РЕСПУБЛИКА ДАГЕСТАН

АДМИНИСТРАЦИЯ МУНИЦИПАЛЬНОГО РАЙОНА «БУЙНАКСКИЙ РАЙОН»

368220, РД, г. Буйнакск, ул. Ленина 61, тел.2-93-93, факс 2-92-24 e-mail:buynakskrayon@e-dag.ru

«12» октября 2018 г. № 198

П О С Т А Н О В Л Е Н И Е

Об утверждении Положения о правилах обработки и защиты персональных данных в Администрации МР «Буйнакский район»

В соответствии с Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», Постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», 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», Законом Республики Дагестан от 11.03.2008 г. № 9 «О муниципальной службе в Республике Дагестан», Администрация МР «Буйнакский район» **п о с т а н о в л я е т:**

1. Утвердить прилагаемые:

- положение об обработке и защите персональных данных в Администрации МР «Буйнакский район» (приложение 1);
- правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и локальными актами оператора (приложение 2);
- перечень должностей служащих органа местного самоуправления, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным (приложение 3);

- типовое обязательство служащего муниципального органа, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним муниципального контракта прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей (приложение 4);

- типовую форму согласия на обработку персональных данных служащих муниципального органа, иных субъектов персональных данных (приложение 5);

- типовую форму разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные (приложение 6);

- порядок доступа служащих органа местного самоуправления в помещения, в которых ведется обработка персональных данных (приложение 7);

правила рассмотрения запросов субъектов персональных данных или их представителей в Администрации МР «Буйнакский район» (приложение 8);

- инструкцию пользователя информационных систем персональных данных Администрации МР «Буйнакский район» (приложение 9);

- типовую форму журнала учета отчуждаемых машинных носителей персональных данных (приложение 10);

- типовую форму перечня помещений, в которых размещены информационные системы персональных данных Администрации МР «Буйнакский район» (приложение 11);

- инструкцию ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных Администрации МР «Буйнакский район» (приложение 12);

- форму уведомления о факте обработки персональных данных без использования средств автоматизации (приложение 13);

- типовое обязательство о соблюдении конфиденциальности персональных данных (приложение 14);

- форму ознакомления с положениями законодательства Российской Федерации о персональных данных, локальными актами Администрации МР «Буйнакский район» по вопросам обработки персональных данных (приложение 15);

- форму уведомления о получении персональных данных от третьих лиц (приложение 16);

- форму уведомления об уничтожении, изменении, прекращении обработки, устранении нарушений, допущенных при обработке персональных данных (приложение 17);

- форму акта на списание и уничтожение машинных (бумажных) носителей информации (приложение 18);

- форму журнала учета передачи персональных данных (приложение 19);

- форму журнала учета обращений субъектов персональных данных (приложение 20);

- форму журнала учета ознакомления сотрудников с порядком обработки персональных данных и изменениями в законодательстве в области защиты персональных данных (приложение 21);

- положение об организации и проведении работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Администрации МР «Буйнакский район» (приложение 22);

- порядок хранения, использования и передачи персональных данных сотрудников Администрации МР «Буйнакский район» (приложение 23).

2. Контроль за исполнением настоящего постановления возложить на заместителя Главы Администрации МР «Буйнакский район» Ахмедзияутдинова М.Т.

Врио Главы муниципального района «Буйнакский район» **А. Джафаров**

Приложение 1

УТВЕРЖДЕНО
постановлением Администрации
МР «Буйнакский район»
«12» октября 2018 г. № 198

ПОЛОЖЕНИЕ
об обработке и защите персональных данных в Администрации МР «Буйнакский район»

I. Общие положения

1.1. Положение об обработке и защите персональных данных в Администрации МР «Буйнакский район» (далее - Положение) определяет цели, содержание и порядок обработки персональных данных, меры, направленные на защиту персональных данных, а также устанавливает процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в области персональных данных в Администрации МР «Буйнакский район» (далее - Администрация).

1.2. Настоящее Положение определяет политику Администрации как оператора, осуществляющего обработку персональных данных, в отношении обработки и защиты персональных данных.

1.3. Настоящее Положение разработано в соответствии с Трудовым кодексом Российской Федерации, Кодексом Российской Федерации об административных правонарушениях (далее - КоАП РФ), Федеральным законом от 27.07.2006 года № 152-ФЗ «О персональных данных» (далее - Федеральный закон «О персональных данных»), Федеральным законом от 27.07.2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 25.12.2008 года № 273-ФЗ «О противодействии коррупции» (далее - Федеральный закон «О противодействии коррупции»), Федеральным законом от 27.07.2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» (далее - Федеральный закон «Об организации предоставления государственных и муниципальных услуг»), Федеральным законом от 02.09.2006 г. № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации» (далее - Федеральный закон «О порядке рассмотрения обращений граждан Российской Федерации»), постановлением Правительства Российской Федерации от 01.11.2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», постановлением Правительства Российской Федерации от 15.09.2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановлением Правительства

Российской Федерации от 21.03.2012 г. № 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», Законом Республики Дагестан от 11.03.2008 г. № 9 «О муниципальной службе в Республике Дагестан».

1.4. Положение определяет порядок обработки персональных данных в Администрации, раскрывает вопросы обеспечения защиты прав при обработке персональных данных, а также устанавливает ответственность лиц, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

1.5. Обработка персональных данных в Администрации осуществляется с соблюдением принципов и условий, предусмотренных законодательством Российской Федерации в области персональных данных и настоящим Положением.

II. **Термины и определения**

В настоящем Положении используются следующие термины и их определения:

Информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Конфиденциальность персональных данных - обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания, если иное не предусмотрено федеральным законом.

Межсетевой экран - локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

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

Обработка персональных данных - действия (операции) с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение 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.

Технические средства информационной системы персональных данных - средства вычислительной техники, информационно - вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы Администрации базами данных и т.п.), средства защиты информации).

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

Пользователь информационной системы персональных данных - лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Ресурс информационной системы - именованный элемент **системного, прикладного или аппаратного обеспечения функционирования информационной системы.**

Средства вычислительной техники - совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Угрозы безопасности персональных данных - совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе 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.

Уровень защищенности персональных данных - комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

Утечка (защищаемой) информации по техническим каналам - неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Целостность информации - способность средства вычислительной техники или информационной системы обеспечивать неизменность

информации в условиях случайного и/или преднамеренного искажения (разрушения).

III. Условия и порядок обработки персональных данных муниципальных служащих Администрации, граждан претендующих на замещение должностей муниципальной службы

3.1. Персональные данные муниципальных служащих Администрации, граждан, претендующих на замещение должностей муниципальной службы Администрации, обрабатываются в целях обеспечения кадровой работы, в том числе в целях содействия муниципальным служащим Администрации в прохождении муниципальной службы, формирования кадрового резерва муниципальной службы, обучения и должностного роста, учета результатов исполнения муниципальными служащими Администрации должностных обязанностей, обеспечения личной безопасности муниципальных служащих Администрации и членов их семьи, обеспечения муниципальным служащим Администрации установленных законодательством Российской Федерации условий труда, гарантий и компенсаций, сохранности принадлежащего им имущества, а также в целях противодействия коррупции.

3.2. В целях, указанных в пункте 3.1 настоящего Положения, обрабатываются следующие категории персональных данных муниципальных служащих Администрации, граждан, претендующих на замещение должностей муниципальной службы Администрации (приложение 3):

- фамилия, имя, отчество (в том числе предыдущие фамилии, имена и (или) отчества, в случае их изменения);
- число, месяц, год рождения;
- место рождения;
- информация о гражданстве (в том числе предыдущие гражданства, иные гражданства);
- вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи;
- адрес места жительства (адрес регистрации, фактического проживания);
- номер контактного телефона или сведения о других способах связи;
- реквизиты страхового свидетельства муниципального пенсионного страхования;
- идентификационный номер налогоплательщика;
- реквизиты страхового медицинского полиса обязательного медицинского страхования;
- реквизиты свидетельства регистрации актов гражданского состояния;
- семейное положение, состав семьи и сведения о близких родственниках (в том числе бывших);
- сведения о трудовой деятельности;
- сведения о воинском учете и реквизиты документов воинского учета;
- 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 об ученой степени;
- информация о владении иностранными языками, степень владения;
- медицинское заключение по установленной форме об отсутствии у гражданина заболевания, препятствующего поступлению на государственную гражданскую службу или ее прохождению;
- фотография;
- сведения о прохождении муниципальной службы, в том числе: 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;
- информация, содержащаяся в трудовом договоре, дополнительных соглашениях к трудовому договору;
- сведения о пребывании за границей;
- информация о классном чине муниципальной службы Российской Федерации (в том числе дипломатическом ранге, воинском или специальном звании, классном чине правоохранительной службы, классном чине муниципальной службы субъекта Российской Федерации);
- информация о наличии или отсутствии судимости;
- информация об оформленных допусках к государственной тайне;
- государственные награды, иные награды и знаки отличия;
- сведения о профессиональной переподготовке и (или) повышении квалификации;
- информация о ежегодных оплачиваемых отпусках, учебных отпусках и отпусках без сохранения денежного содержания;
- сведения о доходах, об имуществе и обязательствах имущественного характера;
- номер расчетного счета;
- номер банковской карты;
- иные документы, предусмотренные федеральными законами, указами Президента Российской Федерации и постановлением Правительства Российской Федерации.

3.3. Обработка персональных данных муниципальных служащих Администрации, граждан, претендующих на замещение должностей муниципальной службы Администрации, осуществляется без согласия указанных лиц в рамках целей, определенных пунктом 3.1 настоящего

Положения, в соответствии с пунктом 2 части 1 статьи 6 и частью 2 статьи 11 Федерального закона «О персональных данных» и положениями Закона Республики Дагестан «О муниципальной службе в Республике Дагестан», Федерального закона «О противодействии коррупции», Трудовым кодексом Российской Федерации.

3.4. Обработка специальных категорий персональных данных муниципальных служащих Администрации, граждан, претендующих на замещение должностей муниципальной службы Администрации, осуществляется без согласия указанных лиц в рамках целей, определенных пунктом 3.1 настоящего Положения, в соответствии с подпунктом 2.3 пункта 2 части 2 статьи 10 Федерального закона «О персональных данных» и положениями Трудового кодекса Российской Федерации, за исключением случаев получения персональных данных работника у третьей стороны.

3.5. Обработка персональных данных муниципальных служащих Администрации, граждан, претендующих на замещение должностей муниципальной службы Администрации, осуществляется при условии получения согласия указанных лиц в следующих случаях:

- при передаче (распространении, предоставлении) персональных данных третьим лицам в случаях, не предусмотренных действующим законодательством Российской Федерации о муниципальной службе;
- при трансграничной передаче персональных данных;
- при принятии решений, порождающих юридические последствия в отношении указанных лиц или иным образом затрагивающих их права и законные интересы, на основании исключительно автоматизированной обработки их персональных данных.

3.6. В случаях, предусмотренных пунктом 3.5 настоящего Положения, согласие субъекта персональных данных оформляется в письменной форме, если иное не установлено Федеральным законом «О персональных данных» (приложение 5).

3.7. Обработка персональных данных муниципальных служащих Администрации, граждан, претендующих на замещение должностей муниципальной службы Администрации, осуществляется кадровым подразделением Администрации и включает в себя следующие действия: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

3.8. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных муниципальных служащих Администрации, граждан, претендующих на замещение должностей муниципальной службы Администрации, осуществляется путем:

- получения оригиналов необходимых документов (заявление, трудовая книжка, автобиография, иные документы, предоставляемые в кадровое подразделение Администрации);
- копирования оригиналов документов;

- внесения сведений в учетные формы (на бумажных и электронных носителях);
- формирования персональных данных в ходе кадровой работы;
- внесения персональных данных в информационные системы, используемые кадровым подразделением Администрации.

3.9. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных осуществляется путем получения персональных данных непосредственно от муниципальных служащих Администрации, граждан, претендующих на замещение должностей муниципальной службы Администрации.

3.10. В случае возникновения необходимости получения персональных данных муниципального служащего Администрации у третьей стороны, следует известить об этом муниципального служащего заранее, получить его письменное согласие и сообщить ему о целях, предполагаемых источниках и способах получения персональных данных (приложение 16).

3.11. Запрещается получать, обрабатывать и приобщать к личному делу муниципального служащего Администрации персональные данные, не предусмотренные пунктом 3.2 настоящего Положения, в том числе касающиеся расовой, политических взглядов, религиозных или философских убеждений, интимной жизни.

3.12. Защита персональных данных муниципального служащего от неправомерного их использования или утраты обеспечивается работодателем за счет своих средств в порядке, установленном федеральными законами.

3.13. При сборе персональных данных сотрудник кадрового подразделения Администрации, осуществляющий сбор (получение) персональных данных непосредственно от муниципальных служащих Администрации, граждан, претендующих на замещение должностей муниципальной службы Администрации, обязан разъяснить указанным субъектам персональных данных юридические последствия отказа предоставить их персональные данные (приложение 6).

3.14. Передача (распространение, предоставление) и использование персональных данных муниципальных служащих Администрации, граждан, претендующих на замещение должностей муниципальной службы Администрации, осуществляется лишь в случаях и в порядке, предусмотренных федеральными законами (приложение 19).

3.15. Уведомить субъекта персональных данных об уничтожении, изменении, прекращении обработки, устранении нарушений, допущенных при обработке персональных данных (приложение 17).

IV. **Условия и порядок обработки персональных данных субъектов в связи с предоставлением муниципальных услуг и исполнением муниципальных функций**

4.1. В Администрации обработка персональных данных физических лиц

осуществляется в целях предоставления муниципальных услуг и исполнения муниципальных функций.

4.2. Персональные данные граждан, обратившихся в Администрации лично, а также направивших индивидуальные или коллективные письменные обращения, или обращения в форме электронного документа, обрабатываются в целях рассмотрения указанных обращений с последующим уведомлением заявителей о результатах рассмотрения.

В соответствии с законодательством Российской Федерации в Администрации подлежат рассмотрению обращения граждан Российской Федерации, иностранных граждан и лиц без гражданства.

