «О противодействии коррупции»;

– Федеральный закон от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;

– Постановление Правительства Российской Федерации от 16.04.2003 г. № 225 «О трудовых книжках»;

– Постановление Правительства Российской Федерации от 27.11.2006 № 719 «Об утверждении Положения о воинском учете»;

– Постановление Правительства Российской Федерации от 04.10.2012 № 1006 «Об утверждении Правил предоставления медицинскими организациями платных медицинских услуг»;

– Постановления Правительства Российской Федерации от 16.04.2012 № 219 «О лицензировании медицинской деятельности (за исключением указанной деятельности, осуществляемой медицинскими организациями и другими организациями, входящими в частную систему здравоохранения, на территории инновационного центра «Сколково») (вместе с «Положением о лицензировании медицинской деятельности (за исключением указанной деятельности, осуществляемой медицинскими организациями и другими организациями, входящими в частную систему здравоохранения, на территории инновационного центра «Сколково»);

– Постановление Государственного комитета по статистике от 05.01.2004 г. № 1 «Об утверждении унифицированных форм первичной учетной документации по учету труда и его оплаты»;

– Постановление Правления Пенсионного фонда Российской Федерации от 16.01.2014 № 2п «Об утверждении формы расчета по начисленным и уплаченным страховым взносам на обязательное пенсионное страхование в ПФР и на обязательное медицинское страхование в ФФОМС плательщикам страховых взносов, производящим выплаты и иные вознаграждения физическим лицам и порядка ее заполнения»;

– Приказ Минздрава России от 30.12.2014 № 956н «Об информации, необходимой для проведения независимой оценки качества оказания услуг медицинскими организациями, и требованиях к содержанию и форме предоставления информации о деятельности медицинских организаций, размещаемой на официальных сайтах министерства здравоохранения Российской Федерации, органов государственной власти, субъектов Российской Федерации, органов местного самоуправления и медицинских организаций в информационно-телекоммуникационной сети Интернет»;

– Приказ Минздравсоцразвития Российской Федерации от 25.01.2011 № 29н «Об утверждении Порядка ведения персонифицированного учета в сфере обязательного медицинского страхования»;

– Приказ Минздравсоцразвития Российской Федерации от 24.12.2012 № 1355н «О б утверждении формы типового договора на оказание и оплату медицинской помощи по обязательному медицинскому страхованию»;

– Приказ Минздрава Российской Федерации от 28.02.2019 № 108н «Об утверждении Правил обязательного медицинского страхования»;

– Письмо Минздрава Российской Федерации от 07.12.2015 № 13-2/1538 «О сроках хранения медицинской документации»;

– Приказ Минкультуры Российской Федерации от 25.08.2010 N 558 «Об утверждении Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения»;

– Устав ООО МЦ «РевмаМед»;

– Договоры, заключаемые между оператором и субъектом персональных данных;

– Согласия субъектов персональных данных на обработку персональных данных;

– Лицензия № ЛО-11-01-002102 от 24.10.2018 на осуществление медицинской деятельности;

– иные нормативные правовые акты Российской Федерации и Республики Коми.

## 4. Права и обязанности субъектов персональных данных

4.1. Права субъектов ПДн:

4.1.1. Субъект ПДн имеет право на получение информации, касающейся обработки его ПДн (за исключением случаев, предусмотренных ч. 8 ст. 14 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»), 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 работников 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 настоящим федеральным законом;

– 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 от 27.07.2006 № 152-ФЗ «О персональных данных» или другими федеральными законами.

4.1.2. Эти сведения должны быть предоставлены субъекту ПДн оператором 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.

4.1.3. Эти сведения предоставляются субъекту ПДн или его представителю оператором при обращении либо при получении запроса субъекта ПДн или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации. Запрос должен содержать:

– 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.

4.1.4. В случае, если указанные сведения, а также обрабатываемые ПДн были предоставлены для ознакомления субъекту ПДн по его запросу, субъект ПДн вправе обратиться повторно к оператору или направить ему повторный запрос в целях получения указанных сведений и ознакомления с ПДн не ранее чем через 30 (тридцать) дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого является субъект ПДн.

4.1.5. Субъект ПДн вправе обратиться повторно к оператору или направить ему повторный запрос в целях получения указанных сведений, а также в целях ознакомления с обрабатываемыми ПДн до истечения срока (30 (тридцати) дней) в случае, если такие сведения и (или) обрабатываемые ПДн не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос дополнительно должен содержать обоснование направления повторного запроса.

