Администрации ЗАТО город Заозерск

Политика
в отношении обработки и защиты персональных данных

<u>Приложения к Политике</u> не подлежат опубликованию в открытых источниках информации в связи с наличием конфиденциальной информации защищаемой Оператором в соответствии с законодательством Российской Федерации.

Город Заозерск, 2018

АДМИНИСТРАЦИЯ
ЗАКРЫТОГО АДМИНИСТРАТИВНО-ТЕРРИТОРИАЛЬНОГО ОБРАЗОВАНИЯ
ГОРОД ЗАОЗЕРСК МУРМАНСКОЙ ОБЛАСТИ
(АДМИНИСТРАЦИЯ ЗАТО ГОРОД ЗАОЗЕРСК)

П О С Т А Н О В Л Е Н И Е

30 мая 2018 года № 303

Об утверждении «Политики
в отношении обработки и защиты персональных данных
в Администрации ЗАТО город Заозерск»

В соответствии с требованиями нормативно-правовых актов Российской Федерации: Конституцией Российской Федерации ст.2,17,18,19 п.2, 23,24; Трудовым кодексом Российской Федерации с.2,11,21,22,57, гл.14, ст. 86-90; Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» в редакции от 01.07.2017 и 29.07.2017 ст.1-3, 4-7,ст.9 п.4; Федеральным законом от 08.06.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изменениями и дополнениями вступившими в силу с 01.10.2017) ст.3 п.7, ст.7 п.4-6,ст.8-9 ст.10 п.2, ст.10.1; постановлением Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»; Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 01.11.2012 № 1119 п.1-17; приказом ФСБ России от 10 июля 2014 № 378 «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»; положением об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденным постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» ст.7 п. а – г; нормативными и методическими документами и рекомендациями по технической защите информации ФСТЭК России и ФСБ России по Северо-Западному

Федеральному округу; рекомендациями Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 31 июля 2017 г. "Рекомендации по составлению документа, определяющего политику оператора в отношении обработки персональных данных, в порядке, установленном Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных»; методическими рекомендациями 8 Центра ФСБ России от 31 марта 2015 года № 149/7/2/6-432 по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности

постановляю:

1. Утвердить прилагаемую «Политику в отношении обработки и защиты персональных данных в Администрации ЗАТО город Заозерск» (далее – Политика) и приложения к ней.

2. Назначить ответственным за исполнение требований Политики и организацию обработки и защиты персональных данных в Администрации ЗАТО город Заозерск, утвержденной пунктом 1 настоящего постановления - Главного инженера-программиста - Начальника отдела информационно-программного обеспечения МКУ «МФЦ ЗАТО город Заозерск» Павлова А.В..

3. Определить оператором ИСПДн организующим и осуществляющим обработку персональных данных, а также определяющим цели и содержание обработки персональных данных, как собственника используемых для обработки содержащихся ПДн в базах данных технических средств, общесистемного, прикладного, специального программного обеспечения, а также средств защиты информации, СКЗИ и ЭП правомерно используемых такими базами данных (в том числе и обрабатываемых ПДн, содержащиеся в базах данных) Администрацию ЗАТО город Заозерск.

3.1. Обязанности оператора информационных систем ПДн в установленном порядке **возложить на:**

-структурные подразделения и Управления Администрации ЗАТО город Заозерск, в которых формируются информационные системы и подсистемы и обрабатываются ПДн сотрудников Администрации ЗАТО город Заозерск и других граждан Российской Федерации, в соответствии с Политикой и приложениями к ней, утвержденными пунктом 1 настоящего постановления.

-структурные подразделения МКУ «МФЦ ЗАТО город Заозерск», действующие в интересах служебной деятельности Администрации ЗАТО город Заозерск в которых обрабатываются ПДн сотрудников Администрации ЗАТО город Заозерск и других граждан Российской Федерации, в соответствии с Политикой и приложениями к ней, утвержденными пунктом 1 настоящего постановления.

4. Ответственному за организацию обработки и защиты персональных данных в Администрации ЗАТО город Заозерск (Павлов А.В.):

В своей деятельности руководствоваться требованиями Политики и приложениями к ней, инструкцией ответственного сотрудника за организацию обработки и защиты персональных данных в информационных системах персональных данных Администрации ЗАТО город Заозерск, утвержденными пунктом 1 настоящего постановления.

5. Ответственному за организацию обработки и защиты персональных данных в Администрации ЗАТО город Заозерск (Павлов А.В.) систематически проводить инструктажи и занятия с муниципальными служащими, служащими, замещающими должности, не отнесенные к должностям муниципальной службы структурных подразделений и управлений Администрации ЗАТО город Заозерск, сотрудниками МКУ «МФЦ ЗАТО город Заозерск», действующими в интересах служебной деятельности Администрации ЗАТО город Заозерск и допущенными к обработке персональных данных, по нормативным правовым актам Российской Федерации, правительства Российской Федерации, правительства Мурманской области, регуляторами Российской Федерации (ФСТЭК России и ФСБ России), Администрации ЗАТО города Заозерска касающихся обработки и защиты персональных данных, с записью в Журнале инструктажа, в соответствии с Политикой и приложениями к ней, утвержденными пунктом 1 настоящего Постановления.

6. Постановление Администрации ЗАТО города Заозерска от 31.12.2015 № 910 «О муниципальных информационных системах муниципального образования ЗАТО город Заозерск – информационных системах персональных данных Администрации ЗАТО города Заозерска и Муниципального казенного учреждения «Информационный Центр»» признать утратившим силу.

7. Контроль за исполнением настоящего постановления оставляю за собой.

8. Настоящее постановление вступает в силу с момента подписания.

И.о. Главы администрации
ЗАТО город Заозерск В.М. Урошлев

Утверждено постановлением Администрации
ЗАТО город Заозерск
от **30.05.2018** № **303**

ПОЛИТИКА
Администрации ЗАТО город Заозерск в отношении обработки и защиты персональных данных

1. Общие положения

1.1. Настоящий документ определяет политику Администрации ЗАТО город Заозерск (далее - АДМ, Оператор) в отношении обработки и защиты персональных данных (далее - Политика), в соответствии с п.п. 2 ч. 1 ст. 18.1. Федерального закона от 27.07.2006 № 152-ФЗ "О персональных данных" и является основополагающим внутренним регулятивным документом Оператора, определяющим ключевые направления его деятельности в области обработки и защиты персональных данных.

1.2. Действие настоящей Политики распространяется на персональные данные (далее - ПНд) сотрудников Оператора, граждан РФ, персональные данные которых обрабатываются в информационных системах ПНд Администрации ЗАТО город Заозерск (далее - Субъект(ы) ПНд).

Администрация ЗАТО город Заозерск являясь Оператором, осуществляющим обработку персональных данных, обеспечивает защиту прав и свобод субъектов персональных данных при обработке их персональных данных, в том числе защиту прав на неприкосновенность частной жизни, личную и семейную тайну и принимает меры для обеспечения выполнения обязанностей Оператора, предусмотренных Федеральным законом от 27 июля 2006 года № 152-ФЗ "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами РФ.

Настоящий документ является общедоступным и подлежит размещению на официальном сайте органов местного самоуправления ЗАТО город Заозерск (далее – ОМСУ).

Локальные нормативные акты и другие документы, регламентирующие обработку персональных данных в Администрации ЗАТО город Заозерск, разрабатываются с учетом положений данной Политики.

Согласно положениям части 1 статьи 18 № 152-ФЗ от 27.07.2006 «О персональных данных», посвященным обязанностям оператора при сборе персональных данных, а также в соответствии с разъяснениями Минкомсвязи России от 12 августа 2015 года о применении положений ФЗ № 242 от 21 июля 2014 года под сбором персональных данных понимается целенаправленный процесс получения персональных данных Оператором непосредственно от Субъекта персональных данных, либо через специально привлеченных для этого третьих лиц. В связи с чем, **локализации подлежат** только те персональные данные, которые были получены Оператором на законных основаниях и в результате осуществляемой им целенаправленной деятельности по организации сбора таких данных, а не в результате случайного (не запрошенного) попадания к нему этих персональных данных.

Случайное, ненамеренное получение, хранение и иные операции с персональными данными российских граждан не влекут обязанности локализовать обработку персональных данных в Администрации ЗАТО город Заозерск, в связи с чем, Администрация ЗАТО город Заозерск **не должна предпринимать** каких-либо действий в отношении персональных данных, случайно к ней попавших.

В частности локализация не требуется в случае:

-незапрашиваемого получения персональных данных, например, с произвольной (случайной) входящей письменной корреспонденцией и с входящими электронными письмами;

-получения персональных данных поступивших к Оператору от других юридических лиц, если такие данные представляют собой контактную информацию сотрудников или представителей таких юридических лиц, переданную в ходе осуществления ими своей законной деятельности.

1.3. Настоящая Политика является обязательным для исполнения всеми работниками Администрации ЗАТО город Заозерск, работающими по трудовому договору, заключенному с Администрацией ЗАТО город Заозерск, которые непосредственно осуществляют обработку или имеют доступ к персональным данным Субъектов, а также лицами, осуществляющими обработку или имеющими доступ к персональным данным Субъектов на основании заключенных с Администрацией ЗАТО город Заозерск договоров, соглашений или на иных законных основаниях в порядке и на условиях, предусмотренных настоящей Политикой (далее - Сотрудники).

1.4. При сборе персональных данных Оператор обеспечивает запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, предусмотренных действующим российским законодательством.

1.5. При обработке персональных данных Оператор применяет правовые, организационные и технические меры по обеспечению безопасности персональных данных в соответствии со ст. 19 Федерального закона от 27.07.2006 № 152-ФЗ "О персональных данных".

1.6. Правовые основания обработки персональных данных:

Правовым основанием обработки персональных данных является совокупность правовых актов, во исполнение которых и в соответствии с которыми оператор осуществляет обработку персональных данных.

1.6.1. Обработка персональных данных представляет собой:

Совокупность правовых актов, во исполнение которых и в соответствии с которыми Оператор осуществляет обработку и защиту персональных данных:

1.6.2. Обработка персональных данных осуществляется в соответствии действующим законодательством РФ:

-Конституцией Российской Федерации ст.2,17,18,19 п.2, 23,24;

-Трудовым кодексом Российской Федерации с.2,11,21,22,57, гл.14, ст. 86-90;

-Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» в редакции от 01.07.2017 и 29.07.2017 ст.1-3, 4-7,ст.9 п.4;

-Федеральным законом от 08.06.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изменениями и дополнениями вступившими в силу с 01.10.2017) ст.3 п.7, ст.7 п.4-6,ст.8-9 ст.10 п.2, ст.10.1;

-постановлением Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;

-Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 01.11.2012 № 1119 п.1-17;

-приказом ФСБ России от 10 июля 2014 № 378 «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

-положением об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденным постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» ст.7 п. а-г;

-нормативными и методическими документами и рекомендациями по технической защите информации ФСТЭК России и ФСБ России.
- рекомендациями Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 31 июля 2017 г. "Рекомендации по составлению документа, определяющего политику оператора в отношении обработки персональных данных, в порядке, установленном Федеральным законом от 27 июля 2006 года № 152-ФЗ "О персональных данных".
-методическими рекомендациями 8 Центра ФСБ России от 31 марта 2015 года № 149/7/2/6-432 по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности

При определении правовых оснований обработки ПДн, **должны определяться основания** для обработки ПДн, изложенные в федеральных законах, законах Мурманской области, а также нормативных правовых актов Российской Федерации, Мурманской области, иных документов, которые требуют обработки ПДн или иных документов, являющихся такими основаниями.
Обработка ПДн без документально определенного и оформленного правового основания обработки ПДн **не допускается.**

1.7. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, **в том числе содержащей:**
-подтверждение факта обработки персональных данных Оператором;
-правовые основания и цели обработки персональных данных;
-цели и применяемые Оператором способы обработки персональных данных;
-наименование и место нахождения Оператора, сведения о лицах (за исключением работников Оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Оператором или на основании федерального закона;
-обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
-сроки обработки персональных данных, в том числе сроки их хранения;
-порядок осуществления субъектом персональных данных прав, предусмотренных федеральным законом;
-информацию об осуществленной или о предполагаемой трансграничной передаче данных;
-наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Оператора, если обработка поручена или будет поручена такому лицу;
-иные сведения, предусмотренные Федеральным законом "О персональных данных" или другими федеральными законами.
-субъект персональных данных вправе требовать от Оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

1.8. Оператор персональных данных имеет право:
-отстаивать свои интересы в суде;
-предоставлять персональные данные субъектов третьим лицам, если это предусмотрено действующим законодательством (налоговые, правоохранительные органы и др.);
-отказывать в предоставлении персональных данных в случаях, предусмотренных законодательством РФ;
-использовать персональные данные субъекта без его согласия в случаях, предусмотренных законодательством РФ.

1.9. При сборе персональных данных **Оператор обязан** предоставить субъекту персональных данных **по его просьбе** информацию, предусмотренную частью 7 статьи 14 Федерального закона "О персональных данных".

1.10. При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети "Интернет", оператор обязан обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, указанных в пунктах 2, 3, 4, 8 части 1 статьи 6 Федерального закона "О персональных данных".

1.11. Настоящая Политика вступает в силу с момента его утверждения Оператором и действует бессрочно до момента отмены действия, либо замены новым Политиками.
Все изменения в Политику вносятся постановлениями Администрации ЗАТО город Заозерск.

2. Основные понятия, используемые в Политике.

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

- **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;

- **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.

- **автоматизированная обработка персональных данных** - обработка персональных данных с помощью средств вычислительной техники;

- **распространение персональных данных** - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

- **предоставление персональных данных** - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

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

- **уничтожение персональных данных** - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

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

- **информационная система персональных данных** - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

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

- **информационная система персональных данных** - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

- **информация** - сведения (сообщения, данные) независимо от формы их представления.

- **использование персональных данных** - действия (операции) с персональными данными, совершаемые должностным лицом Оператора в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении Субъектов персональных данных либо иным образом затрагивающих их права и свободы или права и свободы других лиц;

- **конфиденциальность персональных данных** - обязательное для соблюдения сотрудником, получившим доступ к персональным данным, требования не допускать их распространения без согласия Субъекта персональных данных или иного на то законного основания.

3. Принципы, условия, цели и категории обрабатываемых персональных данных.

Содержание и объем обрабатываемых персональных данных **должны соответствовать** заявленным целям обработки. Обрабатываемые персональные данные **не должны** быть избыточными по отношению к заявленным целям их обработки.

При осуществлении хранения персональных данных Оператор персональных данных **обязан использовать базы данных**, находящиеся на территории Российской Федерации, в соответствии с ч. 5 ст. 18 Федерального закона "О персональных данных".