4.3. В рамках рассмотрения обращений граждан подлежат обработке следующие персональные данные заявителей:

- фамилия, имя, отчество (последнее при наличии);
- почтовый адрес;
- адрес электронной почты;
- указанный в обращении контактный телефон;
- иные персональные данные, указанные заявителем в обращении (жалобе), а также ставшие известными в ходе личного приема или в процессе рассмотрения поступившего обращения.

4.4. В рамках осуществления деятельности по защите прав субъектов персональных данных осуществляется обработка следующих персональных данных заявителей:

- фамилия, имя, отчество (последнее при наличии);
- вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи;
- почтовый адрес места жительства;
- адрес электронной почты;
- номер телефона;
- идентификационный номер налогоплательщика;
- сведения о трудовой деятельности и реквизиты трудовой книжки;
- 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).

4.5. Обработка персональных данных, необходимых в связи с предоставлением муниципальных услуг и исполнением муниципальных функций, осуществляется без согласия субъектов персональных данных в соответствии с пунктом 4 части 1 статьи 6 Федерального закона «О персональных данных», Федеральными законами «Об организации предоставления муниципальных и муниципальных услуг», «О порядке рассмотрения обращений граждан Российской Федерации» и иными нормативными правовыми актами, определяющими предоставление муниципальных услуг и исполнение муниципальных функций в установленной

сфере ведения Администрации.

4.6. Обработка персональных данных, необходимых в связи с предоставлением муниципальных услуг и исполнением муниципальных функций осуществляется структурными подразделениями Администрации, предоставляющими соответствующие муниципальные услуги и (или) исполняющими муниципальные функции, и включает в себя следующие действия: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

4.7. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных субъектов, обратившихся в Администрацию для получения муниципальной услуги или в целях исполнения муниципальной функции, осуществляется путем:

- получения оригиналов необходимых документов (заявление);
- заверения копий документов;
- внесения сведений в учетные формы (на бумажных и электронных носителях);
- внесения персональных данных в прикладные программные подсистемы Единой информационной системы Администрации.

4.8. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных осуществляется путем получения персональных данных непосредственно от субъектов персональных данных (заявителей).

4.9. При предоставлении муниципальной услуги или исполнении муниципальной функции Администрацией запрещается запрашивать у субъектов персональных данных и третьих лиц, а также обрабатывать персональные данные в случаях, не предусмотренных законодательством Российской Федерации.

4.10. При сборе персональных данных уполномоченное должностное лицо структурного подразделения Администрации, осуществляющее получение персональных данных непосредственно от субъектов персональных данных, обратившихся за предоставлением муниципальной услуги или в связи с исполнением муниципальной функции, обязано разъяснить указанным субъектам персональных данных юридические последствия отказа предоставить персональные данные (приложение 6).

4.11. В случае расторжения служебного контракта о прохождении муниципальной службы в Администрации МР «Буйнакский район», служащим которые непосредственно осуществляли обработку персональных данных, необходимо прекратить обработку персональных данных, ставших известными им в связи с исполнением должностных обязанностей (приложение 4).

4.12. Передача (распространение, предоставление) и использование персональных данных заявителей (субъектов персональных данных) Администрацией осуществляется лишь в случаях и в порядке, предусмотренных федеральными законами.

V. **Порядок обработки персональных данных субъектов персональных данных в информационных системах**

5.1. Обработка персональных данных в Администрации осуществляется:
- в информационных системах персональных данных Администрации;
- на аттестованных под обработку персональных данных автоматизированных рабочих местах, входящих в состав Информационных систем Администрации;
- в информационных системах «1С: Зарплата и кадры»;
- на автоматизированных рабочих местах сотрудников кадрового подразделения Администрации.

5.2. Информационные системы персональных данных Администрации (далее - ИСПДн Администрации) содержит персональные данные муниципальных служащих Администрации, субъектов (заявителей), обратившихся в Администрацию в целях получения муниципальных услуг или в связи с исполнением муниципальных функций, и включает:
- персональный идентификатор;
- фамилию, имя, отчество субъекта персональных данных;
- вид документа, удостоверяющего личность субъекта персональных данных;
- серию и номер документа, удостоверяющего личность субъекта персональных данных, сведения о дате выдачи указанного документа и выдавшем его органе;
- адрес места жительства субъекта персональных данных;
- почтовый адрес субъекта персональных данных;
- контактный телефон, факс (при наличии) субъекта персональных данных;
- адрес электронной почты субъекта персональных данных;
- ИНН субъекта персональных данных.

5.3. Аттестованные в соответствии с законодательством Российской Федерации под обработку персональных данных автоматизированные рабочие места, входящие в состав Информационных систем Администрации (далее - АРМ ИС Администрации), включают персональные данные субъектов, получаемые сотрудниками Администрации в рамках предоставления муниципальных услуг и исполнения муниципальных функций, и включают:
- персональный идентификатор;
- адрес места жительства субъекта персональных данных;
- почтовый адрес субъекта персональных данных;
- телефон субъекта персональных данных;
- факс субъекта персональных данных;
- адрес электронной почты субъекта персональных данных.

5.4. Информационная система «1С: Зарплата и кадры», содержит персональные данные муниципальных служащих Администрации и физических лиц, являющихся стороной гражданско-правовых договоров, заключаемых Администрацией, и включает:

- фамилию, имя, отчество субъекта персональных данных;
- дату рождения субъекта персональных данных;
- место рождения субъекта персональных данных;
- серию и номер основного документа, удостоверяющего личность субъекта персональных данных, сведения о дате выдачи указанного документа и выдавшем его органе;
- адрес места жительства субъекта персональных данных;
- почтовый адрес субъекта персональных данных;
- телефон субъекта персональных данных;
- ИНН субъекта персональных данных;
- табельный номер субъекта персональных данных;
- должность субъекта персональных данных;
- номер приказа и дату приема на работу (увольнения) субъекта персональных данных.

5.5. Автоматизированные рабочие места сотрудников кадрового подразделения Администрации предполагают обработку персональных данных муниципальных служащих Администрации, предусмотренных пунктом 3.2 настоящего Положения.

5.6. Классификация информационных систем персональных данных, указанных в пункте 5.1 настоящего Положения, осуществляется в порядке, установленном законодательством Российской Федерации.

5.7. Муниципальным служащим структурных подразделений Администрации, имеющим право осуществлять обработку персональных данных в информационных системах Администрации, предоставляется уникальный логин и пароль для доступа к соответствующей информационной системе Администрации. Доступ предоставляется к прикладным программным подсистемам в соответствии с функциями, предусмотренными должностными регламентами муниципальных служащих Администрации.

Информация может вноситься как в автоматическом режиме, при получении персональных данных с Единого портала муниципальных услуг или официального сайта Администрации, так и в ручном режиме, при получении информации на бумажном носителе или в ином виде, не позволяющем осуществлять ее автоматическую регистрацию.

5.8. Обеспечение безопасности персональных данных, обрабатываемых в информационных системах персональных данных Администрации, достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, а также принятия следующих мер по обеспечению безопасности:

- определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных Администрации;
- применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Администрации,

необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных (приложение 22);

- применение прошедших в установленном порядке процедур оценки соответствия средств защиты информации;
- оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
- учет машинных носителей персональных данных (приложение 10);
- своевременное обнаружение фактов несанкционированного доступа к персональным данным и принятие мер;
- восстановление персональных данных, модифицированных или удаленных, уничтоженных вследствие несанкционированного доступа к ним;
- установление правил доступа к персональным данным, обрабатываемым в информационных системах персональных данных Администрации, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационных системах персональных данных Администрации;
- контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровней защищенности информационных систем персональных данных.

5.9. Структурное подразделение Администрации, ответственное за обеспечение информационной безопасности в Администрации, организует и контролирует ведение учета материальных носителей персональных данных.

5.10. Структурное подразделение Администрации, ответственное за обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных Администрации, должно обеспечить:

- своевременное обнаружение фактов несанкционированного доступа к персональным данным и немедленное доведение этой информации до ответственного за организацию обработки персональных данных в Администрации и руководителя Администрации;
- недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;
- возможность восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- постоянный контроль за обеспечением уровня защищенности персональных данных;
- знание и соблюдение условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

- учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;
- при обнаружении нарушений порядка предоставления персональных данных незамедлительное приостановление предоставления персональных данных пользователям информационной системы персональных данных до выявления причин нарушений и устранения этих причин;
- разбирательство и составление заключений по фактам несоблюдения условий хранения материальных носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений.

5.11. Структурное подразделение Администрации, ответственное за обеспечение функционирования информационных систем персональных данных в Администрации, принимает все необходимые меры по восстановлению персональных данных, модифицированных или удаленных, уничтоженных вследствие несанкционированного доступа к ним.

5.12. Обмен персональными данными при их обработке в информационных системах персональных данных Администрации осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и путем применения программных и технических средств.

5.13. Доступ муниципальных служащих Администрации к персональным данным, находящимся в информационных системах персональных данных Администрации, предусматривает обязательное прохождение процедуры идентификации и аутентификации.

5.14. В случае выявления нарушений порядка обработки персональных данных в информационных системах персональных данных Администрации уполномоченными должностными лицами незамедлительно принимаются меры по установлению причин нарушений и их устранению.

VI. **Обработка персональных данных в рамках межведомственного информационного взаимодействия с применением единой системы межведомственного электронного взаимодействия**

6.1. Администрация в соответствии с законодательством Российской Федерации осуществляет обработку персональных данных в рамках межведомственного электронного информационного взаимодействия в электронном виде с органами муниципальной власти с применением единой системы межведомственного электронного взаимодействия (далее - СМЭВ).

6.2. Администрация в рамках СМЭВ на основании поступивших межведомственных запросов направляет информацию, включающую

персональные данные субъектов, обрабатываемые в Администрации.

VII. **Сроки обработки и хранения персональных данных**

7.1. Сроки обработки и хранения персональных данных муниципальных служащих Администрации, граждан, претендующих на замещение должностей муниципальной службы Администрации, определяются в соответствии с законодательством Российской Федерации. С учетом положений законодательства Российской Федерации, устанавливаются следующие сроки обработки и хранения персональных данных муниципальных служащих:

- персональные данные, содержащиеся в приказах по личному составу муниципальных служащих Администрации (о приеме, о переводе, об увольнении, об установлении надбавок), подлежат хранению в кадровом подразделении Администрации в течение десяти лет, с последующим формированием и передачей в установленном порядке указанных документов в ведомственный архив Администрации МР «Буйнакский район», где хранятся в течение 75 лет (при ликвидации без правопреемника документы по личному составу в упорядоченном состоянии поступают в муниципальный архив);
- персональные данные, содержащиеся в приказах по личному составу о поощрениях, материальной помощи муниципальным служащим Администрации;
- персональные данные, содержащиеся в приказах о поощрениях, материальной помощи муниципальным служащим Администрации, о предоставлении отпусков, о краткосрочных командировках, о дисциплинарных взысканиях муниципальных служащих Администрации, подлежат хранению в кадровом подразделении Администрации в течение пяти лет с последующим уничтожением;
- персональные данные, содержащиеся в документах претендентов на замещение вакантной должности муниципальной службы в Администрации, не допущенных к участию в конкурсе, и кандидатов, участвовавших в конкурсе, хранятся в кадровом подразделении Администрации в течение трех лет со дня завершения конкурса, после чего подлежат уничтожению.

7.2. Сроки обработки и хранения персональных данных, предоставляемых субъектами персональных данных в Администрация в связи с получением муниципальных услуг и исполнением муниципальных функций, указанных в пункте 4.1 настоящего Положения, определяются нормативными правовыми актами, регламентирующими порядок их сбора и обработки.

7.3. Персональные данные граждан, обратившихся в Администрацию лично, а также направивших индивидуальные или коллективные письменные обращения, или обращения в форме электронного документооборота, хранятся в течение сроков, предусмотренных статьей 183 перечня типовых управленческих архивных документов, образующихся в процессе деятельности Государственных органов, органов местного самоуправления и организаций,

с указанием сроков хранения, утвержденного Приказом Министерства Культуры РФ от 25.08.2010 № 558.

7.4. Персональные данные, предоставляемые субъектами на бумажном носителе в связи с предоставлением Администрацией муниципальных услуг и исполнением муниципальных функций, хранятся на бумажных носителях в структурных подразделениях Администрации, к полномочиям которых относится обработка персональных данных в связи с предоставлением муниципальной услуги или исполнением муниципальной функции, в соответствии с утвержденными положениями о соответствующих структурных подразделениях Администрации.

7.5. Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на разных материальных носителях персональных данных, в специальных разделах или на полях форм (бланков) (приложение 13).

7.6. Необходимо обеспечивать раздельное хранение персональных данных на разных материальных носителях, обработка которых осуществляется в различных целях, определенных настоящим Положением.

7.7. Контроль за хранением и использованием материальных носителей персональных данных, не допускающий несанкционированное использование, уточнение, распространение и уничтожение персональных данных, находящихся на этих носителях, осуществляют руководители структурных подразделений Администрации.

7.8. Срок хранения персональных данных, внесенных в информационные системы персональных данных Администрации, указанные в пункте 5.1 настоящего Положения, должен соответствовать сроку хранения бумажных оригиналов.

VIII. **Порядок уничтожения персональных данных при достижении целей обработки или при наступлении иных законных оснований**

8.1. Структурным подразделением Администрации, ответственным за документооборот и архивирование, осуществляется систематический контроль и выделение документов, содержащих персональные данные, с истекшими сроками хранения, подлежащих уничтожению.

8.2. Вопрос об уничтожении выделенных документов, содержащих персональные данные, рассматривается на заседании Центральной экспертной комиссии Администрации (далее - ЦЭК Администрации), состав которой утверждается распоряжением Администрации.

По итогам заседания составляются протокол и Акт о выделении к уничтожению документов, опись уничтожаемых дел, проверяется их комплектность, акт подписывается председателем и членами ЦЭК Администрации и утверждается руководителем Администрации.

8.3. Администрацией в порядке, установленном законодательством

Российской Федерации, определяется подрядная организация, имеющая необходимую производственную базу для обеспечения установленного порядка уничтожения документов. Должностное лицо Администрации, ответственное за архивную деятельность, сопровождает документы, содержащие персональные данные, до производственной базы подрядчика и присутствует при процедуре уничтожения документов (сжигание или химическое уничтожение).