4.1.6. Оператор вправе отказать субъекту ПДн в выполнении повторного запроса, не соответствующего условиям, предусмотренным пунктами 4.1.4 и 4.1.5 настоящего Положения. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на операторе.

4.1.7. Субъект ПДн вправе требовать от Общества 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.

4.1.8. Запросы пользователей информационной системы на получение ПДн, а также факты предоставления ПДн по этим запросам регистрируются в Журнале учета обращений субъектов персональных данных о выполнении их законных прав при обработке персональных данных ООО МЦ «РевмаМед» (Приложение № 2 к настоящему Положению) (далее – Журнал). Данный Журнал ведется в подразделениях, где осуществляется сбор ПДн. Журнал хранится в течение 5 (пяти) лет с момента внесения последней записи, после чего уничтожается ответственным (лицом, комиссией) за организацию обработки ПДн.

4.1.9. Если субъект ПДн считает, что Общество осуществляет обработку его ПДн с нарушением требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» или иным образом нарушает его права и свободы, субъект ПДн вправе обжаловать действия или бездействие оператора в уполномоченный орган по защите прав субъектов ПДн или в судебном порядке.

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

4.2. Обязанности субъектов ПДн:

4.2.1. Субъект ПДн обязан предоставлять полную и достоверную информацию о своих ПДн.

4.2.2. В случае изменений сведений, содержащих ПДн субъект ПДн обязан в течение 3 (трех) рабочих дней сообщить Обществу об изменениях и дополнениях своих ПДн.

## 5. Права и обязанности работодателя и работников Общества, работающих с персональными данными

5.1. Работодатель (оператор) имеет право:

5.1.1. Отстаивать свои интересы в судебных органах;

5.1.2. Предоставлять ПДн субъектов третьим лицам, если это предусмотрено действующим законодательством Российской Федерации (правоохранительные, налоговые органы и др.), а также связано с исполнением договора, стороной которого либо выгодоприобретателем или поручителем, по которому является субъект ПДн;

5.1.3. Отказывать в предоставлении ПДн в случаях, предусмотренных законодательством Российской Федерации;

5.1.4. Использовать ПДн субъекта без его согласия в случаях, предусмотренных законодательством Российской Федерации.

5.2. Работники Общества, допущенные к ПДн, несут ответственность за точное выполнение требований, предъявляемых к ним в целях обеспечения сохранности указанных сведений. До получения доступа к работе, связанной с обработкой ПДн, им необходимо изучить настоящее Положение и дать письменное Обязательство о неразглашении персональных данных (конфиденциальной информации).

5.3. Работники Общества, допущенные к ПДн должны:

- не разглашать ПДн;
- о ставшей им известной утечке ПДн сообщать непосредственному руководителю и ответственному за организацию обработки ПДн Общества;
- знакомиться только с теми документами и выполнять только те работы, к которым они допущены;
- соблюдать правила пользования документами, содержащими ПДн;
- не допускать их необоснованной рассылки;
- выполнять требования режима, исключающие возможность ознакомления с ПДн посторонних лиц, включая и работников Общества, не имеющих к указанным документам прямого отношения;
- использовать информационные ресурсы Общества только для достижения целей деятельности Общества (не использовать в личных целях);
- при ведении деловых переговоров с представителями сторонних организаций или частными лицами ограничиваться выдачей минимальной информации, действительно необходимой для их успешного завершения.

5.4. Обязанности работодателя (оператора):

5.4.1. Операторы и иные лица, получившие доступ к ПДн, обязаны не раскрывать третьим лицам и не распространять ПДн без согласия субъекта ПДн, если иное не предусмотрено федеральным законом.

5.4.2. Оператор обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006 № 152-

ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами. Оператор самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» или другими федеральными законами. К таким мерам могут, в частности, относиться:

– назначение оператором, являющимся юридическим лицом, ответственного за организацию обработки ПДн;

– издание оператором, являющимся юридическим лицом, документов, определяющих политику оператора в отношении обработки ПДн, локальных актов по вопросам обработки ПДн, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;

– применение правовых, организационных и технических мер по обеспечению безопасности ПДн в соответствии со статьей 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;

– осуществление внутреннего контроля и (или) аудита соответствия обработки ПДн Федеральному закону от 27.07.2006 № 152-ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите ПДн, политике оператора в отношении обработки ПДн, локальным актам Общества;

– оценка вреда, который может быть причинен субъектам ПДн в случае нарушения Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;

– ознакомление работников Общества, непосредственно осуществляющих обработку ПДн, с положениями законодательства Российской Федерации о ПДн, в том числе требованиями к защите ПДн, документами, определяющими политику Общества в отношении обработки ПДн, локальными актами по вопросам обработки ПДн, и (или) обучение указанных работников.