3.1. Принципы обработки персональных данных в Российской Федерации, Мурманской области, осуществляемые на основе принципов:

- Соблюдения законности и на справедливой основе.
- Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей.
-**Не допускается** обработка персональных данных, несовместимая с целями сбора персональных данных.
-Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.
-Обработке подлежат только персональные данные, которые отвечают целям их обработки.
-Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.
-При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.
-Хранение ПДн должно осуществляться в форме, позволяющей определить субъект ПДн, не больше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен федеральным законом или иным нормативно-правовым актом. Обрабатываемые ПДн подлежат

уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законодательством.
-Операторы и иные лица, получившие доступ к персональным данным, **обязаны не раскрывать третьим лицам и не распространять** персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

3.2. Цели и условия обработки персональных данных.

Целью обработки ПНд в Администрации ЗАТО город Заозерск является обеспечение 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.
-Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей.
-Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.
-Обработка персональных данных должна осуществляться с соблюдением принципов и правил, предусмотренных действующим Федеральным законодательством РФ.

Общие цели обработки персональных данных:
-обеспечение соблюдения законов Российской Федерации, Мурманской области и иных нормативных правовых актов Российской Федерации, Мурманской области, органов местного самоуправления ЗАТО город Заозерск в области обработки и защиты ПДн;
-учет сотрудников в Администрации ЗАТО город Заозерск;
-соблюдение порядка и правил приема сотрудников на работу в Администрацию ЗАТО город Заозерск;
-использование в уставной деятельности с применением средств автоматизации или без таких средств, включая хранение этих данных в архивах и размещение в информационно-телекоммуникационных сетях с целью предоставления доступа к ним;
-заполнение базы данных автоматизированной информационной системы в целях повышения эффективности и быстрого поиска, проведение мониторинговых исследований, формирование статистических и аналитических отчетов в вышестоящие органы;
-обеспечение личной безопасности сотрудников Администрации ЗАТО город Заозерск;
-предоставление муниципальных услуг в соответствии с Федеральным законом от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг».
-обеспечением защиты прав и свобод Субъектов персональных данных при обработке их персональных данных;
-анализ правовых актов, регламентирующих деятельность оператора, целей фактически осуществляемой оператором деятельности, а также деятельности, которая предусмотрена учредительными документами оператора, и конкретных бизнес-процессов оператора в конкретных информационных системах персональных данных (по структурным подразделениям оператора и их процедурам в отношении определенных категорий субъектов персональных данных).
-определением порядка обработки персональных данных Субъектов персональных данных;
-установлением режима конфиденциальности персональных данных, а также установление ответственности должностных лиц, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

Обработка персональных данных должна осуществляться с соблюдением принципов и правил, предусмотренных действующим Федеральным законодательством РФ.

Цели обработки ПДн в Администрации ЗАТО город Заозерск четко определены и соответствуют:

-заявленным в Уставе ЗАТО город Заозерск, в Соглашениях об информационно-программном обслуживании, заключенных между Администрацией ЗАТО город Заозерск (в том числе – управлениями Администрации ЗАТО город Заозерск) и МКУ «МФЦ ЗАТО город Заозерск», положениях о структурных подразделениях и Управлениях Администрации ЗАТО город Заозерск, их основным полномочиям и правам;

-задачам и функциям структурных подразделений и Управлений Администрации ЗАТО город Заозерск, задачам и функциям должностных лиц Администрации ЗАТО город Заозерск, указанным в соответствующих постановлениях, положениях, регламентах, должностных инструкциях.

Цели обработки ПДн определяют:

-содержание и объем обрабатываемых ПДн;

-категории субъектов ПДн;

-сроки их обработки и хранения;

-порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований.

Обработка ПДн в Администрации ЗАТО город Заозерск осуществляется в порядке:

-после получения согласия субъекта персональных данных, составленного по форме согласно приложению к настоящей Политике или сформированного в информационной системе персональных данных, за исключением случаев, предусмотренных частью 2 статьи 6 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;

- после направления уведомления об обработке персональных данных в Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Мурманской области, за исключением случаев, предусмотренных частью 2 статьи 22 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

-для исполнения переданных полномочий (в том числе государственных), организации кадровой работы, финансовой деятельности в соответствии с действующим Уставом ЗАТО город Заозерск, положениями и регламентами.

3.3. Основные условия проведения обработки ПДн:

-обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;

-обработка персональных данных необходима для достижения целей, осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;

-обработка персональных данных осуществляется в связи с участием лица в конституционном, гражданском, административном, уголовном судопроизводстве, судопроизводстве в арбитражных судах; (п. 3 в ред. Федерального закона РФ от 29.07.2017 № 223-ФЗ);

-обработка персональных данных необходима для исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве (далее - исполнение судебного акта); (Федеральный закон РФ от 29.07.2017 № 223-ФЗ);

-обработка персональных данных необходима для исполнения полномочий органов местного самоуправления и функций организаций, участвующих в предоставлении соответственно государственных и муниципальных услуг, предусмотренных Федеральным законом от 27 июля 2010 года № 210-ФЗ "Об организации предоставления государственных и муниципальных услуг", включая регистрацию субъекта персональных данных на едином портале государственных и муниципальных услуг и (или) региональных порталах государственных и муниципальных услуг; (в ред. Федерального закона РФ от 05.04.2013 № 43-ФЗ);

-обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных

данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем; (в ред. Федеральных законов от 21.12.2013 № 363-ФЗ, от 03.07.2016 № 231-ФЗ);

-обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

-обработка персональных данных необходима для осуществления прав и законных интересов оператора или третьих лиц, в том числе в случаях, предусмотренных Федеральным законом "О защите прав и законных интересов физических лиц при осуществлении деятельности по возврату просроченной задолженности и о внесении изменений в Федеральный закон "О микрофинансовой деятельности и микрофинансовых организациях", либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных; (в ред. Федерального закона от 03.07.2016 № 231-ФЗ);

-обработка персональных данных необходима для осуществления профессиональной деятельности и законной деятельности средства массовой информации либо научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и законные интересы субъекта персональных данных;

-обработка персональных данных осуществляется в статистических или иных исследовательских целях, за исключением целей, указанных в статье 15 152 - ФЗ "О персональных данных", **при условии обязательного обезличивания персональных данных**;

-осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе (далее - персональные данные, сделанные общедоступными субъектом персональных данных);

-осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

Особенности обработки **специальных категорий персональных данных**, а также биометрических персональных данных устанавливаются соответственно статьями 10 и 11 152 - ФЗ "О персональных данных".

Использование и хранение биометрических персональных данных вне информационных систем персональных данных, могут осуществляться **только** на таких материальных носителях информации и с применением такой технологии ее хранения, которые обеспечивают защиту этих данных от неправомерного или случайного доступа к ним, их уничтожения, изменения, блокирования, копирования, предоставления, распространения.

Оператор вправе поручить обработку персональных данных другому лицу **только с согласия субъекта персональных данных**, 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 персональных данных по поручению оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные настоящим Федеральным законом. В поручении оператора должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии со статьей 19 152 - ФЗ "О персональных данных". Лицо, осуществляющее обработку персональных данных по поручению оператора, не обязано получать согласие субъекта персональных данных на обработку его персональных данных.

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.

Оператор вправе передавать персональные данные **органам дознания и следствия**, иным уполномоченным органам на основании, предусмотренным действующим законодательством Российской Федерации.

3.4. К категориям субъектов персональных данных <u>могут быть отнесены:</u>

- граждане РФ, в интересах которых производиться обработка ПНд;
- сотрудники Оператора, бывшие сотрудники, кандидаты на замещение вакантных должностей, а также родственники сотрудников;
- клиенты и контрагенты оператора (физические лица);
- **представители (сотрудники**) клиентов и контрагентов Оператора (юридические лица).

Перечни категорий персональных данных, обрабатываемых Оператором, по каждой категории субъектов персональных данных, приведены на сайте Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций в Реестре операторов, осуществляющих обработку персональных данных, за регистрационным номером **10-0098395.**

3.5. Состав персональных данных.

В состав персональных данных Субъектов ПНд, которые обрабатывает Оператор, входят <u>следующие персональные данные:</u>

- Фамилия, имя, отчество.
- Дата рождения.
- Место рождения.
- Паспортные данные:
• вид документа;
• серия и номер документа;
• орган, выдавший документ (наименование, код подразделения);
• дата выдачи документа;
-Информация о гражданстве (в том числе и информация о предыдущих гражданствах).
-Адрес регистрации места жительства.
-Адрес фактического места жительства.
-Персональный идентификационный номер (СНИЛС).
-Пол.
-Номер контактного ГАТС телефона или мобильного телефона.
-Сведения об образовании, в том числе о послевузовском профессиональном образовании (наименование и год окончания образовательного учреждения, наименование и реквизиты документа об образовании, квалификация, специальность по документу об образовании).
-Сведения о трудовой деятельности, в том числе о прохождении муниципальной службы: дата, основания поступления на муниципальную службу и назначения на должность муниципальной службы, дата, основания назначения, перевода, перемещения на иную должность муниципальной службы, наименование замещаемых должностей муниципальной службы с указанием структурных подразделений, размера денежного содержания, результатов аттестации на соответствие замещаемой должности муниципальной службы, а также сведения о прежнем месте работы. Данные кадровых распорядительных документов о приеме, переводах, увольнении.
-Идентификационный номер налогоплательщика.
-Реквизиты страхового медицинского полиса обязательного медицинского страхования.
-Реквизиты свидетельства государственной регистрации актов гражданского состояния.
-Адрес электронной почты.
-Фотография.
-Сведения об участии в выборных представительных органах.

-Информация, содержащаяся в трудовом договоре, служебном контракте, дополнительных соглашениях к трудовому договору, служебному контракту.
-Информация об оформленных допусках к государственной тайне.
-Государственные награды, иные награды и знаки отличия.
-Информация о наличии или отсутствии судимости.
-Сведения о доходах, об имуществе и обязательствах имущественного характера.
-Номер расчетного счета.
-Номер банковской карты.
-Заработная плата, ее размер, начисления, отчисления во внебюджетные фонды, налоги, вычеты.
-Должности, ф.и.о. и платежные реквизиты контрагентов;
-Иные сведения, указанные заявителем.
-Семейное положение, состав семьи и сведения о близких родственниках (в том числе бывших).
- **Сведения о близких родственниках:**
• Фамилия, имя, отчество;
• Дата рождения;
• Место рождения;
• Адрес регистрации места жительства;
• Место работы и должность;
• Контактные данные.
- Сведения о трудовой деятельности;
- Сведения об образовании;
- Сведения об уровне доходов;
- Адрес электронной почты;
- Номер контактного ГАТС телефона или мобильного телефона;
-Информация о гражданстве (в том числе и информация о предыдущих гражданствах);
- Пол;
- Адрес фактического места жительства;

А также персональные данные, содержащиеся в:
-письменном заявлении гражданина с просьбой о поступлении на работу;
-собственноручно заполненной и подписанной гражданином Российской Федерации анкеты;
-документах о прохождении конкурса на замещение вакантной должности муниципальной службы (если гражданин назначен на должность по результатам конкурса);
-копии распоряжений и приказов Администрации ЗАТО город Заозерск, Управления ЭР,ЖКХ и МИ Администрации ЗАТО город Заозерск, Управления образования, культуры, спорта и молодежной политике Администрации ЗАТО город Заозерск;
-заявлении работника о приеме на работу;
-копии распоряжений и приказов Администрации ЗАТО город Заозерск, Управления ЭР,ЖКХ и МИ Администрации ЗАТО город Заозерск, Управления образования, культуры, спорта и молодежной политике Администрации ЗАТО город Заозерск о переводе работника на иную должность, о временном замещении им иной должности;
-должности, ф.и.о. и платежные реквизиты контрагентов;
-в авансах подотчетному лицу;
-сведениях о банковских и казначейских счетах;
-сведениях о бюджетных финансированиях организаций;
-средствах обязательного медицинского страхования;
-сведениях о расчетах с поставщиками и расчетах по принятым обязательствам;
-сведениях о расчетах по выполненным услугам;
-сведения об обмене с казначейскими системами;
-сведения содержащиеся в платежных документах;

4. Сведения об Операторе и требования к действиям Оператора муниципальной информационной системы ПДн.

Оператором муниципальной информационной системы ПДн (далее – МИС ПДн), организующим и осуществляющим обработку персональных данных, а также определяющим цели и содержание обработки персональных данных этих подсистем ИСПДн, как собственник используемых для обработки содержащихся в базах данных ПДн технических средств, общесистемного, прикладного, специального программного обеспечения, а также средств защиты информации, которое правомерно пользуется такими базами данных (в том числе обрабатывает ПДн, содержащиеся в базах данных) **является:**

- **Администрация ЗАТО город Заозерск** – подсистем МИС ПДн, указанных в приложении к настоящей Политике «Перечень подсистем информационных систем персональных данных Администрации ЗАТО город Заозерск». Обязанности операторов МИС ПДн в установленном порядке возлагаются на сотрудников структурных подразделений и управлений Администрации ЗАТО город Заозерск, в которых формируются подсистемы МИС ПДн;

Требования к действиям Оператора:

-**Оператор ПДн при обработке персональных данных обязан** принимать необходимые организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним посторонних лиц, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

-Для разработки и осуществления мероприятий по обеспечению безопасности персональных данных при их обработке в МИС ПДн, оператором **назначается должностное лицо**, **ответственное за обеспечение безопасности персональных данных**.

-**Перечень должностей** муниципальных служащих, служащих, замещающих должности, не отнесенные к должностям муниципальной службы структурных подразделений и управлений Администрации ЗАТО города Заозерска, допущенных к обработке персональных данных, **в соответствии с матрицей ролей доступа,** указан в приложении к настоящей Политике.

-**Муниципальные служащие**, служащие, замещающие должности, не отнесенные к должностям муниципальной службы структурных подразделений и управлений Администрации ЗАТО город Заозерск, допущенные к обработке персональных данных, сотрудники МКУ «МФЦ ЗАТО город Заозерск», допущенные к обработке персональных данных и действующие в интересах обеспечения служебной деятельности Администрации ЗАТО город Заозерск, **обязаны знать требования** действующего законодательства Российской Федерации, Мурманской области, нормативных правовых актов Российской Федерации, Мурманской области, нормативно-правовых актов администрации ЗАТО города Заозерска в области обработки персональных данных (в том числе с требованиями к защите персональных данных), а также настоящей Политики и **должны быть ознакомлены** с этими документами под личную подпись (приложение к Политике) и подписывают обязательство о неразглашении информации, содержащей ПДн, по форме согласно приложению к настоящей Политике. Должностные инструкции муниципальных служащих, служащих, замещающих должности, не отнесенные к должностям муниципальной службы структурных подразделений и управлений Администрации ЗАТО город Заозерск, допущенных к обработке ПДн, должны содержать сведения о допуске к ПДн и основания, на которых данный допуск осуществлен.

-**Оператором и третьими лицами**, получающими доступ к ПДн, должна обеспечиваться конфиденциальность таких данных. Оператор (или иное, получившее доступ к ПДн лицо) **обязан не допускать** их распространение без согласия субъекта ПДн или наличия иного законного основания, в соответствии с требованиями федерального законодательства РФ.