8.4. По окончании процедуры уничтожения подрядчиком и должностным лицом Администрации, ответственным за архивную деятельность, составляется соответствующий Акт об уничтожении документов, содержащих персональные данные (приложение 18).

8.5. Уничтожение по окончании срока обработки персональных данных на электронных носителях производится путем механического нарушения целостности носителя, не позволяющего произвести считывание или восстановление персональных данных, или удалением с электронных носителей методами и средствами гарантированного удаления остаточной информации.

IX. **Рассмотрение запросов субъектов персональных данных или их представителей**

9.1. Муниципальные служащие Администрации, граждане, претендующие на замещение должностей муниципальной службы Администрации и подавшие документы на участие в конкурсе, и лица, состоящих с ними в родстве (свойстве), а также граждане, персональные данные которых обрабатываются в Администрации в связи с предоставлением муниципальных услуг и осуществлением муниципальных функций, имеют право на получение информации, касающейся обработки их персональных данных, в том числе содержащей (приложение 8):

- подтверждение факта обработки персональных данных в Администрации;
- правовые основания и цели обработки персональных данных;
- применяемые в Администрации способы обработки персональных данных;
- наименование и место нахождения Администрации, сведения о лицах (за исключением муниципальных служащих Администрации), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Администрацией 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 в Администрации;

- порядок осуществления субъектом персональных данных прав, предусмотренных законодательством Российской Федерации в области персональных данных;
- информацию об осуществленной или предполагаемой трансграничной передаче данных;
- наименование организации или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Администрации, если обработка поручена или будет поручена такой организации или лицу;
- иные сведения, предусмотренные законодательством Российской Федерации в области персональных данных.

9.2. Лица, указанные в пункте 9.1 настоящего Положения (далее - субъекты персональных данных), вправе требовать от Администрации уточнения их 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.

9.3. Сведения, указанные в пункте 9.1 настоящего Положения, должны быть предоставлены субъекту персональных данных оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

9.4. Сведения, указанные в пункте 9.1 настоящего Положения, предоставляются субъекту персональных данных или его представителю уполномоченным должностным лицом структурного подразделения Администрации, осуществляющего обработку соответствующих персональных данных при обращении либо при получении запроса субъекта персональных данных или его представителя. Запрос должен содержать:

- номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе;
- сведения, подтверждающие участие субъекта персональных данных в правоотношениях с Администрацией (документ, подтверждающий прием документов на участие в конкурсе на замещение вакантных должностей муниципальной службы, оказание Администрацией муниципальной услуги или осуществление муниципальной функции), либо сведения, иным образом подтверждающие факт обработки персональных данных в Администрации, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

9.5. В случае, если сведения, указанные в пункте 9.1 настоящего Положения, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его

запросу, субъект персональных данных вправе обратиться повторно в Администрацию или направить повторный запрос в целях получения указанных сведений и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

9.6. Субъект персональных данных вправе обратиться повторно в Администрацию или направить повторный запрос в целях получения сведений, указанных в пункте 8.1 настоящего Положения, а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в пункте 9.5 настоящего Положения, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в пункте 9.4 настоящего Положения, должен содержать обоснование направления повторного запроса.

9.7. Администрация (уполномоченное должностное лицо Администрации) вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным пунктами 9.5 и 9.6 настоящего Положения. Такой отказ должен быть мотивированным.

9.8. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами, в том числе, если доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц.

X. **Лицо, ответственное за организацию обработки персональных данных в Администрации**

10.1. Ответственный за организацию обработки персональных данных в Администрации (далее - Ответственный за обработку персональных данных в Администрации) назначается Главой Администрации из числа муниципальных служащих, относящихся к ведущей или главной группе должностей Администрации в соответствии с распределением обязанностей.

10.2. Ответственный за обработку персональных данных Администрации в своей работе руководствуется законодательством Российской Федерации в области персональных данных и настоящим Положением (приложение 15).

10.3. Ответственный за обработку персональных данных Администрации обязан:

- организовывать принятие правовых, организационных и технических мер для обеспечения защиты персональных данных, обрабатываемых в Администрации от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления,

распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных;

- осуществлять внутренний контроль за соблюдением муниципальными служащими Администрации требований законодательства Российской Федерации в области персональных данных, в том числе требований к защите персональных данных;
- доводить до сведения муниципальных служащих Администрации положения законодательства Российской Федерации в области персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных (приложение 21), (приложение 12);
- организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей, а также осуществлять контроль за приемом и обработкой таких обращений и запросов в Администрации (приложение 20);
- в случае нарушения в Администрации требований к защите персональных данных принимать необходимые меры по восстановлению нарушенных прав субъектов персональных данных.

10.4. Ответственный за обработку персональных данных вправе:

10.4.1. иметь доступ к информации, касающейся обработки персональных данных в Администрации и включающей:

- цели обработки персональных данных;
- категории обрабатываемых персональных данных;
- категории субъектов, персональные данные которых обрабатываются;
- правовые основания обработки персональных данных;
- перечень действий с персональными данными, общее описание используемых в Администрации способов обработки персональных данных;
- описание мер, предусмотренных статьями 18.1 и 19 Федерального закона «О персональных данных», в том числе сведения о наличии шифровальных (криптографических) средств и наименования этих средств;
- дату начала обработки персональных данных;
- срок или условия прекращения обработки персональных данных;
- сведения о наличии или об отсутствии трансграничной передачи персональных данных в процессе их обработки;
- сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных, установленными Правительством Российской Федерации;

10.4.2. Привлекать к реализации мер, направленных на обеспечение безопасности персональных данных, обрабатываемых в Администрации, иных муниципальных служащих Администрации с возложением на них соответствующих обязанностей и закреплением ответственности.

10.5. Ответственный за обработку персональных данных

в Администрации несет ответственность за надлежащее выполнение возложенных функций по организации обработки персональных данных в Администрации в соответствии с положениями законодательства Российской Федерации в области персональных данных.

10.6. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных муниципальных служащих, несут ответственность в соответствии с действующим законодательством.

Приложение 7

Приложение 2

УТВЕРЖДЕНО
постановлением Администрации
МР «Буйнакский район»
«12» октября 2018 г. № 198

ПРАВИЛА
осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в Администрации МР «Буйнакский район»

1. Настоящие Правила определяют порядок осуществления внутреннего контроля за соблюдением Администрацией и его сотрудниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных.

2. Внутренний контроль организуется лицом, ответственным за организацию обработки персональных данных в Администрации, который назначается руководителем Администрации из числа муниципальных служащих, относящихся к ведущей или главной группе должностей Администрации, в соответствии с распределением обязанностей.
3. Внутренний контроль соответствия обработки персональных данных требованиям законодательства Российской Федерации и локальных актов Администрации осуществляется путём проведения соответствующих проверок не реже 2 (двух) раз в год.

4. При осуществлении внутреннего контроля соответствия обработки персональных данных требованиям действующего законодательства производится проверка:

- соблюдения принципов обработки персональных данных в Администрации;

- выполнения муниципальными служащими Администрации требований и правил обработки персональных данных в информационных системах персональных данных Администрации;

- перечней персональных данных, обрабатываемых в Администрации в связи с реализацией служебных и трудовых отношений, а также в связи с оказанием муниципальных услуг и осуществлением муниципальных функций;

- актуальности содержащихся в Правилах обработки персональных данных

в каждой информационной системе персональных данных Администрации информации о законности целей обработки персональных данных и оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных;

- правильность осуществления сбора, систематизации, сбора, записи, систематизации, накопления, хранения, уточнения (обновления, изменения), извлечения, использования, передачи (распространения, предоставления, доступа), обезличивания, блокирования, удаления, уничтожения персональных данных в каждой информационной системе персональных данных Администрации;

- актуальности перечня должностей муниципальной службы Администрации, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным;

- актуальности перечня должностей муниципальной службы Администрации, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных;

- соблюдения прав субъектов персональных данных, чьи персональные данные обрабатываются в информационных системах персональных данных Администрации;

- порядка взаимодействия с субъектами персональных данных, чьи персональные данные обрабатываются в информационных системах персональных данных Администрации, в том числе соблюдения сроков, предусмотренных действующим законодательством в области персональных данных, соблюдения требований по уведомлениям, порядка разъяснения субъектам персональных данных необходимой информации, порядка реагирования на обращения субъектов персональных данных, порядка действий при достижении целей обработки персональных данных и отзыве согласий субъектами персональных данных;

- наличия необходимых согласий субъектов персональных данных, чьи персональные данные обрабатываются в информационных системах персональных данных Администрации;

- актуальности сведений, содержащихся в уведомлении Администрации об обработке персональных данных;

- актуальности перечня информационных систем персональных данных в Администрации;

- знания и соблюдения муниципальными служащими Администрации положений действующего законодательства Российской Федерации в области персональных данных;

- знания и соблюдения муниципальными служащими Администрации положений локальных актов Администрации в области обработки и обеспечения безопасности персональных данных;

- знания и соблюдения муниципальными служащими Администрации руководств и иных эксплуатационных документов на применяемые средства автоматизации, в том числе программное обеспечение, и средства защиты информации;

- соблюдения муниципальными служащими Администрации конфиденциальности персональных данных (приложение 14);

- соблюдения муниципальными служащими Администрации требований по обеспечению безопасности персональных данных.

5. Лицо, ответственное за организацию обработки персональных данных в Администрации, при проведении проверки вправе иметь доступ к информации, касающейся обработки персональных данных Администрации и включающей:

- цели обработки персональных данных;
- категории обрабатываемых персональных данных;
- категории субъектов, персональные данные которых обрабатываются;
- правовые основания обработки персональных данных;
- перечень действий с персональными данными, общее описание используемых Администрацией способов обработки персональных данных;
- описание мер, предусмотренных статьями 18.1 и 19 Федерального закона «О персональных данных», в том числе сведения о наличии шифровальных (криптографических) средств и наименования этих средств;
- дату начала обработки персональных данных;
- срок или условия прекращения обработки персональных данных;
- сведения о наличии или об отсутствии трансграничной передачи персональных данных в процессе их обработки;
- сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных, установленными Правительством Российской Федерации;

6. Лицо, ответственное за организацию обработки персональных данных в Администрации, при проведении проверки обязано:

- осуществлять внутренний контроль за соблюдением сотрудниками Администрации требований законодательства Российской Федерации в области персональных данных, в том числе требований к защите персональных данных;
- доводить до сведения сотрудников Администрации положения законодательства Российской Федерации в области персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;
- организовывать прием и обработку обращений и запросов субъектов

персональных данных или их представителей, а также осуществлять контроль за приемом и обработкой таких обращений и запросов в Администрации.

7. Сотрудники Администрации обязаны обеспечить необходимые условия для проведения проверки, обеспечив доступ к оборудованию, в помещения, где осуществляется обработка персональных данных, предоставить необходимую информацию и документы для достижения целей проверки.

8. По результатам проверки составляется акт проверки, который предоставляется руководителю Администрации для рассмотрения и в случае необходимости принятия мер ответственности к лицам, допустившим нарушения требований в области персональных данных.

В акте отражаются сведения о результатах проверки, в том числе о выявленных нарушениях обязательных требований законодательства Российской Федерации, локальных актов в области персональных данных, об их характере и о лицах, допустивших нарушения.

Приложение 3

УТВЕРЖДЕНО
постановлением Администрации
МР «Буйнакский район»
«12» октября 2018 г. № 198

ПЕРЕЧЕНЬ
должностей муниципальных служащих Администрации МР «Буйнакский район», замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным

Должностное лицо	Цель обработки	Категории персональных данных
Глава МР «Буйнакский район»	Организация деятельности Администрации	Персональные данные муниципальных служащих Администрации: фамилия, имя, отчество (в том числе предыдущие фамилии, имена и (или) отчества, в случае их изменения); число, месяц, год рождения; место рождения; информация о гражданстве (в том числе предыдущие гражданства, иные гражданства); вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи; адрес места жительства (адрес регистрации, фактического проживания); номер контактного телефона или сведения о других способах связи; реквизиты страхового свидетельства государственного пенсионного страхования; идентификационный номер налогоплательщика; реквизиты страхового медицинского полиса обязательного медицинского страхования; реквизиты свидетельства государственной регистрации актов гражданского состояния; семейное положение, состав семьи и сведения о близких родственниках (в том числе бывших); сведения о трудовой деятельности; сведения о воинском учете и реквизиты документов воинского учета; 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 об ученой степени; информация о владении иностранными языками, степень владения; медицинское заключение по установленной форме об отсутствии у гражданина заболевания, препятствующего поступлению на муниципальную службу или ее прохождению; фотография; сведения о прохождении муниципальной службы, в том числе: 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; информация, содержащаяся в служебном контракте, дополнительных соглашениях к служебному контракту; сведения о пребывании за границей; информация о классном чине муниципальной службы Российской Федерации (в том числе дипломатическом ранге, воинском или специальном звании, классном чине правоохранительной службы, классном чине муниципальной службы субъекта Российской Федерации), квалификационном разряде муниципальной службы (квалификационном разряде или классном чине муниципальной службы); информация о наличии или отсутствии судимости; информация об оформленных допусках к государственной тайне; государственные награды, иные награды и