5.4.3. Оператор обязан опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки ПДн, к сведениям о реализуемых требованиях к защите ПДн (а при сборе ПДн через интернет – также опубликовать документ в Интернет).

5.4.4. Оператор обязан предоставить документы и локальные акты, указанные в пункте 5.4, и (или) иным образом подтвердить принятие мер, указанных в пункте 5.4.2. по запросу уполномоченного органа по защите прав субъектов ПДн.

5.4.5. Оператор обязан предоставить работнику необходимые условия для выполнения требований по охране конфиденциальных сведений, к которым допускается работник.

5.5. Работник разрешает Обществу производить контроль использования им информационных ресурсов Общества, а также использования им технических средств обработки, хранения и передачи информации, предоставленных Обществом для выполнения работником договорных обязанностей.

5.6. Общество оставляет за собой право, но не принимает каких-либо обязательств контролировать использование работником информационных ресурсов, технических средств обработки, хранения и передачи информации, а также соблюдения мер по охране конфиденциальных сведений.

## 6. Порядок сбора, хранения, использования и передачи персональных данных

### 6.1. Сбор, обработка

6.1.1. Обработка ПДн допускается в следующих случаях:

– обработка ПДн осуществляется с согласия субъекта ПДн на обработку его ПДн;

– обработка ПДн необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения, возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;

– обработка ПДн необходима для исполнения договора, стороной которого является субъект ПДн, а также для заключения договора по инициативе субъекта ПДн;

– обработка ПДн необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта ПДн, если получение согласия субъекта ПДн невозможно;

– обработка ПДн необходима для осуществления прав и законных интересов оператора или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта ПДн;

– обработка ПДн необходима для осуществления профессиональной деятельности журналиста и (или) законной деятельности средства массовой информации либо научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и законные интересы субъекта ПДн;

– обработка ПДн осуществляется в статистических или иных исследовательских целях при условии обязательного обезличивания ПДн;

– осуществляется обработка ПДн, сделанных общедоступными субъектом ПДн;

– осуществляется обработка ПДн, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом;

– в иных случаях, описанных в ст. 6 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

6.1.2. Сбор ПДн осуществляется в соответствии с нормативно-правовыми актами Российской Федерации в области трудовых отношений, настоящим Положением и иными локальными правовыми актами Общества.

6.1.3. Все ПДн субъекта ПДн следует получать у него самого либо его законных представителей. Должностное лицо Общества должно сообщить субъекту ПДн Общества о целях, предполагаемых источниках и способах получения ПДн, куда могут передаваться ПДн и последствиях отказа дать письменное согласие на их получение и обработку.

6.1.4. Если получение ПДн является обязательным в соответствии с федеральным законом, оператор обязан разъяснить субъекту ПДн юридические последствия отказа предоставить его ПДн.

6.1.5. Если ПДн получены не от субъекта ПДн, оператор, за исключением случаев, предусмотренных пунктом 6.1.6 настоящего Положения, до начала обработки таких ПДн обязан предоставить субъекту ПДн следующую информацию:

– наименование либо фамилия, имя, отчество и адрес оператора или его

представителя;

– цель обработки ПДн и ее правовое основание;

– предполагаемые пользователи ПДн;

– установленные Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» права субъекта ПДн;

– источник получения ПДн.

6.1.6. Оператор освобождается от обязанности предоставить субъекту ПДн сведения, предусмотренные пунктом 6.1.5 настоящего Положения, в случаях если:

– субъект ПДн уведомлен об осуществлении обработки его ПДн соответствующим оператором;

– ПДн получены оператором на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем, по которому является субъект ПДн;

– ПДн сделаны общедоступными субъектом ПДн или получены из общедоступного источника;

– оператор осуществляет обработку ПДн для статистических или иных исследовательских целей, для осуществления профессиональной деятельности журналиста либо научной, литературной или иной творческой деятельности, если при этом не нарушаются права и законные интересы субъекта ПДн;

– предоставление субъекту ПДн сведений, предусмотренных пунктом 6.1.5 настоящего Положения, нарушает права и законные интересы третьих лиц.

6.1.7. Общество не обрабатывает ПДн субъекта о его расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях. В соответствии со ст. 24 Конституции Российской Федерации оператор вправе получать и обрабатывать данные о частной жизни субъекта только с его письменного согласия.

6.1.8. Работник, законный представитель предоставляет работнику Общества достоверные сведения о себе. Работник проверяет достоверность сведений, сверяя данные, предоставленные работником, с имеющимися документами.