-**В случае если оператор** на основании договора (муниципального контракта) поручает другому лицу (организации) произвести работы по модификации, производству обновлений и усовершенствований базы ПДн данных и произвести регламентные работы с базой данных или произвести обработку этих ПДн, **существенным условием договора** (муниципального

контракта) должна **является** обязанность обеспечения указанным лицом (организацией) конфиденциальности ПДн и безопасности сведений из базы ПДн, при её обработке.

Базы ПДн целиком (или частичные сведения из БД) передаются другому лицу по акту, в зашифрованном виде, на зарегистрированном в соответствии с требованиями приказа ФАПСИ от 13 июня 2001 г. № 152 - флэш-накопителе или CD&DVD диске (Приложение 6 к настоящей Политике). Ключ для дешифрования передается другому лицу по акту (приложение к настоящей Политике).

- **Оператор обязан установить перечень** контролируемых зон на своей территории, в которых производиться обработка ПНд, хранятся СКЗИ и определить пути эвакуации сотрудников, средств обработки ПНд и СКЗИ в случае возникновения чрезвычайных ситуаций природного или техногенного характера. (приложение к настоящей Политике).

5. Способы и правила обработки ПДн Оператором.

В Администрации ЗАТО город Заозерск **применяются следующие способы обработки ПДн:**

- обработка ПДн без использования средств автоматизации, в том числе и на бумажных носителях;
- обработка ПДн с использованием средств автоматизации;
- смешанная обработка;
- обработка только на бумажных носителях.

5.1. Правила обработки и защиты ПДн в МИС ПДн без использования средств автоматизации.

5.1.1. Обработка ПДн без использования средств автоматизации может осуществляться в виде документов на бумажных носителях и в электронном виде (файлы базы данных) на зарегистрированных электронных машинных носителях информации различного типа (далее – МНИ).

5.1.2. Обработка ПДн, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории ПДн были:

- определены места хранения ПДн (материальных носителей информации) и установлен перечень лиц, осуществляющих обработку ПДн либо имеющих к ним доступ;
- обеспечено раздельное хранение ПДн (материальных носителей информации), обработка которых осуществляется в различных целях;
- соблюдены условия, обеспечивающие сохранность ПДн и исключающие несанкционированный к ним доступ.

5.1.3. При обработке различных категорий ПДн без использования средств автоматизации должен использоваться отдельный материальный носитель для каждой категории персональных данных.

5.1.4. При обработке ПДн, осуществляемой без использования средств автоматизации, на **бумажных носителях**:

- не допускается фиксация на одном бумажном носителе ПДн, цели обработки которых заведомо не совместимы;
- ПДн должны отделяться от иной информации, в частности путем фиксации их на отдельных бумажных носителях, в специальных разделах или на полях форм (бланков);
- документы, содержащие ПДн, формируются в дела в зависимости от цели обработки персональных данных;
- дела с документами, содержащими ПДн, должны иметь внутренние описи документов с указанием цели обработки и категории персональных данных.

5.1.5. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них ПДн (далее - типовые формы), должны соблюдаться следующие условия:

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

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

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

4) типовая форма должна исключать объединение полей, предназначенных для внесения ПДн, цели обработки которых заведомо не совместимы.

5.1.6. Обработка ПДн, осуществляемая без использования средств автоматизации в электронном виде осуществляется на внешних электронных машинных носителях информации.

При отсутствии технологической возможности осуществления обработки ПДн, осуществляемой без использования средств автоматизации, в электронном виде на внешних машинных носителях информации необходимо принимать организационные (охрана помещений) и технические меры (установка сертифицированных средств защиты информации), исключающие возможность несанкционированного доступа к ПДн лиц, не допущенных к их обработке.

При использовании в работе **внешних электронных машинных носителей информации** содержащих ПДн, к ним предъявляются следующие **требования:**

-электронные носители информации, содержащие ПДн, учитываются в «Журнале учета съемных машинных носителей информации содержащих персональные данные» (далее – МНИ или МН) ПДн, составленном по форме согласно приложению к настоящей Политике;

-к каждому электронному носителю **должна оформляться опись файлов**, содержащихся на нем, с указанием цели обработки и категории ПДн;

-при фиксации ПДн на материальных носителях не допускается фиксация и сохранность 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 материальный носитель.

4. При несовместимости целей обработки ПДн, осуществляемой без использования средств автоматизации, зафиксированных на одном электронном носителе, если электронный носитель не позволяет осуществлять обработку ПДн отдельно от других зафиксированных на том же носителе ПДн, должны быть приняты меры по обеспечению раздельной обработки ПДн, **в частности:**

- при необходимости использования или распространения определенных ПДн отдельно от находящихся на том же материальном носителе других ПДн осуществляется копирование ПДн, подлежащих распространению или использованию, способом, исключающим одновременное копирование ПДн, не подлежащих распространению и использованию, и используется (распространяется) копия ПДн;
- при необходимости уничтожения или блокирования части ПДн уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование ПДн, подлежащих уничтожению или блокированию;
- уничтожение или обезличивание части ПДн, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих ПДн с сохранением возможности обработки иных данных, зафиксированных на материальном носителе.

5.1.7. 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 возможностями и особенностями МНИ - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях, либо путем изготовления нового раздела на материальном носителе с уточненными ПДн.

Все документы и внешние электронные носители информации, содержащие ПДн, должны храниться в служебных помещениях в надежно запираемых и опечатываемых шкафах (сейфах), или в помещениях с ограниченным доступом. При этом должны быть созданы надлежащие условия, обеспечивающие их сохранность.

5.1.8. Перечень ПДн, обрабатываемых без использования средств автоматизации.

На основании требований Федерального закона от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации», в структурных подразделениях и управлениях Администрации ЗАТО город Заозерск обрабатываются ПДн граждан (ФИО, адрес, паспортные данные), представленные гражданами в следующих документах и через формы:

- обращения и жалобы граждан через специальную форму на официальном сайте ОМСУ ЗАТО город Заозерск;
- карточки по личному приему граждан;
- ответы по обращениям граждан.

5.2. Правила обработки и защиты ПДн в МИС ПДн с использованием средств автоматизации.

5.2.1. Обработка ПДн с использованием средств автоматизации **допускается в следующих случаях:**

- обработка ПДн осуществляется **только с согласия субъекта ПДн** на обработку его ПДн;
- обработка ПДн необходима для достижения целей, предусмотренных законом, для осуществления и выполнения возложенных на Администрацию ЗАТО город Заозерск как Оператора функций, полномочий и обязанностей;
- обработка ПДн необходима для исполнения договора или муниципального контракта, стороной которого является субъект ПДн, а также для заключения договора или муниципального контракта по инициативе субъекта ПДн;
- обработка ПДн необходима для предоставления муниципальных услуг гражданам РФ и организациям;
- обработка ПДн необходима для осуществления прав и законных интересов сотрудников Администрации ЗАТО город Заозерск или третьих лиц, либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта ПДн;
- обработка ПДн осуществляется в статистических или иных исследовательских целях при условии обязательного обезличивания ПДн;
- осуществляется обработка ПДн, доступ неограниченного круга лиц, к которым предоставлен субъектом ПДн либо по его просьбе (ПДн, сделанные общедоступными субъектом ПДн);
- осуществляется обработка ПДн, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

5.2.2. Обработка ПДн средствами автоматизации должна осуществляться на основании правил, инструкций, руководств, регламентов и иных документов, определяющих технологический процесс обработки информации, содержащей такие данные, определенных для выполнения конкретных операций с заранее определенными целями, с учетом требований настоящего Положения.

5.2.3. Не допускается обработка ПДн в МИС ПДн с использованием средств автоматизации **при отсутствии:**

- утвержденных организационно-технических документов о порядке эксплуатации информационных систем ПДн, включающих акт классификации информационных систем ПДн, инструкции пользователя и других нормативных и методических документов;
- настроенных средств защиты от несанкционированного доступа, средств антивирусной защиты, резервного копирования информации и других программных и технических средств, в соответствии с требованиями безопасности информации и технической защиты информации;
- охраны и организации режима допуска в помещения, предназначенные для обработки ПДн.

5.3. Правила обработки ПДн с согласия субъекта ПДн.

5.3.1. Оператор перед обработкой ПДн **обязательно получает** у субъектов ПДн **письменное согласие на обработку ПДн** (Приложение 1 к Политике).

5.3.2. Согласие на обработку ПДн может быть дано субъектом ПДн или его представителем **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 действующим законодательством электронной подписью.

5.3.3. Получение согласия субъекта ПДн в форме электронного документа на обработку его ПДн в целях предоставления муниципальных услуг, осуществляется в порядке, установленном законодательством Российской Федерации.

5.3.4. В случае получения согласия на обработку ПДн **от представителя субъекта ПДн** полномочия данного представителя на дачу согласия от имени субъекта ПДн **обязательно проверяются оператором.**

5.3.5. Допускается включение согласия в типовые формы (бланки) материальных носителей ПДн и в договор с субъектом ПДн.

5.3.6. Согласие на обработку ПДн может быть отозвано субъектом ПДн путем направления соответствующего запроса в Администрацию ЗАТО город Заозерск.

5.4. Правила обработки ПДн без согласия субъекта ПДн.

Обработка ПДн **без получения согласия** на такую обработку от субъекта ПДн, может осуществляться при наличии оснований, предусмотренных пунктами 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27.07.2006 № 152 - ФЗ «О персональных данных».

5.5. Правила обработки ПДн при поручении обработки ПДн другому лицу.

Администрация ЗАТО город Заозерск как оператор ИСПДн, вправе поручить обработку ПДн другому лицу (поручение оператора):

- **только с согласия субъекта ПДн**, если иное не предусмотрено федеральными законами РФ;
- на основании заключаемого с этим лицом договора, в том числе муниципального контракта;
- путем принятия соответствующего нормативного акта.

Лицо, осуществляющее обработку ПДн по поручению оператора, **обязано** соблюдать принципы и правила обработки ПДн.

В случае если Администрация ЗАТО город Заозерск поручает обработку ПДн другому лицу, **ответственность перед субъектом ПДн** за действия указанного лица несет только Администрация ЗАТО город Заозерск, как Оператор ПНд.

В случае необходимости получения согласия на обработку ПДн от субъекта ПДн обязанность получения такого согласия возлагается на Администрацию ЗАТО город Заозерск как Оператор ПНд.

5.6. Правила обработки ПДн <u>в зависимости от категории обрабатываемых ПДн.</u>

В Администрации ЗАТО город Заозерск устанавливаются следующие особые правила обработки ПДн **в зависимости от категории обрабатываемых ПДн:**

- обработка специальных категорий ПДн в Администрации ЗАТО город Заозерск не производиться, **за исключением указанным в пункте 5.6.1;**
- обработка общедоступных ПДн.

5.6.1. Правила обработки специальных категорий ПДн:

К специальным категориям ПДн **<u>относятся сведения, касающиеся:</u>**

- расовой принадлежности субъекта ПНд;
- национальной принадлежности субъекта ПНд;
- политических взглядов субъекта ПНд;
- религиозных убеждений субъекта ПНд;
- философских убеждений субъекта ПНд;
- состояния здоровья субъекта ПНд;
- интимной жизни субъекта ПНд;
- судимости субъекта ПНд.

В Администрации ЗАТО город Заозерск **разрешается обработка специальных категорий ПДн <u>при обязательном соблюдении любого из следующих условий:</u>**

- субъект ПДн **<u>обязательно должен дать согласие в письменной форме</u>** на обработку своих специальных ПДн;
- обработка ПДн осуществляется в соответствии с законодательством Российской Федерации;
- обработка ПДн необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта ПДн либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия субъекта ПДн невозможно;
- обработка ПДн необходима для установления или осуществления прав субъекта ПДн или третьих лиц;
- в соответствии с законодательством о государственной социальной помощи, трудовым законодательством, пенсионным законодательством Российской Федерации.
- обработка ПДн о судимости осуществляется в пределах полномочий, предоставленных Администрации ЗАТО город Заозерск в соответствии с законодательством Российской Федерации.

5.6.2. Правила обработки общедоступных ПДн:

Общедоступные ПДн физических лиц, полученные от физических лиц, или из сторонних общедоступных источников ПДн, обрабатываются в сроки, не превышающие необходимые для исполнения их обработки, в соответствии с требованиями законодательства РФ. При этом совместно с такими данными должны собираться реквизиты их источника и подтверждение согласия субъекта ПДн на включение такой информации в общедоступные источники ПДн, так как в случае обработки общедоступных ПДн обязанность доказывания того, что обрабатываемые ПДн являются общедоступными, возлагается на Администрацию ЗАТО город Заозерск. По достижении целей обработки общедоступных ПДн, **<u>они подлежат немедленному уничтожению.</u>**

С целью информационного обеспечения и осуществления взаимодействия со сторонними физическими и юридическими лицами в Администрации ЗАТО город Заозерск могут создаваться общедоступные источники ПДн. Создание общедоступного источника ПДн осуществляется по решению Главы администрации ЗАТО город Заозерск. В решении о создании общедоступного источника ПДн **должны быть указаны:**

- цель создания общедоступного источника ПДн;

- ссылка на нормативный акт, устанавливающий необходимость создания общедоступного источника ПДн (при наличии);
- перечень ПДн, которые вносятся в общедоступный источник ПДн;
- порядок включения ПДн в общедоступный источник ПДн;
- порядок уведомления пользователей общедоступного источника ПДн;
- порядок получения письменного согласия субъекта ПДн на включение ПДн в общедоступный источник ПДн.

В общедоступный источник ПДн с письменного согласия субъекта ПДн могут включаться: должность, фамилия, имя, отчество, абонентский номер рабочего телефона, место получения образования, достигнутые результаты и другая информация.

Включение в общедоступные источники ПДн субъекта ПДн допускается только **на основании его письменного согласия**.

Исключение ПДн из указанного общедоступного источника осуществляется при утрате необходимости в обработке таких данных, либо на основании заявления субъекта ПДн в соответствии с действующим законодательством Российской Федерации.

6. Актуализация, исправление, удаление и уничтожение персональных данных, ответы на запросы субъектов ПНд на доступ к персональным данным.

6.1. Оператор обязан сообщить в порядке, предусмотренном статьей 14 Федерального закона "О персональных данных", субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя либо в течение тридцати дней с даты получения запроса субъекта персональных данных или его представителя.

6.2. Оператор обязан предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных. В срок, не превышающий **семи рабочих дней** со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, оператор обязан внести в них необходимые изменения. В срок, не превышающий **семи рабочих дней** со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, оператор обязан уничтожить такие персональные данные. Оператор **обязан уведомить субъекта** персональных данных или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

6.3. В случае подтверждения факта неточности персональных данных Оператор на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязан уточнить персональные данные либо обеспечить их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

6.4. Оператор обязан прекратить обработку персональных данных или обеспечить прекращение обработки персональных данных лицом, действующим по поручению Оператора:

-в случае выявления неправомерной обработки персональных данных, осуществляемой Оператором или лицом, действующим по поручению Оператора, в срок, не превышающий трех рабочих дней с даты этого выявления;

-в случае отзыва субъектом персональных данных согласия на обработку его персональных данных Оператором;

-в случае достижения цели обработки персональных данных и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных.