		знаки отличия; сведения о профессиональной переподготовке и (или) повышении квалификации; информация о ежегодных оплачиваемых отпусках, учебных отпусках и отпусках без сохранения денежного содержания; сведения о доходах, об имуществе и обязательствах имущественного характера; номер расчетного счета; номер банковской карты.
Заместители Главы Администрации курируемых структурных подразделений	Организация деятельности подчинённых структурных подразделений (отделов)	Персональные данные государственных гражданских служащих Управления: фамилия, имя, отчество (в том числе предыдущие фамилии, имена и (или) отчества, в случае их изменения); число, месяц, год рождения; место рождения; информация о гражданстве (в том числе предыдущие гражданства, иные гражданства); вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи; адрес места жительства (адрес регистрации, фактического проживания); номер контактного телефона или сведения о других способах связи; семейное положение, состав семьи и сведения о близких родственниках (в том числе бывших); сведения о трудовой деятельности; сведения о воинском учете; сведения об образовании, в том числе о послевузовском профессиональном образовании (наименование и год окончания образовательного учреждения, квалификация, специальность по документу об образовании); сведения об ученой степени; информация о владении иностранными языками, степень владения; сведения о прохождении муниципальной службы, в том числе: 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; информация, содержащаяся в служебном контракте, дополнительных соглашениях к служебному контракту; информация о классном чине муниципальной службы Российской Федерации (в том числе дипломатическом ранге, воинском или специальном звании, классном чине правоохранительной службы, классном чине гражданской службы субъекта Российской Федерации), квалификационном разряде муниципальной службы (квалификационном разряде или классном чине муниципальной службы); информация о наличии или отсутствии судимости; информация об оформленных допусках к государственной тайне; государственные награды, иные награды и знаки отличия; сведения о профессиональной переподготовке и(или) повышении квалификации; информация о ежегодных оплачиваемых отпусках, учебных отпусках и отпусках без сохранения денежного содержания; сведения о доходах, об имуществе и обязательствах имущественного характера.
Главный бухгалтер (начальник Отдела бухгалтерского учета и отчетности)	Ведение бухгалтерского учета и отчетности расчеты с подотчетными лицами, кассовые операции	Персональные данные муниципальных служащих Администрации: фамилия, имя, отчество (в том числе предыдущие фамилии, имена и (или) отчества, в случае их изменения); число, месяц, год рождения; место рождения; информация о гражданстве; вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи; адрес места жительства (адрес регистрации); реквизиты страхового свидетельства государственного пенсионного страхования;

		идентификационный номер налогоплательщика; семейное положение, состав семьи и сведения о близких родственниках (в том числе бывших); сведения о прохождении муниципальной службы, в том числе: 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; информация, содержащаяся в служебном контракте, дополнительных соглашениях к служебному контракту; сведения о пребывании за границей; информация о классном чине муниципальной службы Российской Федерации (в том числе дипломатическом ранге, воинском или специальном звании, классном чине правоохранительной службы, классном чине гражданской службы субъекта Российской Федерации), квалификационном разряде муниципальной службы (квалификационном разряде или классном чине муниципальной службы); информация об оформленных допусках к государственной тайне; сведения о профессиональной переподготовке и (или) повышении квалификации; информация о ежегодных оплачиваемых отпусках, учебных отпусках и отпусках без сохранения денежного содержания; сведения о доходах; номер расчетного счета; номер банковской карты.

Отдел правового и кадрового обеспечения	Сопровождение и поддержание в рабочем состоянии программ по кадрам	Персональные данные муниципальных служащих Администрации: фамилия, имя, отчество (в том числе предыдущие фамилии, имена и (или) отчества, в случае их изменения); число, месяц, год рождения; место рождения; информация о гражданстве; вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи; адрес места жительства (адрес регистрации); реквизиты страхового свидетельства государственного пенсионного страхования; идентификационный номер налогоплательщика; семейное положение, состав семьи и сведения о близких родственниках (в том числе бывших); сведения о прохождении муниципальной службы, в том числе: 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; информация, содержащаяся в служебном контракте, дополнительных соглашениях к служебному контракту; сведения о пребывании за границей; информация о классном чине муниципальной службы Российской Федерации (в том числе дипломатическом ранге, воинском или специальном звании, классном чине правоохранительной службы, классном чине гражданской службы субъекта Российской Федерации), квалификационном разряде муниципальной службы (квалификационном разряде или классном чине муниципальной службы); информация об оформленных допусках к государственной тайне; сведения о профессиональной переподготовке

		и (или) повышении квалификации; информация о ежегодных оплачиваемых отпусках, учебных отпусках и отпусках без сохранения денежного содержания; сведения о доходах; номер расчетного счета; номер банковской карты.
Руководители курируемых структурных подразделений Администрации	Организация деятельности возглавляемых структурных подразделений	Персональные данные муниципальных служащих Администрации: фамилия, имя, отчество; число, месяц, год рождения; место рождения; информация о гражданстве (в том числе предыдущие гражданства, иные гражданства); вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи; адрес места жительства (адрес регистрации, фактического проживания); номер контактного телефона или сведения о других способах связи; сведения о трудовой деятельности; сведения о воинском учете; сведения об образовании, в том числе о послевузовском профессиональном образовании (наименование и год окончания образовательного учреждения, квалификация, специальность по документу об образовании); сведения о прохождении муниципальной службы, в том числе: 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; сведения о пребывании за границей; информация о классном чине муниципальной службы Российской Федерации (в том числе дипломатическом ранге, воинском или специальном звании, классном чине правоохранительной службы, классном чине гражданской службы субъекта Российской Федерации),

		квалификационном разряде муниципальной службы (квалификационном разряде или классном чине муниципальной службы); информация о наличии или отсутствии судимости; информация об оформленных допусках к государственной тайне; государственные награды, иные награды и знаки отличия; сведения о профессиональной переподготовке и(или) повышении квалификации; информация о ежегодных оплачиваемых отпусках, учебных отпусках и отпусках без сохранения денежного содержания.
Глава МР «Буйнакский район», заместители Главы Администрации, начальники управлений и отделов Администрации	Рассмотрение, учет и контроль за рассмотрением обращений граждан	Персональные данные заявителей: фамилия, имя, отчество (последнее при наличии); почтовый адрес; адрес электронной почты; указанный в обращении контактный телефон; иные персональные данные, указанные заявителем в обращении (жалобе), а также ставшие известными в ходе личного приема или в процессе рассмотрения поступившего обращения.

Приложение 4

УТВЕРЖДЕНО
постановлением Администрации
МР «Буйнакский район»
«12» октября 2018 г. № 198

Главе МР «Буйнакский район»
ул. Ленина,61 д. 2 г. Буйнакск,
368220
от _____

Обязательство муниципального служащего, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним служебного контракта прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей

В связи с расторжением служебного контракта о прохождении муниципальной службы в Администрации МР «Буйнакский район»
в должности муниципальной службы

_____
(должность, наименование структурного подразделения)

я, _____
(Ф.И.О. муниципального служащего)

обязуюсь прекратить обработку персональных данных, ставших известными мне в связи с исполнением должностных обязанностей.

Я предупрежден (а), что в случае нарушения данного обязательства буду привлечен(а) к ответственности в соответствии с действующим законодательством Российской Федерации.

Настоящее обязательство действует с момента его подписания в течение 2 лет со дня расторжения со мной служебного контракта.

Согласен(а) на хранение содержащихся в настоящем Обязательстве моих персональных данных в Администрации МР «Буйнакский район» в течение 2 лет со дня подписания настоящего обязательства*.

_____ _____
(ФИО) (подпись)
«____»_____ 20____ г.

*Настоящее Обязательство хранится в Отделе правового и кадрового обеспечения Администрации в течение двух лет со дня его подписания.

Приложение 5

УТВЕРЖДЕНО
постановлением Администрации
МР «Буйнакский район»
«12» октября 2018 г. № 198

ТИПОВАЯ ФОРМА
Согласия муниципального служащего на обработку персональных данных, на поручение обработки персональных данных третьим лицам и на включение персональных данных в общедоступные источники персональных

Я, _____
(фамилия, имя, отчество)
проживающий (ая) по адресу: _____
паспорт серии _____ № _____, выдан _____
_____
дата выдачи «____»_____ _____г.

свободно, своей волей и в своем интересе в соответствии с требованиями Федерального закона от 27.07.2006 г. № 152 «О персональных данных» даю согласие уполномоченным должностным лицам **Администрации МР «Буйнакский район»**, расположенной по адресу: 368220, Республика Дагестан, г. Буйнакск, ул. Ленина, 61 (далее - Оператор) на обработку (любое действие (операцию) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (предоставление, доступ), обезличивание, блокирование, удаление, уничтожение) Оператором следующих персональных данных:

ФИО; сведения о смене ФИО; дата рождения; место рождения; пол; гражданство; сведения об изменении гражданства; сведения о наличии гражданства другого государства; адрес регистрации; адрес проживания; контактные телефоны; контактные телефоны (или иной вид связи); данные документа, удостоверяющего личность; наименование органа, выдавшего документ, удостоверяющий личность; дата выдачи документа, удостоверяющего личность; данные заграничного паспорта; банковские реквизиты; ИНН; СНИЛС; сведения об образовании; направление подготовки или специальность по документу об образовании; квалификация по документу об образовании; сведения о послевузовском профессиональном образовании; должность; сведения о замещаемой должности; стаж работы; сведения о трудовой

деятельности; классный чин федеральной гражданской службы, дипломатический ранг, воинское или специальное звание, классный чин правоохранительной службы, классный чин гражданской службы субъекта Российской Федерации, квалификационный разряд государственной службы, квалификационный разряд или классный чин муниципальной службы; степень родства; сведения о детях; данные трудовой книжки; реквизиты трудовой книжки; сведения об аттестации; сведения о повышении квалификации; сведения о профессиональной переподготовке; сведения о государственных наградах; сведения о наградах (поощрениях); ученая степень; ученое звание; характеристика; сведения о пенсиях; номер счета; сведения о близких родственниках; сведения об изменении ФИО близкими родственниками; адрес электронной почты; сумма; размер оклада; сведения о пребывании за границей; сведения о доходах, налогах, страховых взносах; сведения о доходах, расходах, об имуществе и обязательствах имущественного характера; сведения о владении иностранными языками; сведения о стажировке; сведения о регистрации по месту жительства; данные свидетельства о государственной регистрации права собственности; сведения о допуске к государственной тайне; фотография, сведения о наличии/отсутствии заболевания, препятствующего поступлению на государственную гражданскую службу или ее прохождению; сведения о судимости, реквизиты документа об образовании; сведения о близких родственниках, постоянно проживающих за границей и (или) оформляющих документы для выезда на постоянное место жительства в другое государство,

в целях исполнения муниципального контракта между мной и Оператором с использованием бумажных носителей и средств вычислительной техники, с соблюдением необходимых правовых, организационных и технических мер, обеспечивающих их защиту от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

В соответствии с требованиями ч. 3 ст. 6 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» даю согласие на поручение обработки (любое действие (операцию) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (предоставление, доступ), обезличивание, блокирование, удаление, уничтожение) следующих персональных данных:

ФИО, номер счета, сумма,

следующему юридическому лицу:

Публичное акционерное общество «Сбербанк России»: 117997, г. Москва, ул. Вавилова, д. 19

в целях начисления заработной платы и иных выплат с использованием бумажных носителей и средств вычислительной техники, с соблюдением принципов и правил обработки персональных данных, предусмотренных Федеральным законом «О персональных данных», а также необходимых правовых, организационных и технических мер, обеспечивающих их защиту от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

Я даю согласие уполномоченным должностным лицам Оператора считать следующие персональные данные общедоступными:

ФИО; должность; контактные телефоны; адрес электронной почты

в целях включения их в общедоступные источники персональных данных (справочники, адресные книги и т.д.). Мои персональные данные должны быть в любое время исключены из общедоступных источников персональных данных в случаях, указанных в ч. 2 ст. 8 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

Срок действия Согласия на обработку персональных данных - с даты подписания Согласия, в течение срока действия служебного контракта, в течение 10 лет после окончания срока действия служебного контракта с последующим хранением в архиве в течение 75 лет. Срок действия согласия на поручение обработки персональных данных третьим лицам и на включение персональных данных в общедоступные источники - в течение срока действия служебного контракта. Согласие может быть досрочно отозвано путем подачи письменного заявления в адрес Оператора.

Я предупрежден (а), что в случае отзыва согласия на обработку персональных данных, Оператор вправе продолжить обработку персональных данных без согласия при наличии оснований, указанных в пп. 2-11 ч. 1 ст. 6 Федерального закона «О персональных данных».

_____	_____	_____
(дата)	(подпись)	(расшифровка подписи)

Приложение 6

УТВЕРЖДЕНО
постановлением Администрации
МР «Буйнакский район»
«12» октября 2018 г. № 198

ТИПОВАЯ ФОРМА
разъяснения субъекту персональных данных юридических последствий отказа представить свои персональные данные

Мне,

_____,
(фамилия, имя, отчество)

_____

разъяснены юридические последствия отказа представить свои персональные данные Администрации МР «Буйнакский район», зарегистрированному по адресу: 368220, г. Буйнакск, ул. Ленина, 61.

В соответствии с Положением об обработке и защите персональных данных в Администрации МР «Буйнакский район» определен перечень персональных данных, которые субъект персональных данных обязан представить в связи с _____
(реализацией права поступления на муниципальную службу, предоставлением муниципальных услуг и исполнением муниципальных функций)

Я предупрежден(а), что в случае отказа предоставить мои персональные данные, Администрацией МР «Буйнакский район» (далее нужное подчеркнуть):

1. Реализация права поступления на муниципальную службу не может быть реализована.
2. Предоставление муниципальных услуг и исполнение муниципальных функций не может быть реализовано.

«___»_____20 __г. _____(_____)
(дата) (подпись) (расшифровка подписи)

Приложение 7

УТВЕРЖДЕНО
постановлением Администрации
МР «Буйнакский район»
«12» октября 2018 г. № 198

ПОРЯДОК
доступа муниципальных служащих Администрации МР «Буйнакский район» в помещения, в которых ведется обработка персональных данных

1. Настоящий Порядок доступа муниципальных служащих Администрации (далее - сотрудники) в помещения, в которых ведется обработка персональных данных, (далее - Порядок) устанавливают единые требования к доступу сотрудников Администрации в служебные помещения в целях предотвращения нарушения прав субъектов персональных данных, обрабатываемых в Администрации, и обеспечения соблюдения требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации», постановления 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» и другими нормативными правовыми актами.

2. Настоящий Порядок обязателен для применения и исполнения всеми сотрудниками Администрации.

3. Помещения, в которых ведется обработка персональных данных, должны отвечать определенным нормам и исключать возможность бесконтрольного проникновения в них посторонних лиц и гарантировать сохранность находящихся в этих помещениях документов и средств автоматизации (приложение 7).

Посторонние посетители допускаются строго в установленные дни и часы приёма и только в присутствии сотрудников Администрации.

4. Ответственными за организацию доступа в помещения Администрации, в которых ведется обработка персональных данных, являются начальники структурных подразделений Администрации.