6.1.9. Ввод ПДн в автоматизированные ИСПДн Общества осуществляется работником в соответствии с его должностными обязанностями.

6.1.10. Работники, осуществляющие ввод и обработку данных с использованием автоматизированных ИСПДн Общества, несут ответственность за полноту введенной информации и не должны вносить изменения, противоречащие информации, полученной непосредственно от субъекта ПДн.

**6.2. Согласие на обработку персональных данных**

6.2.1. В следующих случаях Общество получает от субъекта согласие на обработку его ПДн:

– поручение обработки ПДн другому лицу;

– раскрытие третьим лицам или распространение ПДн, если иное не предусмотрено федеральным законом;

– обработка ПДн в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи, а также в целях политической агитации;

– включение ПДн субъекта в общедоступные источники ПДн, в том числе публикация в средствах массовой информации и интернет (согласие в письменной форме);

– обработка специальных категорий ПДн, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни (согласие в письменной форме);

– обработка сведений, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические ПДн) и которые используются оператором для установления личности субъекта ПДн (согласие в письменной форме);

– трансграничная передача ПДн на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов ПДн (согласие в письменной форме);

– принятие решения на основании исключительно автоматизированной обработки ПДн субъекта, порождающее юридические последствия в отношении субъекта ПДн или иным образом затрагивающее его права и законные интересы (согласие в письменной форме).

6.2.2. Работник Общества, либо лицо, поступающее на работу в Общество, являясь субъектом ПДн, своей волей и в своем интересе принимает решение о предоставлении своих ПДн и дает письменное согласие на их обработку («Согласие на обработку персональных данных работника ООО МЦ «РевмаМед» (Приложение № 1а к настоящему Положению)). Согласие с работника берется с целью признания части его ПДн общедоступными.

6.2.3. Соискатель, являясь субъектом персональных данных, своей волей и в своем интересе принимает решение о предоставлении своих персональных данных и дает согласие на их обработку («Согласие на обработку персональных данных соискателей (Приложение № 1б к настоящему Положению))

6.2.4. Субъекты, ПДн которых Общество обрабатывает без заключения с ними договора, должны дать согласие на обработку их ПДн (Приложение № 1в к настоящему Положению)).

6.2.5. Субъект ПДн принимает решение о предоставлении его 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 федеральным законом. В случае получения согласия на обработку ПДн от представителя субъекта ПДн полномочия данного представителя на дачу согласия от имени субъекта ПДн проверяются оператором.

6.2.6. Согласие на обработку ПДн может быть отозвано субъектом ПДн. В случае отзыва субъектом ПДн согласия на обработку ПДн оператор вправе продолжить обработку ПДн без согласия субъекта ПДн при наличии оснований, указанных в пункте 6.1 и Федеральном законе от 27.07.2006 № 152-ФЗ «О персональных данных».

6.2.7. Отзыв согласия на обработку ПДн происходит по письменному заявлению субъекта ПДн на имя директора Общества с указанием причин отзыва. При подаче заявления необходимо предъявить основной документ, удостоверяющий личность. После отзыва согласия все ПДн, содержащиеся в ИСПДн с использованием средств автоматизации, в течение десяти дней уничтожаются без возможности восстановления, о чем уведомляется субъект ПДн, если иное не установлено законодательством Российской Федерации. Данные, находящиеся на бумажных носителях, передаются в архив и хранятся в течение сроков, установленных законодательством.

### 6.3. Передача персональных данных

6.3.1. Оператор вправе поручить обработку ПДн другому лицу с согласия субъекта ПДн, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, либо путем принятия государственным или муниципальным органом соответствующего акта (далее – поручение оператора). Лицо, осуществляющее обработку ПДн по поручению оператора, обязано соблюдать принципы и правила обработки ПДн, предусмотренные Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных». В поручении оператора должны быть определены перечень действий (операций) с ПДн, которые будут совершаться лицом, осуществляющим обработку ПДн, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность ПДн и обеспечивать безопасность ПДн при их обработке, а также должны быть указаны требования к защите обрабатываемых ПДн в соответствии со ст. 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

6.3.2. Лицо, осуществляющее обработку ПДн по поручению оператора, не обязано получать согласие субъекта ПДн на обработку его ПДн.

6.3.3. В случае, если оператор поручает обработку ПДн другому лицу, ответственность перед субъектом ПДн за действия указанного лица несет оператор. Лицо, осуществляющее обработку ПДн по поручению оператора, несет ответственность перед оператором.