В случае отсутствия возможности уничтожения персональных данных в течение указанного срока Оператор осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

7. Ответственность за организацию обработки персональных данных.

7.1. В соответствии с требованиями ст. 22.1 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» распоряжением Оператора назначается лицо, ответственное за организацию обработки и защиты персональных данных в муниципальных информационных системах ПНд Оператора и действует в соответствии с инструкцией (приложение к Политике).

7.2. Ответственный за организацию обработки и защиты персональных данных получает указания непосредственно от Главы администрации ЗАТО город Заозерск и **подотчетно только ему.**

7.3. В соответствии с ч. 4 ст. 22.1 Федерального закона «О персональных данных» **Ответственный за организацию обработки и защиты персональных данных обязан:**

-осуществлять внутренний контроль и аудит за соблюдением Оператором и его сотрудниками законодательства РФ о персональных данных;

-осуществлять внутренний контроль и аудит за соблюдением Оператором и его сотрудниками числе требований к защите персональных данных;

-доводить до сведения сотрудников Оператора положения законодательства РФ (изменения в законодательстве) о персональных данных, локальных актов Оператора по вопросам обработки персональных данных и требований к защите персональных данных;

-осуществлять контроль за приемом и обработкой обращений и запросов Субъектов ПНд или их представителей.

- осуществлять организацию обработки персональных данных по организации и выполнения законодательных требований при обработке персональных данных в МИС ПНд Оператора.

7.4. На время отсутствия Ответственного за организацию обработки персональных данных его обязанности исполняет сотрудник, замещающий его по штатному расписанию.

7.5. Ответственными за организацию выполнения требований локальных актов Оператора по вопросам обработки персональных данных и их защите в структурных подразделениях Оператора являются руководители этих подразделений. На время отсутствия этих руководителей ответственными являются лица, штатно замещающие их.

7.6. Ответственными за выполнение требований локальных актов Оператора по вопросам обработки персональных данных и их защите на своих рабочих местах в рамках определенных соответствующими должностными инструкциями и полномочиями, являются лица, уполномоченные в установленном порядке обрабатывать персональные данные.

8. Организация защиты персональных данных в муниципальных информационных системах ПНд.

8.1. Общее описание информационных систем персональных данных, эксплуатируемых Оператором при обработке и защите ПНд.

8.1.1. Для обеспечения безопасности персональных данных, обрабатываемых в информационных системах Оператора, применяются организационные, технические, программные методы и средства защиты информации.

-разработка и организация мероприятий по защите персональных данных у Оператора осуществляется ведущим специалистом по информационной безопасности, начальником организационно-правового отдела, юристами организационно-правового отдела.

8.1.2. В целях обеспечения безопасности обрабатываемых персональных данных:

-разработаны положения, инструкции и иные локальные акты по направлениям, связанным с обработкой и защитой персональных данных;

-определяются состав и объем организационных мероприятий по защите персональных данных в соответствии с требованиями законодательства РФ;

-определяется состав технических средств защиты информации для системы защиты персональных данных;

-осуществляется сопровождение и контроль внедрения и эксплуатации средств защиты информации в информационных системах Оператора;

-осуществляется контроль за соблюдением норм и требований законодательства РФ по внутренним проверкам организации обработки и защиты персональных данных у Оператора;

-осуществляется программный контроль входов-выходов любого из сотрудников Оператора, непосредственно осуществляющих обработку персональных данных;

-осуществляется регулярное резервное копирование баз данных МИС ПНд, что позволяет восстановить копию базы данных МИС ПНд на конец предыдущего дня;

-осуществляется регулярное резервное копирование операционных систем серверов МИС ПНд, что позволяет восстановить копию операционной системы МИС ПНд.

8.2. Описание муниципальных информационных систем персональных данных, которые эксплуатируются оператором при осуществлении обработки персональных данных и определение уровня их защищенности в соответствии с постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119.

8.2.1. Описание МИС ПДн Администрации ЗАТО город Заозерск – «1С: Предприятие в конфигурации «Бухгалтерия государственного учреждения», версии 1.0».

8.2.1.1. Основание создания и рамещения:

-Постановление администрации ЗАТО город Заозерск от 25.05.2015 № 387 «Об утверждении Положения о муниципальных информационных системах муниципального образования ЗАТО город Заозерск».

-Размещено в «Реестре муниципальных информационных систем муниципального образования ЗАТО город Заозерск».

8.2.1.2. Назначение:

-**МИС ПДн «1С: Предприятие» в конфигурации «Бухгалтерия государственного учреждения», версии 1.0** поддерживает единый, методически выверенный, взаимосвязанный технологический процесс ведения учета, который предусматривает получение всех необходимых первичных документов и регистров учета и **предназначена для:**

-Учета санкционирования расходов.

-Учета операций доведения бюджетных данных и кассового исполнения.

-Учета наличных денежных средств и денежных документов.

-Учета нефинансовых активов.
-Учета расчетов с поставщиками и подрядчиками.
-Учета расчетов по заработной плате, стипендиям и денежному довольствию
-Учета расчетов с подотчетными лицами.
-Учета расчетов с покупателями и заказчиками.
-Учета НДС.
-Налогового учета налога на прибыль по приносящей доход деятельности в соответствии с гл. 25 НК РФ.
-Формирования отчетности.
-Бюджетной и бухгалтерской отчетность.
-Налоговой отчетности.
-Интеграции с ГИС ГМП и региональными системами.
-Интеграции с АСУФД.

8.2.1.3. Цель создания:

Обеспечение единого методически выверенного, взаимосвязанного технологического процесса ведения бухгалтерского учета, который предусматривает получение всех необходимых первичных документов и регистров учета.

8.2.1.4. Характеристики ИСПНд:

-Группа ИСПДн (иные ПНд, согласно п.5 постановления Правительства РФ от 01.11.2012 № 1119);
-Категория ИСПДн (категория 2, в соответствии с требованиями постановления Правительства РФ от 01.11.2012 № 1119);
-Тип угроз, актуальных для МИС (угрозы 3 типа, в соответствии с требованиями постановления Правительства РФ от 01.11.2012 № 1119);
-Уровень защищенности – 4, в соответствии с требованиями постановления Правительства РФ от 01.11.2012 № 1119;
-Уровень значимости информации УЗ-3, в соответствии с требованиями Федерального закона от 27.07.2006 № 149-ФЗ и приказа ФСТЭК России от 11.02.2013 № 17;
-Режим обработки ПДн (многопользовательский);
-Класс защищенности К3, в соответствии с требованиями Федерального закона от 27.07.2006 № 149-ФЗ и приказа ФСТЭК России от 11.02.2013 № 17;
-Разграничение прав доступа (с разграничением);
-Масштаб МИС (менее чем 1000 субъектов);
-Класс защищенности МИС

8.2.1.5. Структура системы:

-Технологическая платформа 1С Предприятие, версии 8.3;
-Конфигурация «Бухгалтерия государственного учреждения», версии 1.0
-База данных «Бухгалтерия государственного учреждения», версии 1.0
-Система автоматического резервирования каталогов и базы данных «Бухгалтерия государственного учреждения», версии 1.0 на основе программы EFFECTOR SAVER 3.3.1 с открытым исходным кодом.
-Система ручного резервирования каталогов и базы данных «Бухгалтерия государственного учреждения», версии 1.0 на основе программы «Бухгалтерия государственного учреждения», версии 1.0.

8.2.1.6. Объем и содержание персональных данных, обрабатываемых в конфигурации «Бухгалтерия государственного учреждения», версии 1.0.

-Объем базы данных: **500 МБ.**
-Формат хранения базы данных: **.dt**

Содержание персональных данных в базе данных:

-Паспортные данные;
-Должности и ф.и.о. руководителей организаций;
-Должности, ф.и.о. и платежные реквизиты контрагентов;

-Авансы подотчетному лицу;
-Сведения о банковских и казначейских счетах;
-Сведения о бюджетных финансированиях организаций;
-Средства обязательного медицинского страхования;
-Сведения о расчетах с поставщиками и расчетах по принятым обязательствам;
-Сведения о расчетах по выполненным услугам;
-Сведения об обмене с казначейскими системами;
-Сведения, содержащиеся в платежных документах;

8.2.1.7. Реализация системы:

-Работа в системе реализована в виде обработки файлов стандартных офисных приложений MS Office, OpenOffice;
-Работа в системе реализована в виде обработки файлов стандартных приложений и структурированных библиотек программной среды 1С Предприятие;
-Работа в системе реализована в виде использования специализированных файлов приложений с расширениями **.dt, .epf, xml.**

8.2.1.8. Ввод-вывод данных в систему:

-Информация поступает в систему и выводится из системы путем ввода данных операторами.

8.2.1.9. Обработка данных в системе:

-Режим обработки предусматривает следующие действия с данными: сбор, чтение, накопление, систематизацию, уточнение, удаление, резервирование, распределение и представление в форме отчетности;
-Хранение данных осуществляется в специализированной базы данных 1С Предприятие на выделенном сервере на отдельном жестком диске и в отдельном каталоге.
-Хранение резервных копий базы данных осуществляется на отдельных для каждой базы данных дисковых массивах в системе выделенного сервера сетевого хранения.
-Хранение резервных копий базы данных осуществляется также на отдельном внешнем накопителе на жестком диске, находящимся в сейфе с ограниченном доступом.

8.2.1.10. Взаимодействие в системе:

-Исходящая информация передается в виде файлов и отчетов с применением электронных подписей ответственных должностных лиц и программной библиотеки защиты информации «КриптоПро 4.0», в электронном виде по каналам в сети Интернет посредством программного комплекса «СБИС +» и программного комплекса УФК России «СУФД – онлайн»).

8.2.2. Описание МИС ПДн Администрации ЗАТО город Заозерск МИС ПДн «1С: Предприятие» в конфигурации «Зарплата и кадры государственного учреждения», версии 3.1

8.2.2.1. Основание создания и рамещения:

-Постановление администрации ЗАТО город Заозерск от 25.05.2015 № 387 «Об утверждении Положения о муниципальных информационных системах муниципального образования ЗАТО город Заозерск».

-Размещено в «Реестре муниципальных информационных систем муниципального образования ЗАТО город Заозерск».

8.2.2.2. Назначение:

-**МИС ПДн «1С: Предприятие» в конфигурации «Зарплата и кадры государственного учреждения», версии 3.1** поддерживает единый, методически выверенный, взаимосвязанный технологический процесс ведения учета, который предусматривает получение всех необходимых первичных документов и регистров учета и **предназначена для:**

-Отчетов по начисленным и уплаченным суммам страховых взносов, переданным в ПФР, за любой период.
-Предоставления форм статистической отчетности с автоматическим заполнением: П4, П-4(НЗ), З-Ф.
-Расчеты и выплаты заработной платы сотрудникам учреждений, так и для отдельных подразделений или конкретных сотрудников.

-Формирования ведомостей на выплату зарплаты по всем источникам финансирования сразу. Выплаты аванса сотрудникам и нескольких межрасчетных начислений (отпусков, больничных листов и пр.).
-Внесение изменений в штатное расписание учреждений.
-Аттестация госслужащих: формирование аттестационной комиссии, график аттестации, протоколы аттестационной комиссии.
-Ведение реестра государственных служащих.
-Настройка надбавок в процентах от базовой ставки.
-Автоматический контроль изменений групп и соответствующих уровней при кадровых изменениях.

8.2.2.3. Цель создания:

Обеспечение единого методически выверенного, взаимосвязанного технологического процесса ведения бухгалтерского учета, который предусматривает получение всех необходимых первичных документов и регистров учета.

8.2.2.4. Характеристики ИСПНд:

-Группа ИСПДн (иные ПНд, согласно п.5 постановления Правительства РФ от 01.11.2012 № 1119);
-Категория ИСПДн (категория 2, в соответствии с требованиями постановления Правительства РФ от 01.11.2012 № 1119);
-Тип угроз, актуальных для МИС (угрозы 3 типа, в соответствии с требованиями постановления Правительства РФ от 01.11.2012 № 1119);
-Уровень защищенности – 4, в соответствии с требованиями постановления Правительства РФ от 01.11.2012 № 1119;
-Уровень значимости информации УЗ-3, в соответствии с требованиями Федерального закона от 27.07.2006 № 149-ФЗ и приказа ФСТЭК России от 11.02.2013 № 17;
-Режим обработки ПДн (многопользовательский);
-Класс защищенности К3, в соответствии с требованиями Федерального закона от 27.07.2006 № 149-ФЗ и приказа ФСТЭК России от 11.02.2013 № 17;
-Разграничение прав доступа (с разграничением);
-Масштаб МИС (менее чем 1000 субъектов);
-Класс защищенности МИС

8.2.2.5. Структура системы:

-Технологическая платформа 1С Предприятие, версии 8.3;
-Конфигурация «Зарплата и кадры государственного учреждения», версии 3.1
-База данных «Зарплата и кадры государственного учреждения», версии 3.1
-Система автоматического резервирования каталогов и базы данных «Зарплата и кадры государственного учреждения», версии 3.1 на основе программы EFFECTOR SAVER 3.3.1 с открытым исходным кодом.
-Система ручного резервирования каталогов и базы данных «Зарплата и кадры государственного учреждения», версии 3.1 на основе программы «Зарплата и кадры государственного учреждения», версии 3.1.

8.2.2.6. Объем и содержание персональных данных, обрабатываемых в конфигурации «Зарплата и кадры государственного учреждения», версии 3.1:

-Объем базы данных: **200 МБ.**
-Формат хранения базы данных: **.dt**

Содержание персональных данных в базе данных:

-Паспортные данные сотрудников;
-Кадровые сведения о сотрудниках;
-Кадровые сведения об уволенных сотрудниках;
-Сведения о близких родственниках сотрудника;
-Сведения о размере заработной платы;
-Сведения о трудовой деятельности сотрудников;

-Сведения о расчетах и начислениях по заработной плате;
-Формирование расчетов и начислений по заработной плате;
-Сведения и отчетность по выбранным сотрудникам;
-Организация парольной защиты доступа к базе данных;
-Организация и сведения о полномочиях и ролях пользователей базы данных;

8.2.2.7. Реализация системы:

-Работа в системе реализована в виде обработки файлов стандартных офисных приложений MS Office, OpenOffice;
-Работа в системе реализована в виде обработки файлов стандартных приложений и структурированных библиотек программной среды 1С Предприятие;
-Работа в системе реализована в виде использования специализированных файлов приложений с расширениями **.dt, .epf, xml.**

8.2.2.8. Ввод-вывод данных в систему:

-Информация поступает в систему и выводится из системы путем ввода данных операторами.

