Приложение

к приказу финуправления

Администрации Белокалитвинского

района

от «01» 09. 2022 № 34/1

Положение

об обработке персональных данных в финансовом управлении Администрации Белокалитвинского района

(далее – Положение)

СОДЕРЖАНИЕ

|  |  |
| --- | --- |
| 1. Общие положения………………………………………………………………… | 3 |
| 2. Основные понятия………………………………………………………………… | 4 |
| 3. Информация об Операторе……………………………………………………… | 5 |
| 4. Категория, состав персональных данных, обрабатываемых в финансовом управлении…………………………………………………………………………... | 5 |
| 5. Основные принципы обработки персональных данных в финансовом управлении ………………………………………………………………………... | 6 |
| 6. Правила обработки персональных данных……………………………………... | 8 |
| 7. Передача персональных данных…………………………………………………. | 11 |
| 8. Права субъектов персональных данных………………………………………… | 12 |
| 9. Правила рассмотрения запросов субъектов персональных данных или их представителей, запросов уполномоченного органа по защите прав субъектов персональных данных…………………………………………………...................... | 14 |
| 10. Лица, ответственные за выполнение требований по обработке и обеспечению безопасности персональных данных в финансовом управлении ………………………………………………………………………………………… | 17 |
| 11. Правила работы с обезличенными персональными данными………………... | 20 |
| 12. Блокирование, обезличивание и уничтожение персональных данных……… | 21 |
| 13. Порядок доступа в помещения, в которых осуществляется обработка персональных данных……………………………………………………………….. | 22 |
| 14. Гарантии конфиденциальности……………………………………………….... | 24 |
| 15. Контроль эффективности защиты ПДн……………………………………….. | 24 |
|  |  |

1. Общие положения

1.1. Настоящее Положение разработано в соответствии с требованиями пункта 2 раздела 1 статьи 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее также – Федеральный закон № 152-ФЗ) и 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, утвержденного постановлением Правительства Российской Федерации от 21.03.2012 № 211 (Собрание законодательства Российской Федерации, 2012, № 14, ст. 1626).

1.2. Настоящее Положение является общедоступным документом, которое определяет политику, концептуальные основы деятельности финансового управления Администрации Белокалитвинского района (далее – финуправление или Оператор) в отношении обработки персональных данных, осуществляемой как с использованием средств автоматизации, так и без использования таких средств и обеспечения безопасности персональных данных.

1.3. Положение определяет правила обработки персональных данных, устанавливающие процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также определяющие для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, способы и принципы обработки, категории обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований, права и обязанности Оператора при обработке персональных данных, права субъектов персональных данных, основные направления деятельности по обеспечению безопасности персональных данных.

1.4. Цели обработки персональных данных

Обработка персональных данных осуществляется в рамках реализации полномочий финуправления, предусмотренных Положением о финансовом управлении Администрации Белокалитвинского района, утвержденным \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ в целях обеспечения деятельности финуправления, реализации трудовых отношений; поступлении, прохождении и прекращении муниципальной службы; государственной политики по предоставлению гражданам Российской Федерации закрепленного за ними Конституцией Российской Федерации права на обращение в муниципальные органы, в области противодействия коррупции; содействия муниципальным служащим в прохождении муниципальной службы, формирования кадрового резерва муниципальной службы, обучения и должностного роста; учета результатов исполнения муниципальными служащими должностных обязанностей, оказанием гражданам содействия в защите их прав и законных интересов в соответствии с международным, федеральным и региональным законодательством, обеспечения личной безопасности муниципальных служащих, и членов их семьи, обеспечения муниципальным служащим установленных законодательством Российской Федерации условий труда, гарантий и компенсаций, сохранности принадлежащего им имущества; осуществление пропускного режима в здание.

1.5. Обработка персональных данных в финуправлении осуществляется на основании:

Конституции Российской Федерации;

Семейного кодекса Российской Федерации (Федеральный закон от 29.12.1995 № 223-ФЗ);

Трудового кодекса Российской Федерации (Федеральный закон от 30.12.2001 №197-ФЗ) (далее – Трудовой кодекс);

 Федерального закона от 02.03.2007 N 25-ФЗ (ред. от 27.12.2018)

"О муниципальной службе в Российской Федерации"(далее – Закон № 25-ФЗ);

Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;

Федерального закона от 25.12.2008 № 273-ФЗ «О противодействии коррупции» (далее – Закон № 273-ФЗ);

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»;

Постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

Постановления Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без средств автоматизации».