6.3.4. При передаче ПДн субъекта Обществу необходимо соблюдать следующие требования:

- не сообщать ПДн субъекта третьей стороне без согласия субъекта, за исключением случаев, предусмотренных пунктом 6.1.1 настоящего Положения, а также в случаях, установленных федеральным законодательством;
- предупредить лиц, получивших ПДн субъекта, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц исполнения Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;
- разрешать доступ к ПДн только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те ПДн, которые необходимы для выполнения конкретной функции;
- передавать ПДн субъекта представителям субъектов в порядке, установленном Трудовым кодексом Российской Федерации, Семейным кодексом Российской Федерации, и ограничивать эту информацию только теми ПДн субъекта, которые необходимы для выполнения указанными представителями их функций.

6.3.5. В соответствии с законодательством Российской Федерации ПДн, обрабатываемые Обществом, могут быть переданы правоохранительным, судебным органам, органам социальной защиты и другим Обществам, которые имеют на это право на основании федерального законодательства, а также в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороноспособности страны и безопасности государства без получения согласия субъекта ПДн.

6.3.6. Решение о передаче информации, содержащей ПДн, обрабатываемые в Обществе, третьим лицам, за исключением указанного в пункте 6.3.5 настоящего Положения, принимается администрацией Общества только на основании мотивированного письменного запроса, если иное не предусмотрено договором или федеральным

законодательством. Мотивированный запрос должен быть подписан уполномоченным должностным лицом, содержать указание цели и правовое основание предоставления ПДн, срок предоставления этой информации, если иное не установлено федеральными законами.

6.3.7. Порядок передачи информации, содержащей ПДн, обрабатываемые Обществом, внутри Общества определяется должностными обязанностями работников и/или локальными нормативными актами Общества, в соответствии с законодательством Российской Федерации.

**6.4. Хранение и уничтожение**

6.4.1. ПДн могут храниться в бумажном и(или) электронном виде в бухгалтерии, у специалиста по кадрам и других подразделениях Общества с соблюдением предусмотренных нормативно-правовыми актами Российской Федерации и локальными нормативными актами мер по защите ПДн. Право на доступ к местам хранения ПДн предоставляется работникам структурных подразделений и(или) должностным лицам, определенным настоящим Положением, а также приказами о доступе к ПДн, распорядительными документами или письменными указаниями директора Общества.

6.4.2. Хранение ПДн в ИСПДн осуществляется на серверах и автоматизированных рабочих местах Общества с использованием специализированного программного обеспечения.

6.4.3. Хранение ПДн должно осуществляться в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен федеральным законом, договором, стороной которого является субъект ПДн.

6.4.4. Обрабатываемые ПДн подлежат уничтожению (либо обезличиванию) в следующих случаях:

- по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом;
- по требованию субъекта ПДн, его представителя или уполномоченного органа по защите прав субъектов ПДн, если ПДн являются неполными, устаревшими, неточными, незаконно полученными, неправомерно обрабатываемыми или не являются необходимыми для заявленной цели обработки;
- отзыв субъектом ПДн согласия на обработку его ПДн, если иное не предусмотрено договором, стороной которого 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 Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» или другими федеральными законами.

6.4.5. В случае достижения целей обработки ПДн, обработка ПДн прекращается и ПДн (или их материальные носители) подлежат уничтожению в срок, не превышающий 30 (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 Обществом и субъектом ПДн, либо если Общество не вправе осуществлять обработку ПДн без согласия субъекта ПДн на основаниях, предусмотренных законодательством Российской Федерации.

6.4.6. Уничтожение носителей ПДн производится ответственным после поступления от руководителей структурных подразделений, обрабатывающих ПДн, перечня подлежащих уничтожению носителей ПДн (в том числе в электронном виде) с указанием основания

для их уничтожения.
6.4.7. Уничтожение ПДн на машинных носителях информации производится после истечения сроков хранения ПДн ответственным с использованием специального программного обеспечения или средств гарантированного уничтожения информации.
6.4.8. Способ уничтожения носителей ПДн должен исключать возможность восстановления уничтоженных ПДн.
6.4.9. Уничтожению не подлежат ПДн, для которых законодательством Российской Федерации предусмотрены иные сроки хранения.
6.4.10. Уничтожению (стиранию) может подвергаться сама информация о субъекте ПДн, хранящаяся на носителе, а также сам носитель ПДн.
6.4.11. По всем фактам уничтожения ПДн или носителей ПДн составляется Акт об уничтожении персональных данных ООО МЦ «РевмаМед» (Приложение № 3 к настоящему Положению).
6.4.12. Перед непосредственным уничтожением носителей ПДн ответственным осуществляется сверка документов и дел с описью, приведенной в Акте об уничтожении персональных данных ООО МЦ «РевмаМед».
6.4.13. Бумажные носители ПДн уничтожаются в присутствии ответственного, принимавшего участие в сверке (проверке) документов (дел), подлежащих уничтожению.
6.4.14. Уничтожение документов производится путем сожжения, дробления, растворения или химического разложения, превращения в бесформенную массу или порошок. Выбор разрешенных конкретных способов для уничтожения ПДн и их носителей осуществляется ответственным.