8.2.2.9. Обработка данных в системе:

-Режим обработки предусматривает следующие действия с данными: сбор, чтение, накопление, систематизацию, уточнение, удаление, резервирование, распределение и представление в форме отчетности;
-Хранение данных осуществляется в специализированной базы данных 1С Предприятие на выделенном сервере на отдельном жестком диске и в отдельном каталоге.
-Хранение резервных копий базы данных осуществляется на отдельных для каждой базы данных дисковых массивах в системе выделенного сервера сетевого хранения.
-Хранение резервных копий базы данных осуществляется также на отдельном внешнем накопителе на жестком диске, находящимся в сейфе с ограниченном доступом.

8.2.2.10. Взаимодействие в системе:

-Исходящая информация передается в виде файлов и отчетов с применением электронных подписей ответственных должностных лиц и программной библиотеки защиты информации «КриптоПро 4.0», в электронном виде по каналам в сети Интернет посредством программного комплекса «СБИС +» и программного комплекса УФК России «СУФД – онлайн»).

8.2.3. Характеристики безопасности (конфиденциальность, целостность, доступность, подлинность), обеспечивающие обрабатываемые персональные данные.

Конфиденциальность сведений:

-создание локального акта Оператора с определением перечня конфиденциальных сведений;
-строгим отбором Оператором сотрудников для работы с ПНд;
-допуск сотрудников для работы с ПНд производиться только на основании локальных нормативных актов Оператора;
-систематическое обучение сотрудников на занятиях, семинарах правилам и методам работы с конфиденциальной информацией;
-проведение систематических инструктажей сотрудников по работе с конфиденциальной информацией и по мерам информационной безопасности;
-организация внутреннего контроля за порядком обработки и защиты ПНд и соблюдением мер информационной безопасности;
-систематическое логирование деятельности пользователей средствами ОС Windows Server и специальными средствами сбора логов;

Целостность сведений:

-разделенный режим копирования баз данных, включая копирование на локальные и не размещенные в ЛВС Оператора сервера и носители данных;
-систематическое логирование деятельности пользователей средствами ОС Windows Server и специальными средствами сбора логов;

Доступность сведений:

-разделенная работа в базах данных пользователей обеспечивается разделением полномочий доступа к базам данных средствами ОС Windows Server и программы 1С: Предприятие в соответствующих конфигурациях;
-доступ к АРМ пользователей МИС ПДн из ЛВС другим пользователям не предоставляется;
-разделенный учет и работа в базах данных. Подключение к каждой базе данных производиться индивидуально пользователем через канал RDP на сервере терминалов;
-доступ к базам данных программы 1С: Предприятие в соответствующих конфигурациях через сеть Интернет отсутствует, основной сервер 1С: Предприятие к сети Интернет не подключен;
-допуск сотрудников для работы с ПНд производиться только на основании локальных нормативных актов Оператора;

8.2.4. Объекты, в которых размещены ресурсы информационных систем и физические меры защиты объектов, в которых размещены ресурсы информационных систем ПНд.

В соответствии с пунктом 13 Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119, **должны быть выполнены следующие требования:**

- Организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения (п.5 п.п. а-г) приказа ФСБ России от 10 июля 2014 № 378;

- Для выполнения требования, указанного в подпункте "а" пункта 5 приказа ФСБ России от 10 июля 2014 № 378, необходимо обеспечение режима, препятствующего возможности неконтролируемого проникновения или пребывания в помещениях, где размещены используемые ИСПДн, СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ (далее - Помещения), лиц, не имеющих права доступа в Помещения, **которое достигается путем:**

АРМ пользователей:
-размещения АРМ сотрудников в закрываемых на обычные замки помещениях первого и второго этажа здания по пер. Школьный д.1;
-физический доступ в отдел бухгалтерского учета и планирования МКУ «МФЦ ЗАТО город Заозерск» на втором этаже здания по пер. Школьный д.1 имеет возможность блокирования доступа с двух направлений и находиться под охранно-пожарной сигнализацией;
-в случае утраты ключей от помещений **немедленно** заменяется замок;
-уборка в помещениях, где ведется обработка ПДн, производится только в присутствии сотрудников Администрации ЗАТО город Заозерск, ответственных за эти помещения.
-при обнаружении повреждений замков или других признаков, указывающих на возможное проникновение в помещения, в которых ведется обработка ПДн, посторонних лиц, эти помещения **не вскрываются**, а комиссией по защите персональных данных в информационных системах персональных данных Администрации ЗАТО города Заозерска составляется акт и о случившемся немедленно ставится в известность Глава администрации ЗАТО город Заозерск. Одновременно принимаются меры по охране места происшествия и до прибытия сотрудников органов МВД в эти помещения никто не допускается.
-вскрытие помещений, где ведется обработка ПДн, производят только работники, работающие в этих помещениях.
-при отсутствии сотрудников Администрации ЗАТО город Заозерск, работающих в этих помещениях, помещения могут быть вскрыты комиссией по защите персональных данных в информационных системах персональных данных администрации ЗАТО город Заозерск.

Помещение № 12 (место хранения основного сервера 1С):
-помещение № 12 на первом этаже здания по адресу: пер. Школьный д.1 закрывается на обычный замок и находиться под охранно-пожарной сигнализацией;
-физический доступ к панели управления сервером ПНд закрыт на специальный замок;

-программный доступ к панелям администрирования сервера осуществляется с использованием парольной защиты. Пароль администратора известен только сотрудникам отдела ИПО МКУ «МФЦ ЗАТО город Заозерск», как системным администраторам Оператора;
-в случае утраты ключей от помещений **немедленно** заменяется замок;
-уборка в помещении, где ведется обработка ПДн, производится только в присутствии сотрудников, ответственных за эти помещения.
-при обнаружении повреждений замков или других признаков, указывающих на возможное проникновение в помещения, в которых ведется обработка ПДн, посторонних лиц, эти помещения **не вскрываются**, а комиссией по защите персональных данных в информационных системах персональных данных администрации ЗАТО города Заозерска составляется акт и о случившемся немедленно ставится в известность Глава администрации ЗАТО город Заозерск. Одновременно принимаются меры по охране места происшествия и до прибытия сотрудников органов МВД в эти помещения никто не допускается.
-вскрытие помещений, где ведется обработка ПДн, производят только сотрудники отдела ИПО МКУ «МФЦ ЗАТО город Заозерск».
-при отсутствии сотрудников отдела ИПО МКУ «МФЦ ЗАТО город Заозерск» работающих в этих помещениях, помещения могут быть вскрыты комиссией по защите персональных данных в информационных системах персональных данных администрации ЗАТО город Заозерск.
Меры по обеспечению контролируемых зон Оператора (далее - КЗ):
-КЗ размещены на всех этажах здания по пер. Школьный д.1.
-КЗ объединяют помещения, в которых производиться обработка ПНд, хранятся СКЗИ и определить пути эвакуации сотрудников, средств обработки ПНд и СКЗИ в случае возникновения чрезвычайных ситуаций природного или техногенного характера (приложения к настоящей Политике). Границей контролируемых зон **является** периметр выделенных помещений.
Меры в случае угроз природного или техногенного характера и других ЧС:
-все СКЗИ, ЭП должны быть в **обязательном порядке** эвакуированы ответственными за них сотрудниками в соответствии со схемами эвакуации СКЗИ и ЭП (в приложении к Политике).

8.2.5. Типы и характеристики информационных систем ПНд.

Наименование серверной операционной системы:
-Microsoft Windows Server 2012 Standart x 64 rus;
Наименование клиентской операционной системы:
-Microsoft Windows 7 32 x 64 sp.1 rus;
-Microsoft Windows 10 x 64 rus;
Общее количество серверов и рабочих станций клиентов:
-1 сервер баз данных МИС ПНд в клиент-серверном варианте с файловой базой данных;
-12 пользователей сервера МИС ПНд;
-тип соединения с базой данных МИС ПНд сервера: **терминальный, через RDP;**
Тип информационных систем - совокупность изолированных (разделенные базы данных и разделенные конфигурации) и взаимосвязанных информационных подсистем, через единую программную платформу 1С: Предприятие.
Информационное взаимодействие каждой подсистемы информационной системы или информационной системы в целом с другими информационными системами, а также наличие факта передачи персональных данных между ними:
-информационного взаимодействия каждой подсистемы МИС ПНд (как информационной системы) или информационной системы МИС ПНд в целом с другими информационными системами Оператора, а также наличие факта передачи персональных данных между ними **технически не предусмотрено.**
Каналы (линии) связи:
-доступ к ресурсам сети интернет у Оператора осуществляется по оптоволоконным линиям связи через оконечное устройство на границе периметра ЛВС;

-доступ пользователей обрабатывающих ПНд к ресурсам МИС ПНд осуществляется по ЛВС, по кабелям типа UTP-5E;
-у каналов (линий) связи отсутствует возможность несанкционированного подключения внутри ЛВС Оператора к ним, без фактического нарушения их целостности.

Носители защищаемой информации, используемые в каждой подсистеме информационной системы:

-в качестве носителей защищаемой информации, используемых в каждой подсистеме МИС ПНд используются накопители на жестких дисках, установленные на компьютерах пользователей и сервере 1С, объемом от 500 Гб до 2 Тб;
-самостоятельного физического доступа к носителям защищаемой информации (к накопителям на жестких дисках), используемым в каждой подсистеме МИС ПНд, и установленным на компьютерах пользователей и сервере 1С, у пользователей Оператора нет.

8.2.6.Средства защиты информации в МИС ПНд на АРМ пользователей и сервере 1С.

Средства защиты информации в МИС ПНд на АРМ пользователей и сервере 1С:

-сертифицированное средство защиты информации от несанкционированного доступа DallasLock 8.0-K;
-сертифицированное средство антивирусной защиты Kaspersky Endpoint Security 10 для Бизнеса (расширенный пакет Russian Edition);
-сертифицированное средство антивирусной защиты Microsoft Security Essentials;
-сертифицированное средство аппаратного межсетевого экранирования ALTELL NEO 120;

В МИС ПНд **разрешено** использование средств защиты информации, **только** прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.

8.3. Определение актуальности использования СКЗИ для обеспечения безопасности персональных данных.

Требования к криптографическим средствам и условиям их эксплуатации регламентируются приказами 8 центра ФСБ "России от 21.02.2008 № 149/54-144 «Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации», от 21.02.2008 № 149/6/6-622 «Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных». Настройки средств защиты информации от несанкционированного доступа, межсетевых экранов, средств обнаружения вторжений и других СЗИ должны соответствовать требованиям приказов ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» для установленного уровня защищённости персональных данных» и от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

8.3.1.Персональные данные которые обрабатывают сотрудники Оператора и которые передаются через систему Управления Федерального казначейства РФ по Мурманской области (СУФД-онлайн) - **подлежат криптографической защите** в соответствии с законодательством Российской Федерации и требованиями информационной безопасности и регламентами УФК РФ по Мурманской области:

- на каждом рабочем компьютере сотрудников отдела бухгалтерского учета и планирования МКУ «МФЦ ЗАТО город Заозерск» установлены следующие СКЗИ:

- Сертифицированное СКЗИ «Крипто Про» версии 4.0., с индивидуальными пользовательскими лицензиями ;
- Сертифицированное СКЗИ «Континент АП» с лицензией на Оператора – 8 шт.;

-на каждом рабочем компьютере сотрудников ФБО Администрации ЗАТО город Заозерск установлены следующие СКЗИ:

- Сертифицированное СКЗИ «Крипто Про» версии 4.0., с индивидуальной пользовательской лицензией - 4 шт;
- Сертифицированное СКЗИ «Континент АП» версии 3.7, с лицензией на Оператора – 4 шт;
- Сертифицированное СКЗИ «Континент АП TLS VPN Client», версии 1.2 с лицензией на Оператора – 2 шт;
- Сертифицированное СКЗИ «JINN Клиент» для создания электронной подписи и доверенной визуализации документов с лицензией на Оператора – 2 шт;

-на рабочих компьютерах сотрудников Управления ЭР, ЖКХ и МИ Администрации ЗАТО город Заозерск установлены следующие СКЗИ:

- Сертифицированное СКЗИ «Крипто Про» версии 4.0., с индивидуальной пользовательской лицензией - 6 шт;
- Сертифицированное СКЗИ «Континент АП» версии 3.7, с лицензией на Оператора – 6 шт;

Для выполнения требования, указанного в подпункте "б" пункта 5 приказа ФСБ России от 10 июля 2014 № 378, необходимо обеспечение режима хранения **которое достигается путем:**

-Осуществление хранения съемных машинных носителей персональных данных в сейфах (металлических шкафах), оборудованных внутренними замками с двумя или более дубликатами ключей и приспособлениями для опечатывания замочных скважин или кодовыми замками. В случае если на съемном машинном носителе персональных данных хранятся только персональные данные в зашифрованном с использованием СКЗИ виде, допускается хранение таких носителей вне сейфов (металлических шкафов);

-Осуществлять поэкземплярный учет машинных носителей персональных данных, который достигается путем ведения журнала учета носителей персональных данных с использованием регистрационных (заводских) номеров.

8.3.2.Передача данных Оператора по каналам связи, не защищенным от перехвата нарушителем передаваемой по ним информации или от несанкционированных воздействий на эту информацию, <u>осуществляется только:</u>

-сотрудниками отдела бухгалтерского учета и планирования МКУ «МФЦ ЗАТО город Заозерск» через сертифицированное ФСБ России решение для обеспечения удаленного доступа - СКЗИ «Континент АП», работающее как шлюз, через собственный защищенный сервер;

-сотрудниками ФБО Администрации ЗАТО город Заозерск, через сертифицированное ФСБ России решение для обеспечения удаленного доступа - СКЗИ «Континент АП», работающее как шлюз, через собственный защищенный сервер;

-сотрудниками Управления ЭР, ЖКХ и МИ Администрации ЗАТО город Заозерск, через сертифицированное ФСБ России решение для обеспечения удаленного доступа - СКЗИ «Континент АП», работающее как шлюз, через собственный защищенный сервер;

-хранение персональных данных на носителях информации, установленных на рабочих местах сотрудников допущенных к работе с ПНд **не осуществляется**, несанкционированный доступ к ним со стороны нарушителя **может быть исключен с помощью не криптографических методов и способов.**
-СКЗИ штатно функционируют совместно с техническими и программными средствами, которые способны повлиять на выполнение предъявляемых к СКЗИ требований и которые образуют среду функционирования СКЗИ.
-СКЗИ обеспечивают защиту информации при условии соблюдения требований эксплуатационно-технической документации на СКЗИ и требований действующих нормативных правовых документов в области реализации и эксплуатации СКЗИ;
-для обеспечения безопасности персональных данных при их обработке в МИС ПДн используются СЗИ, прошедшие в установленном порядке процедуру оценки соответствия, на основании **аттестата соответствия** объекта информатизации по СЗИ **от 26.06.2015 № ПД /0389923 - 01-09.**

8.3.3. Носители защищаемой информации, используемые в информационной системе ПНд в процессе криптографической защиты ПНд, носители ключевой, парольной и аутентифицирующей информации СКЗИ и порядок доступа к ним.