5. Входные двери оборудуются замками, гарантирующими надежное закрытие помещений в нерабочее время.

6. По завершению рабочего дня, помещения, в которых ведется обработка персональных данных, закрываются.

7. Закрытие и вскрытие помещений, где ведется обработка персональных данных, производят сотрудники, работающие в этих помещениях. В течение дня ключи находятся у сотрудников, по окончании рабочего дня ключи от помещений сдаются на пост охраны Администрации под роспись в журнале приема-сдачи объекта под охрану. Передача ключей иным лицам не допускается.

8. При отсутствии сотрудников Администрации, работающих в этих помещениях, помещения могут быть вскрыты комиссией, созданной по указанию руководителя Администрации.

9. В случае утраты ключей от помещения немедленно заменяется замок.

10. Уборка в помещениях, в которых ведется обработка персональных данных и отсутствуют запираемые на ключ шкафы для носителей персональных данных, производится только в присутствии служащих, работающих в этих помещениях.

11. При обнаружении повреждений запоров или других признаков, указывающих на возможное проникновение в помещения, в которых ведется обработка персональных данных, посторонних лиц, эти помещения не вскрываются, а составляется акт и о случившемся немедленно ставятся в известность руководитель Администрации и органы внутренних дел.

12. Одновременно принимаются меры по охране места происшествия и до прибытия работников органов внутренних дел в эти помещения никто не допускается.

Приложение 9
Приложение 8

УТВЕРЖДЕНО
постановлением Администрации
МР «Буйнакский район»
«12» октября 2018 г. № 198

ПРАВИЛА
рассмотрения запросов субъектов персональных данных или их представителей в Администрации МР «Буйнакский район»

1. Общие положения

Настоящие Правила рассмотрения запросов субъектов персональных данных или их представителей в Администрации МР «Буйнакский район» (далее - Правила) разработаны в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и определяют права субъектов персональных данных, обязанности Администрации МР «Буйнакский район» (далее - Администрация, Оператор) при обращении субъекта персональных данных или его представителя, а также сроки и последовательность действий должностных лиц Администрации при рассмотрении запросов субъектов персональных данных или их представителей (далее - Запрос).

Представитель субъекта персональных данных - лицо, действующее от имени субъекта персональных данных в силу полномочий, основанных на доверенности, указании закона, либо акте уполномоченного на то государственного органа или органа местного самоуправления. При обращении представителя субъекта персональных данных в Администрацию предоставляется документ, подтверждающий полномочия законного представителя.

2. Права субъектов персональных данных

Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

- подтверждение факта обработки персональных данных Администрацией;
- правовые основания и цели обработки персональных данных;
- цели и применяемые Администрацией способы обработки персональных данных;
- наименование и место нахождения Администрации, сведения о лицах (за исключением работников Администрации), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Администрацией 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 законодательством в сфере защиты персональных данных;
- сроки обработки персональных данных, в том числе сроки их хранения;
- порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом «О персональных данных»;
- информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Администрации, если обработка поручена или будет поручена такому лицу;
- иные сведения, предусмотренные Федеральным законом «О персональных данных» или другими федеральными законами.

Сведения, указанные в п.2.1 настоящих Правил, должны быть предоставлены субъекту персональных данных Администрацией в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

Сведения, указанные в п.2.1 настоящих Правил, предоставляются субъекту персональных данных или его представителю Администрацией при обращении либо при получении запроса субъекта персональных данных или его представителя. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с Администрацией (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Администрацией, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

В случае, если сведения, указанные в п. 2.1 настоящих Правил, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно в Администрация или направить повторный запрос в целях получения сведений, указанных в п. 2.1 настоящих Правил, и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в

соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

Субъект персональных данных вправе обратиться повторно в Администрацию или направить повторный запрос в целях получения сведений, указанных в п. 2.1 настоящих Правил, а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в п. 2.4 настоящих Правил, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в п. 2.3 настоящих Правил, должен содержать обоснование направления повторного запроса.

Администрация вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным п. 2.4 и 2.5 настоящих Правил. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на Учреждении.

Субъект персональных данных вправе требовать от Администрации 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.

Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами, в том числе если:

обработка персональных данных, включая персональные данные, полученные в результате оперативно-розыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;

обработка персональных данных осуществляется органами, осуществившими задержание субъекта персональных данных по подозрению в совершении преступления, либо предъявившими субъекту персональных данных обвинение по уголовному делу, либо применившими к субъекту персональных данных меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством Российской Федерации случаев, если допускается ознакомление подозреваемого или обвиняемого с такими персональными данными;

обработка персональных данных осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;

доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц;

обработка персональных данных осуществляется в случаях,

предусмотренных законодательством Российской Федерации о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

3. **Обязанности оператора при обращении к нему субъекта персональных данных либо при получении запроса субъекта персональных данных или его представителя**

Оператор обязан сообщить в порядке, предусмотренном настоящими Правилами, 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.

В случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или персональных данных субъекту персональных данных или его представителю при их обращении либо при получении запроса субъекта персональных данных или его представителя Оператор обязан дать в письменной форме мотивированный ответ, с указанием причин отказа со ссылкой на положение ч. 8 ст. 14 Федерального закона «О персональных данных» или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий тридцати дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса субъекта персональных данных или его представителя.

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.

4. **Порядок рассмотрения запросов субъектов персональных данных или их представителей**

В день поступления запроса субъекта персональных данных или его представителя в Администрации указанный запрос необходимо зарегистрировать в соответствии с правилами документооборота, установленными Администрацией, а также внести соответствующую запись в Журнал учета обращений субъектов персональных данных. Форма Журнала учета обращений субъектов персональных данных утверждена локальным актом Администрации.

Ответственный за организацию обработки персональных данных Администрации осуществляет непосредственный контроль за соблюдением установленного законодательством Российской Федерации и настоящими Правилами порядка рассмотрения запросов субъектов персональных данных или их представителей. На контроль берутся все запросы.

Структурное подразделение, ответственное за исполнение указанного запроса, обеспечивает рассмотрение запроса и подготовку необходимой информации в установленный действующим законодательством срок.

Для проверки фактов, изложенных в запросах, при необходимости организуются служебные проверки в соответствии с законодательством Российской Федерации.

По результатам служебной проверки составляется мотивированное заключение, которое должно содержать объективный анализ собранных материалов. Если при проверке выявлены факты совершения сотрудником Администрации действия (бездействия), содержащего признаки административного правонарушения или состава преступления информация передается незамедлительно в правоохранительные органы. Результаты служебной проверки докладываются руководителю Администрации.

Запрос считается исполненным, если рассмотрены все поставленные в нем вопросы, приняты необходимые меры и даны исчерпывающие ответы заявителю.

Нарушение установленного порядка рассмотрения запросов влечет в отношении виновных должностных лиц ответственность в соответствии с законодательством Российской Федерации.

Приложение 9

УТВЕРЖДЕНО
постановлением Администрации
МР «Буйнакский район»
«12» октября 2018 г. № 198

ИНСТРУКЦИЯ
пользователя информационных систем персональных данных Администрации МР «Буйнакский район»

1. Общие положения

Пользователем информационных систем персональных данных (далее - Пользователь) является уполномоченный сотрудник Администрации МР «Буйнакский район» (далее - Администрация).

Пользователь должен знать законодательные и иные нормативные правовые акты Российской Федерации, методические материалы в сфере обработки персональных данных.

В своей деятельности, связанной с обработкой персональных данных, Пользователь руководствуется Политикой в отношении обработки персональных данных в Администрации МР «Буйнакский район» и настоящей Инструкцией.

Пользователи, участвующие в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющие доступ к аппаратным средствам, программному обеспечению и обрабатываемой информации, несут персональную ответственность за свои действия.

2. Обязанности и права пользователя информационных систем персональных данных

Пользователь обязан:

соблюдать требования Политики в отношении обработки персональных данных в Администрации МР «Буйнакский район» и иных нормативных актов Администрации, устанавливающих порядок работы с персональными данными;

выполнять в информационных системах персональных данных (далее - ИСПДн) только те процедуры, которые необходимы для исполнения его должностных обязанностей;

использовать для выполнения должностных обязанностей только предоставленное ему автоматизированное рабочее место (далее - АРМ) на базе персонального компьютера (автономной ПЭВМ);

пользоваться только зарегистрированными в установленном порядке съемными (отчуждаемыми) машинными носителями информации;

обеспечивать безопасное хранение вышеуказанных материальных носителей информации, исключающее несанкционированный доступ к ним;

немедленно сообщать руководителю структурного подразделения или ответственному за обеспечение безопасности персональных данных в ИСПДн (далее - Ответственный) о нештатных ситуациях, фактах и попытках несанкционированного доступа к обрабатываемой информации, о блокировании, исчезновении (искажении) защищаемой информации;

перед началом обработки в ИСПДн файлов, хранящихся на съемных носителях информации, Пользователь должен осуществлять проверку файлов на наличие компьютерных вирусов. Антивирусный контроль на АРМ должен осуществляться Пользователем не реже одного раза в неделю;

располагать экран монитора в помещении во время работы так, чтобы исключалась возможность ознакомления с отображаемой на них информацией посторонними лицами;

соблюдать установленный режим разграничения доступа к информационным ресурсам: получать пароль, надежно его запоминать и хранить в тайне.

Пользователям ИСПДн запрещается:

записывать и хранить информацию, относящуюся к конфиденциальной информации или персональным данным, на неучтенных материальных носителях информации;

оставлять во время работы материальные носители информации без присмотра, несанкционированно передавать материальные носители информации другим лицам и выносить их за пределы помещения, в котором производится обработка информации;

отключать средства антивирусной защиты; отключать (блокировать) средства защиты информации; производить какие-либо изменения в электрических схемах, монтаже и размещении технических средств;

самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение, изменять установленный алгоритм функционирования технических и программных средств;

обрабатывать в ИСПДн информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к информационным ресурсам ИСПДн;

сообщать (или передавать) посторонним лицам личные атрибуты доступа к ресурсам в ИСПДн;

работать в ИСПДн при обнаружении каких-либо неисправностей; хранить на учтенных носителях информации программы и данные, не относящиеся к рабочей информации;

вводить в ИСПДн персональные данные под диктовку или с микрофона;

привлекать посторонних лиц для производства ремонта технических средств ИСПДн без согласования с Ответственным.

Пользователь имеет право знакомиться с внутренними документами Администрации, регламентирующими его обязанности по занимаемой должности.

3. Организация парольной защиты при работе на объектах информатизации

Пароли доступа к ИСПДн устанавливаются Ответственным.

При формировании пароля необходимо руководствоваться следующими требованиями:

длина пароля должна быть не менее 8-и буквенно-цифровых символов; пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, дни рождения и другие памятные даты, номера телефонов, автомобилей, адреса места жительства, наименования АРМ, общепринятые сокращения) и другие данные, которые могут быть подобраны злоумышленником путем анализа информации;

запрещается использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов;

запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т.п.);

при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях;

в числе символов пароля, обязательно должны присутствовать буквы в верхнем и нижнем регистрах, а также цифры;

запрещается использовать ранее использованные пароли.

При организации парольной защиты запрещается:

записывать свои пароли в очевидных местах, внутренности ящика стола, на мониторе ПЭВМ, на обратной стороне клавиатуры и т.д.;

хранить пароли в записанном виде на отдельных листах бумаги; сообщать свои пароли посторонним лицам, а также сведения о применяемых средствах защиты от НСД.

4. Порядок применения парольной защиты

Плановую смену паролей на доступ в ИСПДн рекомендуется проводить один раз в месяц.

Пользователь обязан незамедлительно сообщить Ответственному факты утраты, компрометации ключевой, парольной и аутентифицирующей информации.

Внеплановая смена личного пароля должна производиться в обязательном порядке в следующих случаях:

компрометации (подозрении на компрометацию) пароля;

в случае прекращения полномочий (увольнение, переход на другую работу внутри организации) Пользователя (в течение 24 часов после окончания последнего сеанса работы данного с ИСПДн);

по инициативе Ответственного.

5. Технология обработки персональных данных

При первичном допуске к работе с ИСПДн Пользователь:

проходит инструктаж по использованию ИСПДн;

знакомится с требованиями нормативно-правовых, руководящих и организационно-распорядительных документов, регламентирующих обработку и обеспечение безопасности персональных данных;

получает у Ответственного идентификатор и личный пароль для входа в ИСПДн.

Перед началом работы Пользователь визуально проверяет целостность пломб системного блока, убеждается в отсутствии посторонних технических средств, включает необходимые средства вычислительной техники.

Авторизацию в ИСПДн (ввод личного идентификатора и пароля) Пользователь осуществляет при отсутствии в помещении посторонних лиц.

В процессе работы на АРМ ИСПДн Пользователь использует технические средства и установленное Ответственным программное обеспечение согласно Техническому паспорту ИСПДн.

Копирование персональных данных на электронные носители информации осуществляется только при наличии производственной необходимости и только на учтенные электронные носители информации.

При необходимости создания на АРМ Пользователя дополнительных электронных документов, содержащих персональные данные, Пользователь создает и хранит такие документы в строго отведенном для этого месте.

Печать документов, содержащих персональные данные, осуществляется только при наличии производственной необходимости на принтер, подключенный Ответственным к АРМ Пользователя. Все бумажные носители, не подлежащие учету по каким-либо техническим или иным причинам (сбой принтера при печати, обнаружение ошибок в документе после распечатки и т.д.) уничтожаются незамедлительно. Распечатанные черновые бумажные варианты вновь создаваемых документов, содержащих персональные данные, уничтожаются незамедлительно после подписания (утверждения) окончательного варианта документа.

В случае возникновения необходимости временно покинуть рабочее помещение во время работы в ИСПДн, Пользователь обязан выключить компьютер, либо заблокировать его, для чего нужно нажать комбинацию клавиш <Ctrl-Alt-Del> и выбрать в диалоговом окне кнопку «Блокировать». Разблокирование компьютера производится набором пароля разблокировки, который был создан при настройке системы блокировки АРМ. При отсутствии в покидаемом помещении других служащих Администрации, Пользователь обязан закрыть дверь помещения на ключ или другой используемый ограничитель доступа.

Покидая рабочее помещение в конце рабочего дня, Пользователь обязан выключить все необходимые средства вычислительной техники и закрыть дверь помещения на ключ.