**6.5. Общедоступные персональные данные**

6.5.1. В целях информационного обеспечения могут создаваться общедоступные источники ПДн (в том числе справочники, адресные книги). В общедоступные источники ПДн с письменного согласия субъекта ПДн могут включаться его фамилию, имя, отчество, наименование организации работодателя, структурное подразделение, должность, номер рабочего телефона, адрес рабочей электронной почты, сообщаемые субъектом ПДн.
6.5.2. Сведения о субъекте ПДн должны быть в любое время исключены из общедоступных источников ПДн по требованию субъекта ПДн либо по решению суда или иных уполномоченных государственных органов.

**6.6. Правила работы с обезличенными данными**

6.6.1. Обезличивание ПДн может быть проведено с целью ведения статистических наблюдений, снижения потенциального ущерба от разглашения ПДн и по достижению целей обработки ПДн или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено законодательством Российской Федерации.
6.6.2. При проведении работ по обезличиванию необходимо руководствоваться Правилами работы с обезличенными персональными данными ООО МЦ «РевмаМед» (Приложение № 5 к настоящему Положению)
6.6.3. Для обезличенных ПДн нет необходимости обеспечения их конфиденциальности.
6.6.4. Для того, чтобы распространять, предоставлять третьим лицам, публиковать, передавать по незащищенным каналам связи и т.п. обезличенные ПДн, необходимо (перед совершением этих действий) убедиться в правильности проведения процедуры обезличивания ПДн. Процедура обезличивания считается проведенной успешно, если по обезличенным ПДн становится невозможным без использования дополнительной информации определить принадлежность ПДн конкретному субъекту ПДн. При этом

необходимо обеспечить конфиденциальность той дополнительной информации, с помощью которой возможно определить принадлежность ПДн конкретному субъекту ПДн.

## 7. Правила рассмотрения запросов субъектов персональных данных и их представителей

**Таблица 1.** Взаимодействие с субъектом ПДн

| № п/п | Событие | Действие | Основания для отказа, исключения |
|---|---|---|---|
| 1. | Запрос субъекта ПДн на получение информации, касающейся обработки его ПДн | Предоставить субъекту ПДн информацию по форме Справки об обработке персональных данных субъекта ООО МЦ «РевмаМед» (Приложение № 5 к настоящему Положению) либо мотивированный отказ со ссылкой на п. 8 ст. 14 ФЗ от 27.07.2006 № 152-ФЗ «О персональных данных» в течение 30 (тридцати) дней со дня получения запроса | см. п. 8 ст. 14 ФЗ от 27.07.2006 № 152-ФЗ «О персональных данных» |
| 2. | Предоставление субъектом сведений, подтверждающих, что обрабатываемые ПДн являются неполными, неточными или неактуальными | Немедленно блокировать или обеспечить блокирование ПДн на период проверки. Внести необходимые изменения в ПДн в течение 7 (семи) рабочих дней со дня получения сведений. Уведомить субъекта ПДн о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым ПДн этого субъекта были переданы | см. п. 2 ст. 21 ФЗ от 27.07.2006 № 152-ФЗ «О персональных данных» |
| 3. | Предоставление субъектом сведений, подтверждающих, что обрабатываемые ПДн являются незаконно полученными или не являются необходимыми для заявленной цели обработки | В срок, не превышающий 7 (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 | см. п. 3 ст. 20 ФЗ от 27.07.2006 № 152-ФЗ «О персональных данных» |
| 4. | Запрос уполномоченного органа по защите прав субъектов ПДн | Ответить на запрос в течение 30 (тридцати) дней со дня получения запроса | см. п. 4 ст. 20 ФЗ от 27.07.2006 № 152-ФЗ «О персональных данных» |
| 5. | Обращение, запрос субъекта ПДн либо уполномоченного органа по защите прав | Прекратить неправомерную обработку ПДн или обеспечить прекращение неправомерной обработки ПДн лицом, действующим по поручению оператора в | см. п. 3 ст. 21 ФЗ от 27.07.2006 № 152-ФЗ «О |