2. Основные понятия

Персональные данные (далее также – ПДн) – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

биометрические персональные данные - сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных (дактилоскопические данные, радужная оболочка глаз, анализы ДНК, рост, вес, а также иные физиологические или биологические характеристики человека, в том числе изображение человека (фотография и видеозапись), которые позволяют установить его личность и используются оператором для установления личности субъекта персональных данных);

Оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

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

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

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

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

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

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

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

АРМ ИСПДн – автоматизированное рабочее место, входящее в состав ИСПДн.

3. Информация об Операторе

3.1. Полное наименование: Финансовое управление Администрации Белокалитвинского района.

3.2. Сокращенное наименование: Финуправление Администрации района.

3.3. Адрес местонахождения: 347042, Ростовская область, г. Белая Калитва, ул. Чернышевского, д. 8.

3.4. Почтовый адрес: 347042, Ростовская область, г. Белая Калитва, ул. Чернышевского, д. 8.

3.5. Телефон/Факс: 8 (86383) 2-67-31.

3.6. Официальный сайт Финуправления: <http://www.fin-bk.ru/>

3.7.Зарегистрирован в реестре операторов персональных данных 12.01.2011 под регистрационным номером 11-0175643.

4. Категория, состав персональных данных,

 обрабатываемых в финуправлении.

4.1. Финуправление осуществляет обработку персональных данных в связи с:

реализацией трудовых отношений;

поступлением, прохождением и прекращением муниципальной службы;

реализацией государственной политики в области противодействия коррупции в исполнительных органах Администрации Белокалитвинского района.

4.2. В ИСПДн финуправления обрабатываются следующие категории персональных данных:

персональные данные муниципальных служащих;

персональные данные членов семьи муниципальных служащих;

персональные данные граждан, претендующих на замещение должностей муниципальной службы;

персональные данные работников;

5. Основные принципы обработки персональных данных

в финуправлении

5.1. Финуправление в своей деятельности обеспечивает соблюдение принципов обработки персональных данных, указанных в ст. 5 Федерального закона № 152-ФЗ.

Обработка персональных данных осуществляться только на законной и справедливой основе.

5.2. Финуправление не осуществляет обработку биометрических персональных данных.

5.3. Финуправление не выполняет обработку специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни.

5.4. Финуправление не поручает обработку персональных данных другим лицам на основании договора.

5.5. Персональные данные субъектов обрабатываются как на бумажных носителях, так и посредством персональных электронных вычислительных машин (автоматизированная обработка).

5.6. Автоматизированная обработка персональных данных осуществляется только в защищенных по требованиям безопасности информации помещениях, установленных Правительством Российской Федерации и федеральными органами исполнительной власти, уполномоченных в области обеспечения безопасности информации.

5.7. Запрещается передача информации, содержащей персональные данные по незащищенным каналам связи.

5.8. Обработка персональных данных в информационных системах персональных данных Финуправления осуществляется в соответствии с требованиями настоящего Положения.

5.9. Обработка персональных данных происходит до утраты правовых оснований и ограничивается достижением конкретных, заранее определенных и законных целей.

5.10. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

5.11. Сбор персональных данных может осуществляться как путем представления их самим субъектом, так и путем получения из иных источников в соответствии с требованиями действующего законодательства Российской Федерации.

Субъект персональных данных самостоятельно принимает решение о предоставление своих персональных данных и дает письменное согласие на их обработку оператором.

В случае недееспособности либо несовершеннолетия субъекта персональных данных все персональные данные субъекта следует получать от его законных представителей. Законный представитель самостоятельно принимает решение о предоставлении персональных данных своего подопечного и дает письменное согласие на их обработку оператором.

Согласие на обработку персональных данных может быть отозвано субъектом персональных данных, законным представителем субъекта персональных данных.

В случаях, когда Оператор может получить необходимые персональные данные субъекта только у третьей стороны, субъект должен быть уведомлен об этом заранее.

5.12. При сборе персональных данных работник структурного подразделения оператора, осуществляющий сбор (получение) персональных данных непосредственно от субъекта персональных данных обязан разъяснить указанным лицам юридические последствия отказа предоставить персональные данные.

5.13. В финуправлении не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

Обработке подлежат только персональные данные, которые отвечают целям их обработки.

Содержание и объем обрабатываемых персональных данных собираемых Оператором соответствуют заявленным целям обработки.

5.14. При обработке персональных данных обеспечиваются точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных.

 Оператор принимает необходимые меры по удалению или уточнению неполных или неточных данных.

5.15. Срок хранения документов, содержащих персональные данные, определяется «Перечнем типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения», утвержденный Приказом Министерства культуры РФ от 25.08.2010 № 558, иными положениями законодательства РФ.

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

Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижению цели обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

5.16. Оператор не производит трансграничную передачу персональных данных (органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу).

5.17. Оператором созданы общедоступные источники персональных данных (справочники, адресные книги).