Приложение 10

УТВЕРЖДЕНО
постановлением Администрации
МР «Буйнакский район»
«12» октября 2018 г. № 198

ЖУРНАЛ
учета отчуждаемых машинных носителей персональных данных

Учетный/ регистрационный (заводской) номер	Дата поста-новки на учет	Вид машинного носителя	Место хранения (размещения)*	Лицо, ответственное за использование и хранение					Отметка об уничтожении	
				Ф.И.О., должность	Дата получения	Подпись	Дата возврата	Подпись	Дата и № акта	Подпись ответственного лица
1	2	3	4	5	6	7	8	9	10	11

*в случае если на отчуждаемом машинном носителе персональных данных хранятся только персональные данные в зашифрованном с использованием СКЗИ виде, допускается хранение таких носителей вне сейфов (металлических шкафов).

Приложение 11

УТВЕРЖДЕНО
постановлением Администрации
МР «Буйнакский район»
«12» октября 2018 г. № 198

ПЕРЕЧЕНЬ
помещений, в которых размещены информационные системы персональных данных Администрации МР «Буйнакский район»

Администрацией МР «Буйнакский район» используются следующие информационные системы персональных данных:

- «1С: Предприятие 8.2», находящаяся по адресу: г. Махачкала, пл. Ленина, д. 2, кабинет № 36;
- «1С: Зарплата и кадры», находящаяся по адресу: г. Махачкала, пл. Ленина, д. 2, кабинет № 36.

Приложение 12

УТВЕРЖДЕНО
постановлением Администрации
МР «Буйнакский район»
«12» октября 2018 г. № 198

ИНСТРУКЦИЯ
ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных Администрации МР «Буйнакский район»

1. Общие положения

Ответственный за обеспечение безопасности персональных данных в информационных системах персональных данных Администрации МР «Буйнакский район» (далее - Ответственный) назначается приказом Администрации МР «Буйнакский район» (далее - Администрация) и отвечает за обеспечение конфиденциальности, целостности и доступности персональных данных (далее - ПДн) в процессе их обработки в информационных системах персональных данных (далее - ИСПДн) Администрации.

Ответственный должен знать законодательные и иные нормативные правовые акты Российской Федерации, методические материалы в сфере обработки и защиты ПДн.

В своей деятельности Ответственный руководствуется Политикой в отношении обработки персональных данных в Администрации МР «Буйнакский район», настоящей Инструкцией, рекомендациями Ответственного за организацию обработки персональных данных (далее - Ответственный за организацию обработки ПДн).

2. Основные функции и обязанности ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных

Функции Ответственного:

Ответственный изучает все стороны деятельности Администрации и вырабатывает рекомендации по защите ПДн при решении следующих основных вопросов:

проведение аналитической работы по комплексной защите и предупреждению утечки ПДн;

подготовка решений в отношении сведений о работах, выполняемых Администрацией, подлежащих защите;

координация внедрения и эксплуатации систем защиты и безопасности

информации, обрабатываемой техническими средствами;

проведение работ по контролю эффективности принимаемых мер по выявлению и закрытию возможных каналов утечки ПДн;

подготовка предложений по совершенствованию действующей системы защиты ПДн с последующим предоставлением Ответственному за организацию обработки ПДн Администрации;

учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей ПДн;

обеспечение соответствия проводимых работ в части обработки ПДн технике безопасности, правилам и нормам охраны труда;

осуществление в пределах своей компетенции иных функций в соответствии с целями и задачами Администрации.

Ответственный обязан:

Соблюдать требования нормативно-правовых и организационно - распорядительных документов по обеспечению безопасности ПДн при их обработке в ИСПДн.

Знать состав, структуру, назначение и выполняемые задачи ИСПДн, а также состав информационных технологий и технических средств, позволяющих осуществлять обработку ПДн.

Осуществлять общее техническое сопровождение ИСПДн:

контролировать соблюдение требований по размещению и использованию технических средств, указанных в инструкциях по эксплуатации этих средств;

контролировать сохранность пломб на оборудовании автоматизированных рабочих мест;

вести журнал учета и выдачи используемых материальных носителей ПДн;

контролировать использование съемных материальных носителей информации, в том числе запрещать использование неучтенных носителей информации;

проводить инструктаж сотрудников, осуществляющих обработку ПДн и имеющих доступ к ПДн, обрабатываемым в ИСПДн Администрации (далее - Пользователи ИСПДн) по правилам работы в ИСПДн.

Осуществлять настройку и сопровождение подсистемы регистрации и учета ИСПДн:

реализовывать полномочия доступа (чтение, запись) для каждого пользователя к элементам защищаемых информационных ресурсов (том, каталог, файл, запись, поле записи) на основе утвержденного руководителем списка сотрудников, допущенных к работе в ИСПДн; назначать пароли Пользователей ИСПДн;

контролировать плановую смену паролей Пользователями ИСПДн для доступа в ИСПДн;

своевременно удалять профиль Пользователя ИСПДн при увольнении или переводе сотрудника;

вводить в базу данных системы защиты от несанкционированного доступа (далее - НСД) описания событий, подлежащих регистрации

в системном журнале;

регулярно проводить анализ системного журнала для выявления попыток несанкционированного доступа к ИСПДн;

своевременно информировать Ответственного за организацию обработки ПДн о несанкционированных действиях персонала для организации расследования попыток НСД.

Сопровождать подсистему обеспечения целостности рабочего программного обеспечения (ПО) ИСПДн:

обеспечивать регулярное и своевременное обновление антивирусного программного обеспечения Администрации;

обеспечивать поддержание установленного порядка эксплуатации антивирусного программного обеспечения;

обеспечивать регулярное и своевременное создание резервных копий ИСПДн Администрации;

осуществлять настройку и сопровождение системы защиты от НСД в ИСПДн.

Проводить периодическое тестирование функций системы защиты от НСД при изменении программной среды и полномочий Пользователей ИСПДн.

Требовать прекращения обработки ПДн в случае нарушения установленного порядка работ или нарушения функционирования средств и систем защиты информации.

Участвовать в анализе ситуаций, касающихся функционирования средств защиты информации и служебных расследований фактов НСД.

Участвовать при проведении внутреннего контроля соответствия обработки ПДн требованиям к защите ПДн.

Контролировать выполнение Пользователями ИСПДн требований Инструкции пользователя информационных систем персональных данных Администрации, а также установленных требований для обеспечения уровней защищенности ПДн.

Контролировать правильность применения Пользователями ИСПДн средств защиты информации.

В случае получения от Пользователей ИСПДн информации о фактах утраты, компрометации ключевой, парольной и аутентифицирующей информации, а также любой другой информации ограниченного доступа, незамедлительно принять все необходимые меры для обеспечения безопасности ПДн в пределах своих полномочий.

Обеспечивать функционирование и поддерживать работоспособность на автоматизированных рабочих местах ИСПДн: антивирусного программного обеспечения; средств защиты от несанкционированного доступа.

В случае нарушения работоспособности технических средств и программного обеспечения ИСПДн, в том числе средств защиты ИСПДн, принимать меры по их своевременному восстановлению и выявлению причин, приведших к нарушению работоспособности. Своевременно информировать Ответственного за организацию обработки ПДн о выявленных нарушениях требований по обеспечению безопасности ПДн и попытках

несанкционированного доступа к ИСПДн.

Права ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных

Ответственный имеет право:

Знакомиться с нормативными актами Администрации, регламентирующими процессы обработки и защиты ПДн.

Вносить предложения руководителю Администрации по совершенствованию существующей системы защиты информации.

Привлекать по согласованию с Ответственным за организацию обработки ПДн и руководителем Администрации к работе по созданию и совершенствованию системы защиты ПДн других сотрудников Администрации.

Требовать от Пользователей ИСПДн соблюдения требований Инструкции пользователя информационных систем персональных данных Администрации и иных нормативно-правовых и организационнораспорядительных документов по обеспечению безопасности ПДн.

Участвовать в работе по совершенствованию мероприятий, обеспечивающих безопасность ПДн, вносить свои предложения по совершенствованию организационных и технических мер защиты ПДн в ИСПДн.

Инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения безопасности ПДн.

Требовать прекращения работы в ИСПДн, как в целом, так и отдельных Пользователей ИСПДн, в случае выявления нарушений требований по обеспечению безопасности ПДн или в связи с нарушением функционирования ИСПДн.

Обращаться за необходимыми разъяснениями по вопросам обработки и обеспечения безопасности ПДн к Ответственному за организацию обработки ПДн.

Приложение 13

УТВЕРЖДЕНО
постановлением Администрации
МР «Буйнакский район»
«12» октября 2018 г. № 198

Уведомление
о факте обработки персональных данных
без использования средств автоматизации

Я, _____

(фамилия, имя, отчество)

паспорт серии _____ № _____
выдан _____
_____

дата выдачи «____»_____ _____ г.

работающий (ая) в должности
_____
_____
_____
(должность, наименование структурного подразделения)

проинформирован (а):
- о факте обработки мною персональных данных, обработка которых осуществляется в Администрации МР «Буйнакский район» (далее – Оператор) без использования средств автоматизации*;
- о категориях обрабатываемых персональных данных;
- о правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами Оператора.

*обработка персональных данных, содержащихся в информационной системе персональных данных либо извлечённых из такой системы, считается осуществлённой без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляется при непосредственном участии человека.

Я предупрежден (а) о том, что в случае нарушения установленного законодательства российской Федерации порядка сбора, хранения, использования или распространения персональных данных я несу ответственность, предусмотренную ст. 13.11 КоАП РФ.

_____ _____ _____
(дата) (подпись) (расшифровка подписи)

Приложение 14

УТВЕРЖДЕНО
постановлением Администрации
МР «Буйнакский район»
«12» октября 2018 г. № 198

Обязательство о соблюдении конфиденциальности персональных данных

Я, _____

(фамилия, имя, отчество)

паспорт серии _____ № _____

выдан _____

_____

дата выдачи «____»_____ _____ г.

работающий (ая) в должности

_____

_____

_____

(должность, наименование структурного подразделения)

предупрежден (а) о том, что на период исполнения должностных обязанностей в соответствии с должностным регламентом мне будет предоставлен допуск к информации, содержащей персональные данные. Настоящим добровольно принимаю на себя обязательства:

1. Не передавать и не разглашать третьим лицам информацию, содержащую персональные данные, которая мне доверена (будет доверена) или станет известной в связи с исполнением должностных обязанностей.

2. В случае попытки третьих лиц получить от меня информацию, содержащую персональные данные, сообщать непосредственному начальнику.

3. Не использовать информацию, содержащую персональные данные, с целью получения выгоды.

4. Выполнять требования нормативных правовых актов, регламентирующих вопросы защиты персональных данных.

5. После расторжения со мной служебного контракта (трудового договора) не разглашать и не передавать третьим лицам известную мне информацию, содержащую персональные данные.

Я предупрежден (а) о том, что в случае разглашения мной сведений, касающихся персональных данных, или их утраты я несу ответственность, предусмотренную КоАП РФ.

_____ _____ _____

(дата) (подпись) (расшифровка подписи)

Приложение 15

УТВЕРЖДЕНО
постановлением Администрации
МР «Буйнакский район»
«12» октября 2018 г. № 198

Форма ознакомления с положениями законодательства Российской Федерации о персональных данных, локальными актами Администрации МР «Буйнакский район» по вопросам обработки персональных данных

Я, _____

(фамилия, имя, отчество)

паспорт серии _____ № _____

выдан _____

_____

дата выдачи «____»_____ _____ г.

работающий (ая) в должности

_____

_____

_____

(должность, наименование структурного подразделения)

ознакомлен (а) с

- положениями законодательства Российской Федерации о персональных данных, в том числе с требованиями к защите персональных данных (Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 15.09.2008 г. № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановлением Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 05.09.2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных»);
- документом, определяющим политику Администрации МР «Буйнакский район» в отношении персональных данных;
- локальными актами Администрации МР «Буйнакский район» по вопросам обработки персональных данных.

_____ _____ _____

(дата) (подпись) (расшифровка подписи)

Приложение 16

УТВЕРЖДЕНО
постановлением Администрации
МР «Буйнакский район»
«12» октября 2018 г. № 198

Уведомление о получении персональных данных от третьих лиц

Уважаемый (ая) _____

(фамилия, имя, отчество)

На основании _____

_____

Администрацией МР «Буйнакский район» (далее - Оператор) получена от

_____

_____

(наименование и адрес организации)

следующая информация, содержащая Ваши персональные данные:

_____

_____

_____

с целью: _____

_____

_____

предполагаемые пользователи

_____

Вы имеете право:

- на полную информацию о Ваших персональных данных, обрабатываемых Оператором;

- на свободный бесплатный доступ к Вашим персональным данным, включая право на получение копий любой записи, содержащей Ваши персональные данные, за исключением случаев, предусмотренных действующим законодательством;

- требовать от Оператора уточнения Ваших персональных данных, их блокирования или уничтожения в случае, если персональные данные являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав, получать иную информацию, касающуюся обработки Ваших персональных данных.

_____ _____ _____

(дата) (подпись) (расшифровка подписи)

Настоящее уведомление на руки получил:

_____ _____ _____

(дата) (подпись) (расшифровка подписи)

Приложение 17

УТВЕРЖДЕНО
постановлением Администрации
МР «Буйнакский район»
«12» октября 2018 г. № 198

Уведомление об уничтожении, изменении, прекращении обработки, устранении нарушений, допущенных при обработке персональных данных

Уважаемый (ая) _____

(фамилия, имя, отчество)

В связи с _____

_____

_____

_____

_____

_____

_____

(причина)

Сообщаем Вам, что Администрацией МР «Буйнакский район» прекращена обработка Ваших персональных данных и указанная информация подлежит уничтожению (изменению).

_____

_____

_____

_____

_____

(информация, содержащая персональные данные)

_____ _____ _____

(дата) (подпись) (расшифровка подписи)

Настоящее уведомление на руки получил:

_____ _____ _____

(дата) (подпись) (расшифровка подписи)

Приложение 18

УТВЕРЖДЕНО
постановлением Администрации
МР «Буйнакский район»
«12» октября 2018 г. № 198

Акт на списание и уничтожение машинных (бумажных) носителей информации

Комиссия в составе:

Председатель комиссии:	
Члены комиссии:	

составила настоящий акт в том, что перечисленные в нем машинные (бумажные) носители информации подлежат уничтожению как утратившие практическое значение и непригодные для перезаписи.