| № п/п | Событие | Действие | Основания для отказа, исключения |
|---|---|---|---|
| | субъектов ПДн о выявлении неправомерной обработки ПДн | срок, не превышающий 3 (трех) рабочих дней с даты этого выявления. В случае, если обеспечить правомерность обработки ПДн невозможно, оператор в срок, не превышающий 10 (десяти) рабочих дней с даты выявления неправомерной обработки ПДн, обязан уничтожить такие ПДн или обеспечить их уничтожение с составлением Акта об уничтожении ПДн ООО МЦ «РевмаМед». Уведомить субъекта ПДн о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым ПДн этого субъекта были переданы | персональных данных» |
| 6. | Получение ПДн субъектов от третьих лиц | Уведомить субъекта об обработке его ПДн либо убедиться, что третье лицо (на основании заключенного договора с этим лицом о получении ПДн) получило согласие субъекта ПДн на передачу его ПДн | |

## 8. Доступ к персональным данным субъектов

8.1. Доступ работников Общества к ПДн осуществляется в соответствии со списками, которые утверждаются приказом директора Общества. Руководитель, разрешающий доступ работника своего подразделения к носителю ПДн, несет персональную ответственность за данное разрешение.

8.2. Ознакомление лиц с ПДн субъектов должно осуществляться только по необходимости и в тех объемах, которые необходимы для выполнения возложенных на них функций.

## 9. Обработка персональных данных, осуществляемой без использования средств автоматизации

9.1. Обработка ПДн, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории ПДн можно было определить места хранения ПДн (материальных носителей) и установить перечень лиц, осуществляющих обработку ПДн.

9.2. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность ПДн и исключающие несанкционированный к ним доступ. Лица, осуществляющие обработку ПДн без использования средств автоматизации, должны быть проинформированы о факте обработки ими ПДн, категориях, обрабатываемых ПДн, а также об особенностях и правилах осуществления такой обработки.

9.3. ПДн при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных

материальных носителях ПДн, в специальных разделах или на полях форм (бланков).
9.4. При фиксации ПДн на носителях не допускается фиксация на одном материальном носителе ПДн, цели обработки которых заведомо не совместимы. Для обработки различных категорий ПДн, осуществляемой без использования средств автоматизации, для каждой категории ПДн должен использоваться отдельный носитель.
9.5. Уничтожение или обезличивание части ПДн, если это допускается носителем, может производиться способом, исключающим дальнейшую обработку этих ПДн с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).
9.6. Уточнение ПДн при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на носителе, а если это не допускается техническими особенностями носителя, - путем фиксации на том же носителе сведений о вносимых в них изменениях либо путем изготовления нового носителя с уточненными ПДн.
9.7. Необходимо обеспечивать раздельное хранение ПДн (носителей), обработка которых осуществляется в различных целях.
9.8. При хранении носителей должны соблюдаться условия, обеспечивающие сохранность ПДн и исключающие несанкционированный к ним доступ.

## 10. Обеспечение безопасности персональных данных

10.1. Безопасность ПДн при их обработке в информационных системах 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 в информационной системе информационные технологии.
10.2. Размещение информационных систем, специальное оборудование и организация работы с ПДн должны обеспечивать сохранность носителей ПДн и средств защиты информации, а также исключать возможность неконтролируемого пребывания в этих помещениях посторонних лиц.
10.3. Лица, получившие доступ к ПДн, обязаны не допускать их распространения без согласия субъекта ПДн или наличия иного законного основания.
10.4. В случае, если Общество на основании договора поручает обработку ПДн другому лицу, существенным условием договора является обязанность обеспечения указанным лицом конфиденциальности ПДн и безопасности ПДн при их обработке.
10.5. Меры по обеспечению конфиденциальности ПДн, принимаемые в Обществе, должны включать, но не ограничиваясь этим, следующее:

- определение перечня ПДн и мест обработки таких данных;
- ограничение доступа к ПДн, их носителям, путем установления порядка обращения с этими данными и носителями, контроля за соблюдением такого порядка;
- учет лиц, получивших доступ к ПДн, и (или) лиц, которым такие данные были предоставлены или переданы;
- учет носителей (документов), содержащих ПДн.

10.5.1. Организационные меры безопасности:

- инструктаж работников по правилам обеспечения безопасности обрабатываемых ПДн;

– учет и хранение съемных носителей информации и порядок их обращения, исключающие хищение, подмену и уничтожение;

– мониторинг и реагирование на инциденты информационной безопасности, связанные с ПДн, включая проведение внутренних проверок, разбирательств и составление заключений;

– постоянный контроль за соблюдением требований по обеспечению безопасности ПДн (реализуется путем внутренних аудитов).