8.3.3.1. Носители защищаемой информации, используемые в информационной системе в процессе криптографической защиты персональных данных, носители ключевой, парольной и аутентифицирующей информации СКЗИ и порядок доступа к ним определяются требованиями нормативно – правовых документов Оператора и требованиями Регуляторов РФ к криптографическим средствам и условиям их эксплуатации **регламентируются:**
-Федеральным законом РФ от 6 апреля 2011 № 63 «Об электронной подписи».
-приказом ФСБ России от 10 июля 2014 № 378 «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».
-приказом 8 центра ФСБ России от 21.02.2008 № 149/54-144 «Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации», -приказом 8 центра ФСБ России от 21.02.2008 № 149/6/6-622 «Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных».
-приказом ФАПСИ от 13 июня 2001 № 152 "Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну".

Настройки средств защиты информации от несанкционированного доступа, межсетевых экранов, средств обнаружения вторжений и других СЗИ **должны соответствовать требованиям:**
-приказа ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» для установленного уровня защищённости персональных данных»;
-приказа ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

Работа с носителями ключевой, парольной и аутентифицирующей информации в сфере финансовой деятельности определены регламентом УФК РФ по Мурманской области.

Работа с носителями ключевой, парольной и аутентифицирующей информации в сфере деятельности государственных информационных систем определены регламентами УУЦ РФ «Электронный город +» и УУЦ РФ по Мурманской области «ТЕНЗОР».

8.3.3.2. Носители защищаемой информации, используемые в информационной системе в процессе криптографической защиты персональных данных, носители ключевой, парольной и аутентифицирующей информации СКЗИ и порядок доступа к ним **определяются требованиями:**

-электронные подписи, предназначенные для обеспечения финансовой деятельности Оператора получаются в соответствии с регламентом УФК РФ по Мурманской области;

-электронные подписи, предназначенные для обеспечения финансовой деятельности Оператора учитываются, хранятся и защищаются в соответствии с требованиями приказа ФАПСИ от 13 июня 2001 года № 152 "Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну".

-электронные подписи, предназначенные для обеспечения работы в сфере деятельности государственных информационных систем получаются в соответствии с регламентами УУЦ РФ «Электронный город +» и УУЦ РФ по Мурманской области «ТЕНЗОР».

-электронные подписи, предназначенные для обеспечения работы в сфере деятельности государственных информационных систем Оператора, учитываются, хранятся и защищаются в соответствии с требованиями приказа ФАПСИ от 13 июня 2001 года № 152 "Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну".

8.4. Определение актуальных угроз МИС ПНд.

Оператор осуществляет определение типа угроз безопасности персональных данных, актуальных для информационной системы с учетом оценки возможного вреда во исполнении п.5 части 1 статьи 18.1 Федерального закона "О персональных данных".

Под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого может стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

Для обеспечения безопасности персональных данных при их обработке в МИС ПДн используются СЗИ, прошедшие в установленном порядке процедуру оценки соответствия и на основании аттестата соответствия объекта информатизации по СЗИ от 26.06.2015 № ПД /0389923 - 01-09 **разработаны следующие документы по угрозам:**

-Модель нарушителя информационной безопасности на объекте информатизации «Муниципальная информационная система Муниципального образования ЗАТО город Заозерск» **№ ПД/0389923-01-15/1.**

-Модель угроз безопасности персональных данных при их обработке в «Муниципальной информационной системе Муниципального образования ЗАТО город Заозерск» **№ ПД/0389923-01-15.**

8.5. Порядок привлечения специализированных сторонних организаций к разработке, модификации и обновлению баз данных МИС ПДн Оператора и средств защиты информации в МИС ПДн Оператора.

Порядок привлечения специализированных сторонних организаций к разработке и эксплуатации новых ИСПДн, модификации и обновлению баз данных, их задачи и функции на различных стадиях создания и эксплуатации ИСПДн определяются Главой администрации ЗАТО город Заозерск исходя из особенностей эксплуатации информационных систем ПДН.

Разработка систем защиты ПДн в ИСПДн Администрации ЗАТО город Заозерск и контроль за эксплуатацией ИСПДн осуществляются сотрудниками отдела ИПО МКУ «МФЦ ЗАТО город Заозерск» отвечающими в соответствии с Соглашением об информационно-техническом обеспечении за информатизацию и защиту информации.

Для проведения мероприятий по обеспечению безопасности ПДн для ИСПДн первого и второго класса и распределенных систем третьего класса специализированные сторонние организации должны иметь лицензии ФСТЭК России и ФСБ России на осуществление деятельности по технической защите конфиденциальной информации.

Без наличия соответствующих лицензий проведение мероприятий по защите ПДн возможно только для нераспределенных информационных систем третьего класса, а также для информационных систем четвертого класса.

В случае если Администрация ЗАТО город Заозерск, как оператор ПДн, на основании договора (муниципального контракта) поручает другому лицу (организации) произвести работы по модификации (производству обновлений и усовершенствований) базы ПДн данных и произвести регламентные работы с базой данных или произвести обработку этих ПДн, **существенным условием договора** (муниципального контракта) **должна является** обязанность обеспечения указанным лицом конфиденциальности ПДн и безопасности базы ПДн при её обработке. Базы ПДн передаются другому лицу **по акту** в зашифрованном виде на носителе (Флэш-диске, CD&DVD диске) (приложение к Политике).

9. Работники Оператора, осуществляющие обработку ПНд.

9.1. Состав работников Оператора (перечень их должностей), осуществляющих обработку персональных данных, определяется руководителями подразделений Оператора, обрабатывающих персональные данные субъектов ПНд и утверждается распоряжением Администрации ЗАТО город Заозерск.

9.2. Работники Оператора, непосредственно осуществляющие обработку персональных данных, должны быть ознакомлены с положениями законодательства РФ о персональных данных, в том числе с требованиями к защите персональных данных, положениями и актами Оператора, определяющими политику в отношении обработки персональных данных **под личную подпись** (приложение к Политике).

9.3. С работников Оператора, непосредственно осуществляющих обработку персональных данных, должны быть в установленном порядке оформлены обязательства о выполнении требований положений и актов Оператора по обработке, защите и неразглашении информации ограниченного доступа (далее—Обязательство) (Приложение 5 к Политике).
Обязательство о неразглашении информации ограниченного доступа подлежит оформлению со всеми лицами, осуществляющими обработку персональных данных у Оператора или имеющими к ним служебный доступ.

9.4. Обязанности работника как оператора ПНд.

Оператор ПДн при обработке ПДн субъектов ПДн **обязан:**

- строго соблюдать принципы и правила обработки ПДн;
- в случае если обработка ПДн осуществляется по поручению оператора ПДн, строго соблюдать и выполнять требования оператора ПДн;

- **не раскрывать третьим лицам и не распространять ПДн** без согласия субъекта ПДн, если иное не предусмотрено федеральным законом;
- по требованию субъекта ПДн либо по решению суда или иных уполномоченных государственных органов исключить из общедоступных источников ПДн сведения о субъекте ПДн;
- обеспечить конкретность и информированность субъекта ПНд перед дачей им согласия на обработку ПДн;
- получать согласие на обработку ПДн, если иное не предусмотрено действующим законодательством;
- в случае получения согласия на обработку ПДн от представителя субъекта ПДн **обязательно проверять** полномочия данного представителя на дачу согласия от имени субъекта ПДн;
- по требованию уполномоченного органа по защите прав субъектов ПДн, представить доказательство получения согласия субъекта ПДн на обработку его ПДн или доказательство наличия оснований обработки ПДн без получения согласия;
- строго соблюдать требования к содержанию согласия в письменной форме субъекта ПДн на обработку его ПДн;
- незамедлительно прекратить обработку специальных категорий ПДн, **если таковая обработка производилась** и если устранены причины, вследствие которых осуществлялась обработка, если иное не установлено федеральным законодательством РФ;
- убедиться в том, что иностранным государством, на территорию которого осуществляется передача ПДн, обеспечивается адекватная защита прав субъектов ПДн, до начала осуществления трансграничной передачи ПДн (**если такая передача предусмотрена НПА Оператора**);
- предоставить субъекту ПДн сведения по запросу субъекта ПДн в доступной форме, в которых не должны содержаться ПДн, относящиеся к другим субъектам ПДн, за исключением случаев, если имеются законные основания для раскрытия таких ПДн;
- мотивировать и представить доказательства обоснованности отказа в выполнении повторного запроса субъекта ПДн;
- разъяснить субъекту ПДн порядок принятия решения на обработку его ПДн и возможные юридические последствия такого решения, предоставить возможность заявить возражение против такого решения, а также разъяснить порядок защиты субъектом ПДн своих прав и законных интересов;
- предоставить субъекту ПДн по его просьбе информацию, касающуюся обработки его ПДн;
- разъяснить субъекту ПДн юридические последствия отказа предоставить его ПДн, если предоставление ПДн является обязательным в соответствии с федеральным законом;
- до начала обработки ПДн, полученных не от субъекта ПДн, предоставить субъекту ПДн информацию о своем наименовании и адресе, цели обработки ПДн и ее правовом основании, предполагаемых пользователях ПДн, об установленных правах субъекта ПДн, источник получения ПДн;
- принимать меры, необходимые и достаточные для обеспечения выполнения своих обязанностей в области ПДн, если иное не предусмотрено федеральными законами;
- опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки ПДн, к сведениям о реализуемых требованиях к защите ПДн;
- по запросу уполномоченного органа по защите прав субъектов ПДн представить документы и локальные акты, определяющие политику в отношении обработки ПДн, и сведения о реализуемых требованиях к защите 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;

- сообщить субъекту ПДн или его представителю 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 при получении запроса субъекта ПДн или его представителя;
- в случае отказа в предоставлении информации о наличии ПДн соответствующего субъекта ПДн или его представителю при их обращении либо при получении запроса субъекта ПДн или его представителя дать в письменной форме мотивированный ответ;
- предоставить безвозмездно субъекту ПДн или его представителю возможность ознакомления с ПДн, относящимися к этому субъекту ПДн;
- внести в ПДн необходимые изменения или уничтожить такие ПДн в случае предоставления субъектом ПДн или его представителем сведений, подтверждающих, что ПДн являются неполными, неточными или неактуальными;
- строго соблюдать сроки по уведомлениям, блокированию и уничтожению ПДн;
- 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;
- сообщить в уполномоченный орган по защите прав субъектов ПДн по запросу этого органа необходимую информацию;
- 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 оператор обязан осуществить блокирование неправомерно обрабатываемых ПДн, относящихся к этому субъекту ПДн, или обеспечить их блокирование (если обработка ПДн осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки;
- в случае выявления неточных ПДн при обращении субъекта ПДн или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов ПДн оператор обязан осуществить блокирование ПДн, относящихся к этому субъекту ПДн, или обеспечить их блокирование (если обработка ПДн осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки, если блокирование ПДн не нарушает права и законные интересы субъекта ПДн или третьих лиц;
- уточнять ПДн субъекта ПНд, либо обеспечить их уточнение (если обработка ПДн осуществляется другим лицом, действующим по поручению оператора ПДн) и снять блокирование ПДн в случае подтверждения факта неточности ПДн на основании сведений, представленных субъектом ПДн или его представителем либо уполномоченным органом по защите прав субъектов ПДн, или иных необходимых документов;
- прекратить неправомерную обработку ПДн или обеспечить прекращение неправомерной обработки ПДн лицом, действующим по поручению оператора ПДн в случае выявления неправомерной обработки ПДн, осуществляемой оператором или лицом, действующим по поручению оператора;
- уничтожить ПДн или обеспечить их уничтожение в случае, если обеспечить правомерность обработки ПДн невозможно;
- 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 об устранении допущенных нарушений или об уничтожении ПДн;
- 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 случае достижения цели обработки ПДн, если обработка ПДн осуществляется без согласия субъекта ПДн на основаниях, предусмотренных федеральным законом;
- в случае отзыва субъектом ПДн согласия на обработку его ПДн, если обработка ПДн осуществляется без согласия субъекта ПДн на основаниях, предусмотренных федеральным законом;
- уведомить уполномоченный орган по защите прав субъектов ПДн о своем намерении осуществлять обработку ПДн;
- уведомить уполномоченный орган по защите прав субъектов ПДн в случае изменения сведений, указанных в уведомлении о своем намерении осуществлять обработку ПДн;
- назначить лицо, ответственное за организацию обработки ПДн и администратора безопасности ИСПДн;
- предоставлять лицу, ответственному за организацию обработки ПДн, необходимые сведения;
- неукоснительно соблюдать все требования настоящего Положения;
- ознакомить муниципальных служащих, служащих, замещающих должности, не отнесенные к должностям муниципальной службы структурных подразделений и Управлений Администрации ЗАТО город Заозерск и сотрудников МКУ «МФЦ ЗАТО город Заозерск», допущенных к обработке персональных данных в интересах служебной деятельности Администрации ЗАТО город Заозерск, с требованиями действующего законодательства Российской Федерации, Мурманской области, нормативных правовых актов Российской Федерации, Мурманской области в области персональных данных (в том числе с требованиями к защите персональных данных), нормативными правовыми актами органов местного самоуправления ЗАТО города Заозерска по вопросам обработки персональных данных, и организовать обучение таких работников.

9.5. Требования к муниципальным служащим и служащим, замещающим должности, не отнесенные к должностям муниципальной службы структурных подразделений и управлений Администрации ЗАТО город Заозерск, сотрудникам МКУ «МФЦ ЗАТО город Заозерск», действующим в интересах служебной деятельности Администрации ЗАТО город Заозерск и допущенным к обработке ПДн.

9.5.1. Ответственный работник за организацию обработки и защиты ПДн:

В соответствии с пунктом 14 Требований к защите персональных данных утвержденных постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119, для обеспечения 3 уровня защищенности персональных данных при их обработке в информационных системах помимо выполнения требований, предусмотренных пункта 5 приказа ФСБ России от 10 июля 2014 № 378, необходимо обеспечение режима защиты ПНд, **которое достигается путем:**

- назначение должностного работника, ответственного за обеспечение безопасности персональных данных в информационной системе.