№ п/п	Вид носителя	Учетный номер носителя	Дата поступления	Краткое содержание информации

Всего подлежит списанию и уничтожению _____наименований машинных (бумажных) носителей информации
(подпись)

Правильность произведённых записей в акте проверил:

_____

(подпись)

Машинные (бумажные) носители информации перед уничтожением сверили с записями в акте и полностью уничтожили путём

_____

_____

«_____»_____ 20 __ г.

Председатель комиссии: _____

Члены комиссии: _____

_____

_____

_____

Приложение 19

УТВЕРЖДЕНО
постановлением Администрации
МР «Буйнакский район»
«12» октября 2018 г. № 198

Журнал учета передачи персональных данных

№	Сведения о запрашивающем лице	Состав запрашиваемых персональных данных	Цель получения персональных данных	Отметка о передаче или отказе в передаче персональных данных	Дата передачи/отказа в передаче персональных данных	Подпись ответственного сотрудника
1	2	3	4	5	6	7

Приложение 20

УТВЕРЖДЕНО
постановлением Администрации
МР «Буйнакский район»
«12» октября 2018 г. № 198

Журнал учета обращений субъектов персональных данных

№	Сведения об обратившемся субъекте персональных данных	Краткое содержание обращения (цель получения информации)	Отметка о предоставлении или отказе в предоставлении информации	Дата передачи/ отказа в предоставлении информации	Подпись обратившегося субъекта персональных данных	Подпись ответственного сотрудника
1	2	3	4	5	6	7

Приложение 21

УТВЕРЖДЕНО
постановлением Администрации
МР «Буйнакский район»
«12» октября 2018 г. № 198

Журнал учета ознакомления сотрудников с порядком обработки персональных данных и изменениями в законодательстве в области защиты персональных данных

№	ФИО сотрудника	Должность сотрудника	Дата ознакомления	Подпись сотрудника
1	2	3	4	5
Суть ознакомления (обучение сотрудников/ изменение в законодательстве), ФИО сотрудника, ответственного за ознакомление				

Приложение 22

УТВЕРЖДЕНО
постановлением Администрации
МР «Буйнакский район»
«12» октября 2018 г. № 198

ПОЛОЖЕНИЕ
по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Администрации МР «Буйнакский район»

ОБЩИЕ ПОЛОЖЕНИЯ

Настоящее Положение по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Администрации МР «Буйнакский район» (далее - Положение) разработано в соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказом Федеральной службы по техническому и экспортному контролю 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».

Цель разработки настоящего Положения - установление порядка организации и проведения работ по обеспечению безопасности персональных данных (далее - ПДн) в информационных системах персональных данных (далее - ИСПДн) Администрации МР «Буйнакский район» (далее - Администрация, Оператор) на протяжении всего жизненного цикла ИСПДн.

ПОРЯДОК ОРГАНИЗАЦИИ И ПРОВЕДЕНИЯ РАБОТ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Под организацией обеспечения безопасности ПДн при их обработке в ИСПДн понимается формирование и реализация совокупности согласованных по цели, задачам, месту и времени организационных и технических

мероприятий, направленных на минимизацию ущерба от возможной реализации угроз безопасности ПДн, реализуемых в рамках создаваемой системы защиты персональных данных (далее - СЗПДн).

СЗПДн включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности ПДн, уровня защищенности ПДн, который необходимо обеспечить, и информационных технологий, используемых в информационных системах.

Безопасность ПДн при их обработке в ИСПДн обеспечивает оператор или лицо, осуществляющее обработку ПДн по поручению оператора на основании заключаемого с этим лицом договора (далее - уполномоченное лицо). Договор между оператором и уполномоченным лицом должен предусматривать обязанность уполномоченного лица обеспечить безопасность ПДн при их обработке в информационной системе.

Выбор средств защиты информации для СЗПДн осуществляется оператором в соответствии с нормативными правовыми актами, принятыми Федеральной службой безопасности Российской Федерации (далее - ФСБ России) и Федеральной службой по техническому и экспортному контролю (далее - ФСТЭК России) во исполнение Федерального закона «О персональных данных».

Структура, состав и основные функции СЗПДн определяются исходя из уровня защищенности ПДн при их обработке в ИСПДн.

СЗПДн создается в три этапа:

Этап 1. Предпроектное обследование ИСПДн и разработка технического задания на создание СЗПДн.

Этап 2. Проектирование СЗПДн, закупка, установка, настройка необходимых средств защиты информации.

Этап 3. Ввод ИСПДн с СЗПДн в эксплуатацию.

Этап 1. Проведение предпроектного обследования и разработка технического задания на создание СЗПДн.

1.1 Назначение ответственного за организацию обработки ПДн Администрацией.

1.2 Создание комиссии по определению уровня защищенности ПДн при их обработке в ИСПДн Администрации.

1.3 Определение целей обработки ПДн Администрацией.

1.4 Определение перечня ИСПДн Администрации и состава ПДн, обрабатываемых в ИСПДн.

1.5 Определение перечня обрабатываемых Администрацией ПДн.

1.6 Определение сроков обработки и хранения ПДн, исходя из требования, что ПДн не должны храниться дольше, чем этого требуют цели обработки этих ПДн, по достижению которых ПДн подлежат уничтожению.

1.7 Определение перечня используемых в ИСПДн (предлагаемых к использованию в ИСПДн) общесистемных и прикладных программных средств.

1.8 Определение режимов обработки ПДн в ИСПДн в целом и в

отдельных компонентах.

1.9 Назначение ответственного за обеспечение безопасности ПДн в ИСПДн (далее - Ответственный) для разработки и осуществления технических мероприятий по организации и обеспечению безопасности ПДн при их обработке в ИСПДн. Для каждой ИСПДн может быть назначен отдельный Ответственный.

1.10 Назначение ответственного пользователя криптосредств, обеспечивающего функционирование и безопасность криптосредств, предназначенных для обеспечения безопасности ПДн. Утверждение перечня лиц, допущенных к работе с криптосредствами, предназначенными для обеспечения безопасности ПДн в ИСПДн (пользователей криптосредств).

1.11 Определение перечня помещений, в которых размещены ИСПДн и материальные носители ПДн.

1.12 Определение конфигурации и топологии ИСПДн в целом и их отдельных компонент, физических, функциональных и технологических связей как внутри этих систем, так и с другими системами различного уровня и назначения.

1.13 Определение технических средств и систем, используемых в ИСПДн, включая условия их расположения.

1.14 Формирование технических паспортов ИСПДн.

1.15 Разработка организационно-распорядительных документов (далее - ОРД), регламентирующих процесс обработки и защиты ПДн:

- Политика в отношении обработки персональных данных;
- Инструкции (ответственного за организацию обработки ПДн, ответственного за обеспечение безопасности ПДн в ИСПДн, пользователя ИСПДн, ответственного пользователя крипто средств);
- Раздел должностных инструкций сотрудников Администрации в части обеспечения безопасности ПДн при их обработке, включая установление персональной ответственности за нарушения правил обработки ПДн.

1.16 Получение (при необходимости) согласия на обработку ПДн субъектом ПДн, подписание обязательства о соблюдении конфиденциальности ПДн сотрудником Администрации.

1.17 Утверждение форм уведомлений субъектов ПДн и форм журналов, необходимых в целях обеспечения безопасности ПДн.

1.18 Определение уровня защищенности ПДн при их обработке в ИСПДн в соответствии с «Требованиями к защите ПДн при их обработке в информационных системах персональных данных», утвержденными постановлением Правительства Российской Федерации от 01.11.2012 № 1119 (подготовка и утверждение акта определения уровня защищенности ПДн при их обработке в ИСПДн).

1.19 Определение типа угроз безопасности ПДн, актуальных для информационной системы, с учетом оценки возможного вреда в соответствии с нормативными правовыми актами, принятыми во исполнение Федерального закона «О персональных данных». Определение угроз безопасности ПДн

в конкретных условиях функционирования ИСПДн (разработка моделей угроз безопасности ПДн при их обработке в ИСПДн).

1.20 Формирование технического задания на разработку СЗПДн по результатам предпроектного обследования на основе нормативнометодических документов ФСТЭК России и ФСБ России с учетом установленного уровня защищенности ПДн при их обработке в ИСПДн.

Техническое задание на разработку СЗПДн должно содержать:

- обоснование разработки СЗПДн;
- исходные данные создаваемой (модернизируемой) ИСПДн в техническом, программном, информационном и организационном аспектах;
- уровень защищенности ПДн при их обработке в ИСПДн;
- ссылку на нормативные документы, с учетом которых будет разрабатываться СЗПДн, и приниматься в эксплуатацию ИСПДн;
- конкретизацию мероприятий и требований к СЗПДн;
- состав и содержание работ по этапам разработки и внедрения СЗПДн;
- перечень предполагаемых к использованию сертифицированных средств защиты информации.

Этап 2. Проектирование СЗПДн, закупка, установка, настройка и опытная эксплуатация необходимых средств защиты информации.

2.1 Создание СЗПДн является необходимым условием обеспечения безопасности ПДн, в том случае, если существующие организационные и технические меры обеспечения безопасности не соответствуют требованиям к обеспечению безопасности ПДн для соответствующего уровня защищенности ПДн при их обработке в ИСПДн и/или не нейтрализуют всех угроз безопасности ПДн для данной ИСПДн.

2.2 Технические меры защиты ПДн предполагают использование программно-аппаратных средств защиты информации. При обработке ПДн с использованием средств автоматизации применение технических мер защиты является обязательным условием, а их количество и степень защиты определяется в процессе предпроектного обследования информационных ресурсов Администрации. Применение технических мер должно быть регламентировано нормативным актом Администрации.

2.3 Средства защиты информации, применяемые в ИСПДн, в установленном порядке проходят процедуру оценки соответствия, включая сертификацию на соответствие требованиям по безопасности информации.

2.4 На стадии проектирования и создания СЗПДн для ИСПДн Администрации проводятся следующие мероприятия:

- разработка технического проекта СЗПДн;
- приобретение (при необходимости), установка и настройка серийно выпускаемых технических средств обработки, передачи и хранения информации;
- разработка мероприятий по защите информации в соответствии с предъявляемыми требованиями;

- приобретение, установка и настройка сертифицированных технических, программных и программно-технических средств защиты информации, в том числе (при необходимости) средств криптографической защиты информации;
- реализация разрешительной системы доступа пользователей ИСПДн к обрабатываемой в ИСПДн информации;
- подготовка эксплуатационной документации на используемые средства защиты информации;
- корректировка (дополнение) организационно-распорядительной документации в части защиты информации.

Этап 3. Ввод ИСПДн с СЗПДн в промышленную эксплуатацию.

3.1 На стадии ввода в ИСПДн (СЗПДн) осуществляются:

- опытная эксплуатация средств защиты информации в комплексе с другими техническими и программными средствами в целях проверки их работоспособности в составе ИСПДн (при необходимости);
- приемо-сдаточные испытания средств защиты информации по результатам опытной эксплуатации (при необходимости);
- контроль выполнения требований (возможно проведение данного контроля в виде аттестации по требованиям безопасности ПДн).

3.2 Контроль за выполнением настоящих требований организуется и проводится оператором (уполномоченным лицом) самостоятельно и (или) с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации. Указанный контроль проводится не реже 1 раза в 3 года в сроки, определяемые оператором (уполномоченным лицом).

ПРОВЕДЕНИЕ РАБОТ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Работы по обеспечению безопасности ПДн проводятся в соответствии с Планом мероприятий по защите персональных данных (Приложение 2). Внутренние проверки режима обработки и защиты ПДн Администрацией проводятся в соответствии с Планом внутренних проверок режима обработки и защиты персональных данных (Приложение 3). По результатам проведения внутренней проверки составляется Отчет о результатах проведения внутренней проверки режима обработки и защиты персональных данных в Учреждении (Приложение 4).

Контроль за проведением работ по обеспечению безопасности ПДн осуществляет ответственный за организацию обработки ПДнв виде методического руководства, участия в разработке требований по защите ПДн, организации работ по выявлению возможных каналов утечки информации, согласования выбора средств вычислительной техники и связи, технических и программных средств защиты, участия в оценке соответствия ИСПДн

Администрации требованиям безопасности ПДн.

При необходимости к проведению работ по обеспечению безопасности ПДн могут привлекаться специализированные организации, имеющие лицензию ФСТЭК России на осуществление деятельности по технической защите конфиденциальной информации.

В соответствии с п. 5.2 Методических рекомендаций по обеспечению с помощью крипто средств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации, утвержденных руководством 8 Центра ФСБ России 21.02.2008 № 149/54-144, при необходимости использования при создании СЗПДн средств криптографической защиты информации к проведению работ по обеспечению безопасности ПДн Администрации необходимо привлекать специализированные организации, имеющие лицензии ФСБ России на осуществление работ по распространению шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведения, составляющие государственную тайну, на осуществление технического обслуживания шифровальных (криптографических) средств, на осуществление работ по оказанию услуг в области шифрования информации, не содержащих сведений, составляющих государственную тайну.

РЕШЕНИЕ ВОПРОСОВ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ДИНАМИКЕ ИЗМЕНЕНИЯ ОБСТАНОВКИ И КОНТРОЛЯ ЭФФЕКТИВНОСТИ ЗАЩИТЫ

Модернизация СЗПДн для функционирующих ИСПДн Администрации должна осуществляться в случае:

- изменения состава или структуры ИСПДн или технических особенностей ее построения (изменения состава или структуры программного обеспечения, технических средств обработки ПДн, топологии ИСПДн);
- изменения состава угроз безопасности ПДн в ИСПДн;
- изменения уровня защищенности ПДн при их обработке в ИСПДн;
- прочих случаях, по решению оператора.

В целях определения необходимости доработки (модернизации) СЗПДн не реже одного раза в год ответственным за организацию обработки ПДн должна проводиться проверка состава и структуры ИСПДн, состава угроз безопасности ПДн в ИСПДн и уровня защищенности ПДн при их обработке в ИСПДн, соблюдения условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией. Результаты проверки оформляются актом проверки и утверждаются руководителем Администрации.