10.5.2. Меры физической безопасности:

– ограничение доступа пользователей в помещения, где размещены технические средства, позволяющие осуществлять обработку ПДн, а также хранятся носители информации. Приказом по Обществу устанавливается контролируемая зона Общества, вводятся в действие Список помещений с ограниченным доступом и Список лиц, имеющих право посещать помещения Общества с ограниченным доступом. Лица, не указанные в Списке, в том числе обеспечивающие техническое и бытовое обслуживание (уборку, ремонт оборудования и технических средств), при наличии необходимости могут посещать помещения с ограниченным доступом в сопровождении ответственных лиц;

– размещение технических средств, позволяющих осуществлять обработку ПДн, в пределах охраняемой территории;

– организация физической защиты помещений и собственно технических средств, позволяющих осуществлять обработку ПДн.

10.5.3. Технические меры безопасности:

– разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;

– регистрация действий пользователей и обслуживающего персонала, контроль доступа и действий пользователей, обслуживающего персонала и посторонних лиц;

– резервирование технических средств, дублирование массивов и носителей информации;

– использование защищенных каналов связи;

– предотвращение внедрения в информационные системы вредоносных программ (программ-вирусов) и программных закладок.

## 11. Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

11.1. Контроль выполнения работ по обеспечению безопасности ПДн (далее – Контроль) в Обществе осуществляется путем проведения периодических контрольных мероприятий (в рамках внутренних аудитов) и внутренних проверок по фактам произошедших инцидентов информационной безопасности.

11.2. В рамках проведения контрольных мероприятий в Обществе выполняются:

– проверка наличия и актуальности планов, регистрационных журналов, актов, договоров, отчетов, протоколов и других свидетельств выполнения мероприятий по обеспечению безопасности ПДн;

– проверка осведомленности и соблюдения персоналом требований к обеспечению безопасности ПДн;

– проверка соответствия перечня лиц, которым предоставлен доступ к ПДн, и их

полномочий по доступу к определенным категориям ПДн фактическому состоянию;

– проверка локальных актов, определяющих условия хранения материальных носителей, обеспечивающих сохранность ПДн и исключающих несанкционированный к ним доступ, перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер;

– проверка документов, определяющих места хранения ПДн, перечня лиц, осуществляющих обработку ПДн либо имеющих к ним доступ;

– проверка документов об информировании лиц, осуществляющих обработку ПДн, обработка которых осуществляется без использования средств автоматизации, категориях обрабатываемых ПДн, а также об особенностях и правилах осуществления такой обработки;

– проверка получения и передачи ПДн третьим лицам с согласия субъекта ПДн либо с последующим уведомлением субъекта о факте обработки его ПДн;

– проверка наличия и исправности функционирования технических средств защиты информации, используемых для обеспечения безопасности ПДн, в соответствии с требованиями эксплуатационной и технической документации;

– инструментальная проверка соответствия настроек технических средств защиты информации требованиям к обеспечению безопасности ПДн (при необходимости);

– проверка соответствия моделей угроз для информационных систем ПДн условиям функционирования данных систем;

– проверка соответствия организационно-распорядительной документации по обеспечению безопасности ПДн действующим требованиям законодательства Российской Федерации, руководящих документов ФСБ России, ФСТЭК России.

11.3. Все собранные в ходе проведения контрольных мероприятий в Обществе свидетельства и сделанные по их результатам заключения должны быть зафиксированы документально.

11.4. Контрольные мероприятия проводятся как периодически в соответствии с планом и программой аудита, так и внепланово по решению руководства Общества и в случае возникновения инцидентов информационной безопасности.

11.5. Внутренние проверки в Обществе в обязательном порядке проводятся в случае выявления следующих фактов:

– нарушение конфиденциальности, целостности, доступности ПДн;

– халатность и несоблюдение требований к обеспечению безопасности ПДн;

– несоблюдение условий хранения носителей ПДн;

– использование средств защиты информации, которые могут привести к нарушению заданного уровня безопасности (конфиденциальность/целостность/доступность) ПДн или другим нарушениям, приводящим к снижению уровня защищенности ПДн.

11.6. Задачами внутренней проверки являются:

– установление обстоятельств нарушения, в том числе времени, места и способа его совершения;

– установление лиц, непосредственно виновных в данном нарушении;

– выявление причин и условий, способствовавших нарушению.

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

Общество, а также должностные лица, виновные в нарушении норм, регулирующих получение, обработку и защиту ПДн, несут дисциплинарную, гражданскую, административную, уголовную и иную ответственность, предусмотренную законодательством Российской Федерации.