Ответственный работник за организацию обработки и защиты ПДн:

-Осуществляет инструктаж и ознакомление муниципальных служащих, служащих, замещающих должности, не отнесенные к должностям муниципальной службы структурных подразделений и управлений Администрации ЗАТО город Заозерск, сотрудников МКУ «МФЦ ЗАТО город Заозерск», действующих в интересах служебной деятельности Администрации ЗАТО город Заозерск и допущенных к обработке персональных данных, сотрудников находящихся на испытательном сроке перед приемом на работу в Администрацию ЗАТО город Заозерск с требованиями действующего законодательства Российской Федерации, Мурманской области, нормативных правовых актов Российской Федерации, Мурманской области в области информационной безопасности, безопасности персональных данных (в том числе и с требованиями к защите персональных данных), нормативными правовыми актами органов

местного самоуправления ЗАТО город Заозерск по вопросам информационной безопасности, обработки и защиты персональных данных, включая настоящую Политику;
-**Осуществляет инструктаж и ознакомительную беседу с сотрудником** при оформлении трудового договора;
-Осуществляет инструктаж и ознакомительную беседу с сотрудником при оформлении испытательного срока до заключения трудового договора;
-Осуществляет инструктаж и ознакомительную беседу с сотрудником при первоначальном допуске к обработке ПДн;
-Осуществляет инструктаж и ознакомительную беседу с сотрудником при назначении на должность, связанную с обработкой конфиденциальной информации и обработкой ПДн;
-Осуществляет инструктаж с сотрудником после внесения изменений в действующее законодательство Российской Федерации, Мурманской области, нормативные правовые акты Российской Федерации, Мурманской области в области персональных данных, нормативные правовые акты органов местного самоуправления ЗАТО город Заозерск по вопросам обработки персональных данных.
-Осуществляет инструктаж, проводит внеплановые инструктажи и занятия по указанию Главы администрации ЗАТО город Заозерск.

9.5.2. Муниципальные служащие, служащие, замещающие должности, не отнесенные к должностям муниципальной службы структурных подразделений и Управлений Администрации ЗАТО город Заозерск, сотрудники МКУ «МФЦ ЗАТО город Заозерск», действующие в интересах служебной деятельности Администрации ЗАТО город Заозерск и допущенные к обработке персональных данных и к конфиденциальной информации, **обязаны:**

- неукоснительно следовать принципам и правилам обработки и защиты конфиденциальной информации и ПДн;
- знать и строго соблюдать положения действующего законодательства Российской Федерации, Мурманской области, нормативных правовых актов Российской Федерации, Мурманской области в области информационной безопасности, защиты конфиденциальной информации и персональных данных;
- знать и строго соблюдать требования и положения нормативных правовых актов органов местного самоуправления ЗАТО город Заозерск по вопросам обработки, защиты и обеспечения информационной безопасности конфиденциальной информации и ПДн;
- сотрудники находящихся **на испытательном сроке** перед приемом на работу в Администрацию ЗАТО город Заозерск, и после заключения трудового договора, **по указанию своего непосредственного руководителя обязаны своевременно не позднее второго рабочего дня прибыть на инструктаж по информационной безопасности, порядку и правилам обработки и защиты конфиденциальной информации и ПДн к ответственному за информационную безопасность лицу,** а также получить у него под личную роспись **временный логин и пароль** для доступа к соответствующему ресурсу МИС органов местного самоуправления ЗАТО город Заозерск. После официального вступления в трудовые отношения с Администрацией ЗАТО город Заозерск пароль и логин для данного сотрудника будет заменен на постоянный;
- знать и строго соблюдать инструкции, руководства и иные эксплуатационные документы на применяемые средства автоматизации, в том числе программное обеспечение ПДн и средства защиты информации;
- соблюдать конфиденциальность обработки и защиты ПДн, самостоятельно без согласия субъекта ПДн, не предоставлять третьим лицам и не распространять ПДн, если иное не предусмотрено федеральным законодательством РФ;
- не допускать нарушений требований и правил обработки и обеспечения безопасности конфиденциальной информации и ПДн;

- обо всех подозрениях и ставших известными случаях нарушений требований и правил обработки и обеспечения безопасности ПДн сообщать ответственному за организацию обработки ПДн.

Муниципальные служащие, служащие, замещающие должности, не отнесенные к должностям муниципальной службы структурных подразделений и Управлений Администрации ЗАТО города Заозерска, сотрудники МКУ «МФЦ ЗАТО города Заозерска», действующие в интересах служебной деятельности Администрации ЗАТО город Заозерск и допущенные к обработке персональных данных, **несут личную ответственность** за соблюдение требований действующего законодательства Российской Федерации, Мурманской области, нормативных правовых актов Российской Федерации, Мурманской области в области персональных данных, нормативных правовых актов органов местного самоуправления ЗАТО города Заозерска по вопросам обработки персональных данных, в том числе настоящей Политики.

10. Обязанности работодателя (Оператора) и работников Оператора при обработке ПНд.

10.1. В целях обеспечения прав и свобод человека и гражданина **работодатель и его представители** при обработке персональных данных работника **обязаны соблюдать следующие общие требования:**

-Обработка персональных данных работника может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности сотрудников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества;

-При определении объема и содержания обрабатываемых персональных данных работника работодатель должен руководствоваться требованиями Конституции Российской Федерации, требованиями Трудового Кодекса и иными федеральными законами Российской Федерации;

-Все персональные данные работника следует получать у него самого. Если персональные данные работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие.

Работодатель должен сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение;

-Работодатель **не имеет права** получать и обрабатывать персональные данные работника о его политических, религиозных и иных убеждениях и частной жизни.

В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьей 24 Конституции Российской Федерации, работодатель вправе получать и обрабатывать данные о частной жизни работника **только с его письменного согласия**;

-Работодатель **не имеет права** получать и обрабатывать персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законодательством РФ;

-При принятии решений, затрагивающих интересы работника, работодатель не имеет права основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронного получения;

-Защита персональных данных работника от неправомерного их использования или утраты должна быть обеспечена работодателем за счет его средств в порядке, установленном федеральным законодательством РФ;

-Работники или их представители должны быть ознакомлены под расписку с документами Оператора, устанавливающими порядок обработки персональных данных сотрудников, а также об их правах и обязанностях в этой области;

-Работники **не должны** любым способом отказываться от своих прав на сохранение и защиту прав и свобод как человека и гражданина.

-сотрудники находящихся **на испытательном сроке** перед приемом на работу в Администрацию ЗАТО город Заозерск, и сотрудники **заключившие трудовые отношения** с Администрацией ЗАТО город Заозерск, **по указанию своего непосредственного руководителя обязаны своевременно не позднее второго рабочего дня прибыть на инструктаж по информационной безопасности, порядку и правилам обработки и защиты конфиденциальной информации и ПДн к ответственному за информационную безопасность лицу,** а также получить у него под личную роспись **временный логин и пароль** для доступа к соответствующему ресурсу МИС органов местного самоуправления ЗАТО город Заозерск. После официального вступления в трудовые отношения с Администрацией ЗАТО город Заозерск пароль и логин для данного сотрудника будет заменен на постоянный.

10.2. Обязанности работника:

-Передавать работодателю или его представителю комплекс достоверных, документированных персональных данных, состав которых установлен Трудовым кодексом РФ;
-Своевременно сообщать работодателю об изменении своих персональных данных.

10.3. Права работника:

-Требовать исключения или исправления неверных или неполных сведений о своих персональных данных;
-На свободный, бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей свои персональные данные;
-Определять своих представителей для защиты своих интересов при обработке своих персональных данных;
-На сохранение и защиту своей личной и семейной тайны.

10.4. Обработка, передача и хранение персональных данных работника.

К обработке, передаче и хранению персональных данных работника **могут** иметь доступ следующие сотрудники Оператора, **в соответствии с матрицей ролей доступа:**

-Глава администрации ЗАТО город Заозерск;
-Первый заместитель Главы администрации ЗАТО город Заозерск - начальник Управления ЭР, ЖКХ и МИ и его заместитель;
-Заместитель Главы администрации ЗАТО город Заозерск по социальным вопросам - начальник Управления образования, культуры, спорта и молодежной политики и его заместитель;
-Начальник организационно - правового отдела Администрации ЗАТО город Заозерск и его заместитель;
-Юристы организационно - правового отдела Администрации ЗАТО город Заозерск;
-Начальник ФБО Администрации ЗАТО город Заозерск и его заместитель;
-Главный и ведущий специалист Администрации ЗАТО город Заозерск;-Главный бухгалтер отдела бухгалтерского учета и планирования МКУ «МФЦ ЗАТО город Заозерск» и его заместитель;
-Главный инженер программист-начальник Отдела ИПО МКУ «МФЦ ЗАТО город Заозерск» и лицо его официально по приказу замещающее;
-Ведущий специалист по кадровому менеджменту Администрации ЗАТО город Заозерск и лицо его официально по распоряжению замещающее;
-Ведущий специалист по учету обращений граждан в Администрацию ЗАТО город Заозерск;
-Ведущий специалист по социальной защите населения Администрации ЗАТО город Заозерск;
-Ведущие инженеры программисты Отдела ИПО МКУ «МФЦ ЗАТО город Заозерск»;
-Инженер программист 1 категории Отдела ИПО МКУ «МФЦ ЗАТО город Заозерск»;
-Ведущие бухгалтера отдела бухгалтерского учета и планирования МКУ «МФЦ ЗАТО город Заозерск»;
-Ведущие экономисты отдела бухгалтерского учета и планирования МКУ «МФЦ ЗАТО город Заозерск»;

-Секретари по работе с обслуживающими учреждениями МКУ «МФЦ ЗАТО город Заозерск»;
-Сам работник, носитель своих персональных данных;

Другие сотрудники Оператора имеют доступ к персональным данным работника только с письменного согласия самого работника, носителя данных.

10.5. Режим конфиденциальности персональных данных сотрудников снимается в случаях их обезличивания или по истечении 75 лет срока хранения, если иное не определено законами и настоящей Политикой.

10.6. При передаче персональных данных работника работодатель **должен соблюдать следующие требования:**

-не сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в случаях, установленных федеральным законом или соглашением сторон;
-не сообщать персональные данные работника в коммерческих целях без его письменного согласия;
-предупредить лиц, получающих персональные данные работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные работника, обязаны соблюдать режим конфиденциальности.
Данная Политика не распространяется на обмен персональными данными сотрудников в порядке, установленном федеральными законами РФ;
-разрешать доступ к персональным данным сотрудников только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций **в соответствии с матрицей ролей доступа к ПНд**;
-не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником своей трудовой функции;
-передавать персональные данные работника представителям сотрудников Оператора в порядке, установленном Трудовым Кодексом РФ, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций;
-передача персональных данных работника или передача персональных данных работника его представителем внешнему потребителю может допускаться в минимальных объемах и только в целях выполнения задач, соответствующих объективной причине сбора этих данных;
-при передаче персональных данных работника потребителям (в том числе и в коммерческих целях) за пределы организации Оператора, работодатель **не должен сообщать** эти данные третьей стороне **без письменного согласия работника**, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника или в случаях, установленных федеральным законом;
-все меры конфиденциальности при сборе, обработке и хранении персональных данных сотрудника распространяются как на бумажные, так и на электронные (автоматизированные) носители информации;
-**не допускается** отвечать на вопросы, связанные с передачей персональной информации по телефонной или факсимильной связи;

10.7. Порядок обезличивания ПНд работниками Оператора.

Осуществление обезличивания ПДн:

Обезличивание ПДн при обработке ПДн с использованием средств автоматизации осуществляется на основании нормативных правовых актов, правил, инструкций, руководств, регламентов и иных документов для достижения заранее определенных и заявленных целей.

Допускается обезличивание ПДн при обработке ПДн без использования средств автоматизации производить способом, исключающим дальнейшую обработку этих ПДн с сохранением возможности обработки иных данных, зафиксированных на материальном носителе.

Обезличивание ПДн может быть проведено с целью ведения статистических данных, снижения ущерба от разглашения защищаемых ПДн, снижения класса информационных систем ПДн Администрации ЗАТО город Заозерск и по достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

Способы обезличивания при условии дальнейшей обработки ПДн:

- уменьшение перечня обрабатываемых сведений;
- замена части сведений идентификаторами;
- обобщение – понижение точности некоторых сведений;
- понижение точности некоторых сведений (например, «Место жительства» может состоять из города и населенного пункта)
- деление сведений на части и обработка в разных информационных системах;
- иные способы, не противоречащие действующему законодательству Российской Федерации, Мурманской области.

Способом обезличивания в случае достижения целей обработки ПДн или в случае утраты необходимости в достижении этих целей является сокращение перечня ПДн.

Перечень должностей муниципальных служащих и служащих, замещающих должности, не отнесенные к должностям муниципальной службы структурных подразделений и управлений Администрации ЗАТО город Заозерск, должностей сотрудников МКУ «МФЦ ЗАТО город Заозерск», действующих в интересах служебной деятельности по проведению мероприятий по обезличиванию обрабатываемых ПДн в Администрации ЗАТО город Заозерск, приведен в Приложении № 9 к настоящей Политике.

Решение о необходимости обезличивания ПДн принимает Глава администрации ЗАТО город Заозерск **лично**.

Муниципальные служащие и служащие, замещающие должности, не отнесенные к должностям муниципальной службы структурных подразделений и Управлений Администрации ЗАТО города Заозерска, сотрудники МКУ «МФЦ ЗАТО города Заозерска», допущенные к обработке ПДн и действующие в интересах служебной деятельности по проведению мероприятий по обезличиванию обрабатываемых ПДн в Администрации ЗАТО город Заозерск, готовят предложения по обезличиванию ПДн, обоснование такой необходимости и способ обезличивания и совместно с ответственным за организацию обработки ПДн, осуществляют непосредственное обезличивание выбранным способом.

Обезличенные ПДн **не подлежат разглашению и нарушению конфиденциальности информации.**

Обезличенные ПДн могут обрабатываться с использованием и без использования средств автоматизации.

При обработке обезличенных ПДн с использованием средств автоматизации **необходимо соблюдение:**

- Требований по организации парольной защиты в муниципальных информационных системах и в других информационных системах Администрации ЗАТО город Заозерск;
- Инструкции об антивирусной защите в муниципальных информационных системах и в других информационных системах Администрации ЗАТО город Заозерск;
- Инструкции по работе со съемными машинными носителями информации на флэш-накопителях, на внешних жестких дисках, CD&DVD дисках, SD картах различных модификаций, портативных вычислительных устройствах с возможностью обработки информации (ноутбуки, нетбуки, планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие устройства и иные устройства) в Администрации ЗАТО город Заозерск;

- Регламента резервного копирования и восстановления работоспособности технических средств, программного обеспечения, баз данных в муниципальных информационных системах Администрации ЗАТО город Заозерск;
- Правил доступа в помещения, где расположены элементы ИСПДн; и места хранения баз данных;

При обработке обезличенных ПДн без использования средств автоматизации **необходимо соблюдение:**

- правил хранения бумажных носителей;
- правил доступа к ним и в помещения, где они хранятся.

10.8. Осуществление блокирования ПДн работниками Оператора.

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

Блокирование ПДн конкретного субъекта ПДн должно осуществляться во всех информационных системах ПДн, включая архивы баз данных, содержащих такие ПДн.

Блокирование ПДн 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.