Анализ инцидентов безопасности ПДн и составление заключений в обязательном порядке должно проводиться в случае выявления следующих фактов:

- несоблюдение условий хранения носителей ПДн;

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

Приложение 1

к Положению по организации и проведению работ
по обеспечению безопасности персональных данных при
их обработке в информационных системах персональных
данных Администрации МР «Буйнакский район»

**План мероприятий по защите персональных данных
в Администрации МР «Буйнакский район»**

№ п\п	Наименование мероприятия	Срок выполнения	Примечание
1.	Документальное регламентирование работы с ПДн	При необходимости	Разработка организационно-распорядительных документов по защите ПДн, либо внесение изменений в существующие
2.	Получение согласий субъектов ПДн (физических лиц) на обработку ПДн в случаях, когда этого требует законодательство	Постоянно	В случаях, предусмотренных Федеральным законом «О персональных данных», обработка ПДн осуществляется только с согласия в письменной форме субъекта ПДн. Равнозначным содержащему собственноручную подпись субъекта ПДн согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью
3.	Пересмотр договора с третьими лицами на поручение обработки ПДн	При необходимости	В случае поручения обработки ПДн субъектов ПДн третьим лицам (например, кредитно-финансовым организациям) в договор включается пункт о соблюдении конфиденциальности при обработке ПДн, а также учитываются требования ч.3 ст.6 Федерального закона «О персональных данных»

4.	Ограничение доступа сотрудников к ПДн	При необходимости (при создании ИСПДн)	В случае создания ИСПДн, а также приведения имеющихся ИСПДн в соответствие с требованиями закона необходимо разграничить доступ сотрудников Оператора к ПДн
5.	Взаимодействие с субъектами ПДн	Постоянно	Работа с обращениями субъектов ПДн, ведение журналов учета передачи персональных данных, обращений субъектов ПДн, уведомление субъектов ПДн об уничтожении, изменении, прекращении обработки, устранении нарушений, допущенных при обработке ПДн, получении ПДн от третьих лиц
6.	Ведение журналов учета отчуждаемых электронных носителей персональных данных, средств защиты информации	Постоянно	
7.	Повышение квалификации сотрудников в области защиты ПДн	Постоянно	Повышение квалификации сотрудников, ответственных за выполнение работ - не менее раза в три года, повышение осведомленности сотрудников - постоянно (данное обучение проводит ответственный за обеспечение безопасности ПДн в ИСПДн)
8.	Инвентаризация информационных ресурсов	Раз в полгода	Проводится с целью выявления в информационных ресурсах присутствия ПДн
9.	Установка сроков обработки ПДн и процедуры их уничтожения по окончании срока обработки	При необходимости	Для ПДн Оператором устанавливаются сроки обработки ПДн, которые документально подтверждаются в нормативных документах Оператора. При пересмотре сроков необходимые изменения вносятся в соответствующие документы.

10.	Уничтожение электронных (бумажных) носителей информации при достижении целей обработки ПДн	При необходимости	Уничтожение электронных (бумажных) носителей информации при достижении целей обработки ПДн производится с оформлением Акта на списание и уничтожение электронных (бумажных) носителей информации
11.	Определение уровня защищенности ПДн при их обработке в ИСПДн	При необходимости	Определение уровня защищенности ПДн при их обработке в ИСПДн осуществляется при создании ИСПДн, при изменении состава ПДн, объёма обрабатываемых ПДн, субъектов ПДн.
12.	Выявление угроз безопасности и разработка моделей угроз и нарушителя	При необходимости	Разрабатывается при создании системы защиты ИСПДн
13.	Аттестация ИСПДн на соответствие требованиям по обеспечению безопасности ПДн	При необходимости	Проводится совместно с лицензиатами ФСТЭК
14.	Эксплуатация ИСПДн и контроль безопасности ПДн	Постоянно	
15.	Понижение требований по защите ПДн путем сегментирования ИСПДн, отключения от сетей общего пользования, обеспечения обмена между ИСПДн с помощью сменных носителей, создания автономных ИСПДн на выделенных АРМ и прочих доступных мер	При необходимости	В случае создания ИСПДн, а также приведения имеющихся ИСПДн в соответствии с требованиями закона

Приложение 2

к Положению по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Администрации МР «Буйнакский район»

План внутренних проверок режима обработки и защиты персональных данных в Администрации МР «Буйнакский район»

№	Мероприятие	Периодичность	Дата, подпись
	Организационные меры по вопросам обработки ПДн		
1.	Осуществление внутреннего контроля и (или) аудита соответствия обработки ПДн ФЗ-152«О персональных данных» и принятым в соответствии с ним нормативным правовым актам	Раз в полгода	
2.	Проверка ознакомления сотрудников, непосредственно осуществляющих обработку ПДн, с положениями законодательства Российской Федерации о ПДн, в том числе требованиями к защите ПДн	Раз в полгода	
3.	Проверка получения согласий субъектов ПДн на обработку ПДн в случаях, когда этого требует законодательство	Раз в полгода	
4.	Проверка подписания сотрудниками, осуществляющими обработку ПДн, основных форм, необходимых в целях выполнения требований законодательства в сфере обработки и защиты ПДн: - уведомления о факте обработки ПДн без использования средств автоматизации; - обязательства о соблюдении конфиденциальности ПДн; - формы ознакомления с положениями законодательства Российской Федерации о ПДн, локальными актами Администрации по вопросам обработки ПДн; - типового обязательства о прекращении обработки ПДн в случае расторжения служебного контракта (трудового договора); - разъяснения субъекту ПДн юридических последствий отказа предоставить свои ПДн	Раз в полгода	
5.	Проверка уничтожения материальных носителей ПДн с составлением соответствующего акта	Ежегодно	
6.	Проверка ведения журналов по учету обращений субъектов ПДн и учету передачи ПДн субъектов третьим лицам	Раз в полгода	
7.	Проведение внутренних проверок на предмет выявления изменений в правилах обработки и защиты ПДн	Ежегодно	
8.	Проверка соблюдения условий хранения материальных носителей ПДн	Раз в полгода	

9.	Проверка состояния актуальности Уведомления об обработке (намерении осуществлять обработку) ПДн	Раз в полгода	
10.	Поддержание в актуальном состоянии организационно-распорядительных документов по вопросам обработки ПДн, в том числе документов, определяющих политику Администрации в отношении обработки ПДн	Раз в полгода	
Технические меры по вопросам защиты ПДн			
11.	Организация анализа и пересмотра имеющихся угроз безопасности ПДн, а также предсказание появления новых, еще неизвестных, угроз	Ежегодно	
12.	Оценка вреда, который может быть причинен субъектам ПДн в случае нарушения ФЗ-152 «О персональных данных»	Ежегодно	
13.	Проверка применения для обеспечения безопасности ПДн средств защиты информации, прошедших в установленном порядке процедуру соответствия	Раз в полгода	
14.	Оценка эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию ИСПДн	При необходимости	
15.	Контроль учета машинных носителей ПДн	Раз в полгода	
16.	Контроль за принимаемыми мерами по обеспечению безопасности ПДн и уровня защищенности ИСПДн	Раз в полгода	
17.	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в ИСПДн	Ежеквартально	
18.	Контроль внесения изменений в структурно-функциональные характеристики ИСПДн	Ежеквартально	
19.	Контроль корректности настроек средств защиты информации	Раз в полгода	
20.	Контроль за обеспечением резервного копирования	Ежеквартально	
21.	Поддержание в актуальном состоянии организационно-распорядительных документов по вопросам защиты ПДн	Раз в полгода	

Приложение 3

к Положению по организации и проведению работ по
обеспечению безопасности персональных данных при их
обработке в информационных системах персональных данных
Администрации МР «Буйнакский район»

Отчёт о результатах проведения внутренней проверки режима обработки и защиты персональных данных в Администрации МР «Буйнакский район»

1.1. Внутренняя проверка произведена на основании Положения по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Администрации МР «Буйнакский район» от «____» _____ 20___ г.

1.2. Проверка проводилась «___»_____ 20 г. по адресу:
_____
_____

1.3. В ходе проверки были проведены следующие мероприятия:
1) _____
_____
_____
_____
_____

1.4. Результаты проведения проверки:
1) _____
_____
_____
_____
_____

1.5. Необходимые мероприятия.
На основании проведения внутренней проверки режима обработки и защиты ПДн рекомендуется осуществить следующие мероприятии:
1) _____
_____
_____
_____

Подписи ответственных лиц, проводивших внутреннюю проверку режима обработки и защиты ПДн:

_____	_____	_____
(дата)	(подпись)	(расшифровка подписи)
_____	_____	_____
(дата)	(подпись)	(расшифровка подписи)
_____	_____	_____
(дата)	(подпись)	(расшифровка подписи)

Приложение 23

УТВЕРЖДЕНО
постановлением Администрации
МР «Буйнакский район»
«12» октября 2018 г. № 198

ПОРЯДОК
хранения, использования и передачи персональных данных сотрудников Администрации МР «Буйнакский район»

ОБЩИЕ ПОЛОЖЕНИЯ

Настоящий Порядок хранения, использования и передачи персональных данных сотрудников Администрации МР «Буйнакский район» (далее - Порядок) разработан в соответствии с Трудовым кодексом Российской Федерации, Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

Цель разработки настоящего Порядка - определение порядка обработки (хранения, использования, передачи) персональных данных сотрудников Администрации МР «Буйнакский район» (далее - Администрация, Оператор); обеспечение защиты прав и свобод сотрудников Администрации при обработке их персональных данных.

ХРАНЕНИЕ И ИСПОЛЬЗОВАНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ СОТРУДНИКОВ

Хранение персональных данных должно осуществляться в форме, позволяющей определить сотрудника Администрации, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого является сотрудник. Обрабатываемые персональные данные подлежат уничтожению, либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом. Хранение персональных данных сотрудников Администрации может осуществляться на бумажных и машинных носителях, доступ к которым ограничен списком лиц, допущенных к обработке персональных данных.

Все отчуждаемые машинные носители персональных данных подлежат строгому учету. Форма Журнала учета отчуждаемых машинных носителей персональных данных утверждена нормативным актом Администрации.

Персональные данные сотрудников, содержащиеся на машинных носителях персональных данных, должны храниться на автоматизированных

рабочих местах и серверах информационных систем персональных данных Администрации, установленных в пределах помещений, утвержденных Приказом об обеспечении безопасности помещений, в которых размещены информационные системы персональных данных.

Персональные данные сотрудников, содержащиеся на материальных носителях персональных данных, должны храниться в пределах помещений, утвержденных Приказом об обеспечении безопасности материальных носителей персональных данных.

Все хранимые или используемые средства защиты информации (далее - СЗИ), эксплуатационная и техническая документация к ним подлежат поэкземплярному учету и выдаются под расписку в Журнале поэкземплярного учета СЗИ, эксплуатационной и технической документации к ним пользователям СЗИ, несущим персональную ответственность за их сохранность. Форма соответствующего Журнала утверждена нормативным актом Администрации.

Хранение персональных данных сотрудников должно происходить в порядке, исключающем их утрату или их неправомерное использование.

Использование персональных данных сотрудников осуществляется Администрацией исключительно в целях выполнения требований трудового законодательства Российской Федерации.

Обработка персональных данных сотрудников Администрации осуществляется только специально уполномоченными лицами, перечень которых утверждается приказом Администрации, при этом указанные в приказе сотрудники должны иметь право получать только те персональные данные субъекта, которые необходимы для выполнения непосредственных должностных обязанностей.

Лица, осуществляющие обработку персональных данных без использования средств автоматизации (в том числе сотрудники организации-оператора или лица, осуществляющие такую обработку по договору с оператором), должны быть проинформированы о факте обработки ими персональных данных, обработка которых осуществляется оператором без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами Администрации (при их наличии).

Передача персональных данных сотрудников между структурными подразделениями Администрации осуществляется только между сотрудниками, включенными в перечень лиц, имеющих доступ к персональным данным.

Обработка персональных данных сотрудников должна осуществляться только в пределах помещений Администрации и с использованием средств вычислительной техники Администрации.

Администрация вправе поручить обработку персональных данных сотрудников другим юридическим или физическим лицам на основании

договора (далее - поручение Администрации) с согласия сотрудника, если иное не предусмотрено Федеральным законом «О персональных данных».

Лицо, осуществляющее обработку персональных данных по поручению Администрации, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом «О персональных данных».

Сотрудники Администрации и иные лица, получающие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия сотрудников, если иное не предусмотрено федеральным законодательством в сфере защиты персональных данных.

ПЕРЕДАЧА ПЕРСОНАЛЬНЫХ ДАННЫХ

При передаче персональных данных сотрудника Оператор должен соблюдать следующие требования:

- не сообщать персональные данные сотрудника третьей стороне без письменного согласия сотрудника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью сотрудника, а также в случаях, предусмотренных Гражданским кодексом Российской Федерации или иными федеральными законами;
- предупреждать лица, получающие персональные данные сотрудников, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц обеспечения конфиденциальности, полученных персональных данных;
- не сообщать персональные данные сотрудника в коммерческих целях без его письменного согласия;
- передавать персональные данные сотрудника представителям сотрудников в порядке, установленном Гражданским кодексом Российской Федерации, и ограничивать эту информацию только теми персональными данными сотрудника, которые необходимы для выполнения указанными представителями их функций;
- не отвечать на вопросы, связанные с передачей персональных данных сотрудника по телефону или факсу, за исключением случаев, связанных с выполнением соответствующими сотрудниками своих непосредственных должностных обязанностей, адресатам в чью компетенцию входит получение такой информации.

В целях обеспечения контроля правомерности использования переданных по запросам персональных данных лицами, их получившими, сведения о лице, направившем запрос, дата передачи персональных данных или дата уведомления об отказе в их предоставлении, а также состав переданной информации фиксируются в Журнале учета передачи персональных данных. Форма соответствующего Журнала утверждена локальным актом Администрации.

ЛИСТ ОЗНАКОМЛЕНИЯ

№ п/п	Ф.И.О.	Должность	Дата	Подпись