После устранения выявленной неправомерной обработки ПДн оператор ПДн осуществляет снятие блокирования ПДн.

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

10.9. Осуществление уничтожения ПДн работниками Оператора.

Уничтожение ПДн - это действия, в результате которых становится невозможным восстановить содержание ПДн в информационной системе ПДн и (или) в результате которых уничтожаются материальные носители ПДн.

Уничтожение ПДн производится только в следующих случаях:

- обрабатываемые ПДн подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральными законами РФ;
- 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 достижения цели обработки ПДн;
- в случае отзыва субъектом ПДн согласия на обработку его ПДн и в случае, если сохранение ПДн более не требуется для целей обработки ПДн.

В случае отзыва субъектом ПДн согласия на обработку своих ПДн (по форме согласно Приложению № 10 к настоящему Политике) оператор ПДн обязан прекратить обработку ПДн и уничтожить ПДн в срок, **не превышающий 3-х** дней, с даты получения указанного отзыва, если иное не предусмотрено соглашением между оператором и субъектом ПДн. Об уничтожении ПДн оператор обязан уведомить субъекта ПДн.

При уничтожении ПДн необходимо:

- убедиться в необходимости уничтожения ПДн;
- убедиться в том, что уничтожаются те ПДн, которые предназначены для уничтожения;

- уничтожить ПДн подходящим способом в соответствии с настоящей Политикой или способом, указанным в соответствующем требовании или нормативном правовом акте Оператора или ФЗ РФ;
- проверить необходимость уведомления об уничтожении ПДн;
- при необходимости уведомить об уничтожении ПДн требуемых лиц.

При уничтожении ПДн применяются следующие способы:

- измельчение в бумагорезательной (бумагоуничтожительной) машине - для документов, исполненных на бумаге;
- тщательное вымарывание (с проверкой тщательности вымарывания) - для сохранения возможности обработки иных данных, зафиксированных на материальном носителе, содержавшем ПДн;
- физическое уничтожение носителей информации - физическое разрушение или физически - сильная деформация - для носителей информации на жестком магнитном диске (уничтожению подлежат внутренние жесткие диски и их микросхемы управления и контроля), CD&DVD -диски, USB- и Flash-носители (уничтожению подлежат модули и микросхемы долговременной памяти);
- стирание с помощью сертифицированных средств уничтожения информации - для записей в базах данных и отдельных документов на машинном носителе, с составлением акта уничтожения.

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 Российской Федерации.

При необходимости уничтожения части ПДн **допускается уничтожать** материальный носитель одним из указанных в настоящих Правилах способов, с предварительным копированием сведений, не подлежащих уничтожению, способом, исключающим одновременное копирование ПДн, подлежащих уничтожению.

Уничтожение носителей персональных данных производится **комиссией** по защите персональных данных, классификации и определения уровня защищенности информационных систем персональных данных в информационных системах персональных данных Администрации ЗАТО город Заозерск, состав которой утверждается постановлением Оператора, с оформлением Акта об уничтожении носителей персональных данных согласно Приложению 11 к настоящей Политике. **Уничтожение может быть произведено любым способом, полностью исключающим возможность восстановления носителя.**

Хранение актов об уничтожении носителей персональных данных осуществляется в течение срока исковой давности, если иное не установлено нормативными правовыми актами Российской Федерации, Мурманской области.

В случае отсутствия возможности уничтожения ПДн в течение сроков, указанных в настоящем подпункте, Оператор, осуществляет блокирование таких ПДн или обеспечивает их блокирование (если обработка ПДн осуществляется другим лицом, действующим по поручению Оператора) и обеспечивает уничтожение ПДн **в срок <u>не более чем 6 (шесть) месяцев</u>**, если иной срок не установлен федеральными законами РФ.

10.10. Осуществление трансграничной передачи ПДн субъекта ПНд работниками Оператора.

<u>Трансграничная передача персональных данных:</u>

10.10.1. При необходимости трансграничной передачи персональных данных на территории иностранных государств **Оператор обязан** убедиться в том, что иностранным государством, на территорию которого осуществляется передача персональных данных, обеспечивается адекватная и законодательная защита прав субъектов персональных данных, до начала осуществления трансграничной передачи персональных данных.

10.10.2. Трансграничная передача персональных данных на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных

данных, **может осуществляться в случаях:**
- наличия Согласия в письменной форме субъекта персональных данных на трансграничную передачу его персональных данных;
-предусмотренных международными договорами РФ;
- предусмотренных федеральными законами РФ, если это необходимо в целях защиты основ конституционного строя РФ, обеспечения обороны страны и безопасности государства, а также обеспечения безопасности устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, Оператора и государства в сфере транспортного комплекса от актов незаконного вмешательства;
- исполнения договора, стороной которого является субъект персональных данных;
- защиты жизни, здоровья, иных жизненно важных интересов субъекта персональных данных или других лиц при невозможности получения согласия в письменной форме субъекта персональных данных.

10.10.3. Согласно разъяснениям Минкомсвязи России от 12 августа 2015 года о применении положений ФЗ № 242 от 21 июля 2014 года передача персональных данных за пределы РФ **возможна, с соблюдением условий**, указанных в законе «О персональных данных» (в частности, при наличии согласия физического лица на трансграничную передачу его данных).

Персональные данные граждан РФ, первоначально внесенные в базу данных на территории РФ («первичная база данных») и актуализируемые в ней, могут далее передаваться в базы данных, расположенные за пределами России («вторичные базы данных»), администрируемые иными лицами, с соблюдением положений о трансграничной передаче данных. До трансграничной передачи персональных данных третьим лицам Обществу необходимо подписать с такими третьими лицами соглашение о передаче данных, получить согласие субъекта персональных данных на трансграничную передачу и в общем порядке реализовать иные меры защиты данных, предусмотренные настоящим Политикам и действующим российским законодательством.

10.10.4. Если в отношении определенного набора персональных данных уже были ранее выполнены требования ФЗ-242, повторная локализация таких персональных данных в Обществе не требуется. Если персональные данные были при сборе записаны в базу данных, расположенную на территории Российской Федерации, то впоследствии такие персональные данные могут вноситься работником (представителем) Оператора в принадлежащую ему электронную базу данных, находящуюся за пределами Российской Федерации.

10.11. Процедуры, направленные на предотвращение и выявление нарушений законодательства в отношении обработки и защиты ПДн и устранение таких последствий.

К процедурам, направленным на предотвращение и выявление нарушений законодательства в отношении обработки ПДн и устранение таких последствий, **относятся:**

- реализация мер, направленных на обеспечение выполнения оператором ПДн своих служебных обязанностей в соответствии с трудовым договором;
- обеспечение личной ответственности муниципальных служащих, служащих, замещающих должности, не отнесенные к должностям муниципальной службы структурных подразделений и управлений Администрации ЗАТО город Заозерск, сотрудников МКУ «МФЦ ЗАТО город Заозерск», действующие в интересах служебной деятельности Администрации ЗАТО город Заозерск и допущенные к обработке персональных данных;
- организация рассмотрения запросов субъектов ПДн или их представителей и ответов на такие запросы в соответствии с Правилами рассмотрения запросов субъектов персональных данных или их представителей, утверждаемыми постановлением Администрации ЗАТО город Заозерск;
- **организация внутреннего контроля** соответствия обработки ПДн требованиям к защите ПДн, установленным действующим законодательством в области ПДн и нормативными правовыми актами органов местного самоуправления ЗАТО город Заозерск в соответствии с

Правилами осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в Администрации ЗАТО город Заозерск и утверждаемыми постановлением Администрации ЗАТО город Заозерск и определена соответствующей инструкцией Оператора (приложение к Политике);

- определение порядка доступа муниципальных служащих, служащих, замещающих должности, не отнесенные к должностям муниципальной службы структурных подразделений и Управлений Администрации ЗАТО город Заозерск, сотрудников МКУ «МФЦ ЗАТО город Заозерск» действующих в интересах служебной деятельности Администрации ЗАТО город Заозерск и допущенные в помещения, в которых ведется обработка и защита ПДн;
- проведение необходимых мероприятий по обеспечению безопасности ПДн и носителей;
- проведение периодических проверок условий обработки и защиты ПДн (1 раз в 6 месяцев по состоянию на 01 декабря и 01 июля, с составлением протокола проверки (приложение к Политике);
- повышение осведомленности муниципальных служащих, служащих, замещающих должности, не отнесенные к должностям муниципальной службы структурных подразделений и управлений Администрации ЗАТО город Заозерск, сотрудников МКУ «МФЦ ЗАТО город Заозерск», действующих в интересах служебной деятельности Администрации ЗАТО город Заозерск и занимающих должности, служебные обязанности по которым предусматривают обработку ПДн либо доступ к ПДн, путем их ознакомления с требованиями действующего законодательства Российской Федерации, Мурманской области, нормативных правовых актов Российской Федерации, Мурманской области в области персональных данных (в том числе с требованиями к защите персональных данных), нормативными правовыми актами органов местного самоуправления ЗАТО город Заозерск по вопросам обработки и защиты персональных данных и конфиденциальной информации, с проблемами возникающими в Российской Федерации и в мире, связанными с вирусной активностью и нарушениями информационной и кибербезопасности, включая настоящую Политику;
- блокирование, внесение изменений и уничтожение ПДн в предусмотренных действующим законодательством в области обработки и защиты ПДн случаях;
- разъяснение прав субъекту ПДн в вопросах обработки и обеспечения безопасности их ПДн;
- по указанию Главы администрации ЗАТО город Заозерск осуществлять оказание содействия правоохранительным органам в случаях нарушений законодательства РФ в отношении обработки и защиты ПДн;
- публикация на официальном сайте органов местного самоуправления ЗАТО город Заозерск в информационно-телекоммуникационной сети «Интернет» документов, определяющих политику в отношении обработки и защиты ПДн в соответствии с требованиями действующего законодательства Российской Федерации.
- родственники и члены семей. Персональные данные работника могут быть предоставлены родственникам или членам его семьи **только с письменного разрешения самого сотрудника**. В случае развода бывшая супруга (супруг) имеют право обратиться в организацию с письменным запросом о размере заработной платы сотрудника без его согласия.
- другие организации. Сведения о работающем сотруднике или уже уволенном могут быть предоставлены другой организации только с письменного запроса на бланке организации, с приложением копии нотариально заверенного заявления согласия самого работника.
- защита персональных данных работника на электронных носителях. Все папки, содержащие персональные данные сотрудника, должны быть защищены стойким паролем.

10.12. Особый порядок сбора и обработки персональных данных Субъектов, поступающих на любой электронный адрес Оператора, в целях возможного дальнейшего трудоустройства.

-субъект ПНд самостоятельно принимает решение о предоставлении своих персональных данных и предоставляет согласие на обработку таких персональных данных свободно, своей волей и в

своем интересе. Согласие на обработку персональных данных может быть дано Субъектом ПНд путем направления персональных данных на любой электронный адрес Оператора;
-случайное, незапрашиваемое получение, хранение и иные операции с персональными данными российских граждан поступившими на любой электронный адрес Оператора, **не влечет** обязанности Оператора локализовать обработку таких персональных данных.

10.12.1. В соответствии с частью 5 статьи 18 ФЗ «О персональных данных», а также разъяснениями Минкомсвязи России от 12 августа 2015 года **о применении положений ФЗ № 242 от 21 июля 2014 года:**

- локализации подлежат только те персональные данные, которые были получены Оператором в результате осуществляемой им целенаправленной деятельности по организации сбора таких данных, **а не в результате случайного (не запращиваемого Оператором) попадания** к нему персональных данных. Случайное, ненамеренное получение, хранение и иные операции с персональными данными российских граждан **не влекут обязанности локализовать** обработку персональных данных Оператором, в связи с чем Оператор не должен предпринимать каких-либо действий в отношении персональных данных, случайно к нему попавших, в том числе в случае получения персональных данных поступивших Оператору от других юридических лиц, если такие данные представляют собой контактную информацию сотрудников или представителей таких юридических лиц, переданную в ходе осуществления ими своей законной деятельности.

- обязанность Оператора обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, считается исполненной, когда указанные действия были совершены при сборе персональных данных с использованием базы данных, находящейся на территории Российской Федерации. В связи с чем, если в отношении определенного набора персональных данных уже были ранее выполнены требования ФЗ-242, **повторная локализация таких персональных данных Оператором <u>не требуется</u>.**

10.13. Взаимодействие с уполномоченными органами в области обработки и защиты ПДн.

В соответствии с законодательством Российской Федерации в области обеспечения безопасности ПДн функции контроля и надзора за соответствием порядка обработки персональных данных требованиям действующего законодательства возлагаются на федеральные органы исполнительной власти, уполномоченные в области обеспечения безопасности, противодействия техническим разведкам и технической защиты информации, контроля и надзора в сфере информационных технологий и связи.

Взаимодействие с уполномоченными органами организуется в пределах их полномочий и компетенций:

10.13.1. С территориальными органами Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) по вопросам:

- предоставления информации, необходимой для реализации полномочий;
- осуществления проверочных и контрольных мероприятий в пределах предоставленных полномочий;
- выполнения требований об уточнении, блокировании или уничтожении недостоверных или полученных незаконным путем персональных данных;
- принятия в установленном законодательством Российской Федерации порядке мер по приостановлению или прекращению обработки персональных данных.

10.13.2. С территориальными органами ФСТЭК России по вопросам:

- предоставления информации, необходимой для реализации полномочий и осуществления проверочных и контрольных мероприятий;

- организации и проведения мероприятий, направленных на обеспечение безопасности персональных данных при их обработке в ИСПДн.

10.13.3. С территориальными органами ФСБ России по вопросам:

- предоставления информации, необходимой для реализации полномочий и осуществления проверочных и контрольных мероприятий;
- организации и обеспечения функционирования шифровальных (криптографических) средств, предназначенных для обеспечения безопасности персональных данных при их обработке в ИСПДн.

Организация взаимодействия с уполномоченными органами в области обеспечения безопасности персональных данных возлагается на оператора ПДн и осуществляется в соответствии с Правилами рассмотрения запросов субъектов персональных данных или их представителей, утвержденными постановлением Администрации ЗАТО город Заозерск.

Взаимодействие с уполномоченными органами в области защиты персональных данных регистрируется в Журнале учета обращений уполномоченного органа по защите прав субъектов персональных данных по форме согласно Приложению № 15 к настоящей Политике.

11. Ответственность должностных лиц Оператора.

Муниципальные служащие, служащие, замещающие должности, не отнесенные к должностям муниципальной службы структурных подразделений и Управлений Администрации ЗАТО город Заозерск, сотрудники МКУ «МФЦ ЗАТО город Заозерск», действующие в интересах служебной деятельности Администрации ЗАТО город Заозерск и виновные в нарушении норм, регулирующих получение, обработку и защиту ПДн, несут дисциплинарную административную, гражданско-правовую или уголовную ответственность в соответствии с действующим законодательством Российской Федерации.