Персональные данные, сообщаемые субъектом (год и место рождения, адрес, абонентский номер, сведения о профессии и др.), включаются в такие источники только с письменного согласия субъекта персональных данных.

5.18. Финуправление обезличивает персональные данные субъектов персональных данных только в случаях и в целях предоставления статистической отчетности для заинтересованной стороны в соответствии с требованиями законодательства Российской Федерации.

6. Правила обработки персональных данных

6.1. В соответствии с требованиями Федерального закона № 152-ФЗ в целях обработки персональных данных Финуправлением сформированы следующие ИСПДн:

 «1С» предназначена для обработки персональных данных в связи с реализацией трудовых отношений, реализацией государственной политики по предоставлению гражданам Российской Федерации закрепленного за ними Конституцией Российской Федерации права на обращение в государственные органы и осуществления государственных функций (полномочий, обязанностей).

Персональные данные в Финуправлении обрабатываются только в ИСПДн, указанных в «Перечне ИСПДн и персональных данных обрабатываемых в Финуправлении» в соответствии с требованиями настоящего Положения.

В ИСПДн выполнен весь комплекс мероприятий по обеспечению безопасности информации в соответствии с требованиями к защите персональных данных при их обработке в ИСПДн, установленных Правительством Российской Федерации и Федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации.

С целью обеспечения соответствующего уровня безопасности информации в ИСПДн применены сертифицированные средства защиты информации от несанкционированного доступа и антивирусные средства.

6.2. При возникновении законной потребности у структурных подразделений Финуправления для обработки иных персональных данных лицо, ответственное за обработку персональных данных формирует заявку на имя лица, ответственного за организацию обработки персональных данных, согласованную с администратором информационной безопасности.

Заявка формируется в простой письменной форме с указанием:

- основания обработки;

- цели обработки;

- способов обработки;

- перечня действий с персональными данными;

- срока или условий прекращения обработки персональных данных;

- категории персональных данных, субъектов персональных данных;

- ф.и.о, должности лиц, которые будут допущены к обрабатываемым персональным данным;

- наименования информационной системы персональных данных и необходимого количества автоматизированных рабочих мест.

6.3. Допуск муниципальных служащих, работников Финуправления к обработке персональных данных осуществляется в строгом соответствии с Перечнем должностей муниципальной службы финансового управления Администрации Белокалитвинского района, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным (далее также – Перечень).

Ответственность за организацию допуска государственных гражданских служащих, работников Финуправления возлагается на лиц, ответственных за обработку персональных данных и администратора информационной безопасности.

6.4. Порядок учета лиц, допущенных к работе с персональными данными в ИСПДн Финуправления.

Основанием для допуска работника к обработке персональных данных в Финуправлении является распоряжение о приеме его на соответствующую должность, включенную в Перечень.

Формирование учетной записи в ИСПДн осуществляется администратором информационной безопасности на основании копии распорядительного документа о приеме на работу.

Основанием для прекращения допуска работника к обработке персональных данных является распоряжение об увольнении лица, включенного в Перечень, или исключение лица из Перечня в связи с переводом на иную должность, не связанную с обработкой персональных данных.

6.5. Муниципальные служащие и работники, непосредственно осуществляющие обработку персональных данных, а также муниципальные служащие и работники, имеющие доступ к персональным данным, обязаны подписать обязательство о прекращении обработки персональных данных, ставших известными им в связи с исполнением должностных обязанностей, в случае расторжения с ними контракта или трудового договора.

6.6. Порядок обработки персональных данных в Финуправлении без использования средств автоматизации.

6.6.1. Обработка персональных данных без использования средств автоматизации (хранение, защита от несанкционированного доступа, копирование, уничтожение, распространение) осуществляется в Финуправлении согласно «Положению об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утвержденному постановлением Правительства Российской Федерации 15.09.2008 № 687.

6.6.2. Обработка персональных данных без использования средств автоматизации осуществляется в виде документов на бумажных носителях.

6.6.3. Персональные данные, предоставляемые субъектами на бумажном носителе в связи с исполнением Финуправлением муниципальных функций, хранятся на бумажных носителях в структурных подразделениях Финуправления, к полномочиям которых относится обработка персональных данных.

6.6.4. При неавтоматизированной обработке персональных данных на бумажных носителях:

не допускается фиксация на одном бумажном носителе персональных данных, цели обработки которых заведомо несовместимы;

персональные данные должны обособляться от иной информации, в частности путем фиксации их на отдельных бумажных носителях, в специальных разделах или на полях форм (бланков);

документы, содержащие персональные данные, формируются в дела в зависимости от цели обработки персональных данных.

6.6.5. Документы, содержащие персональные данные, должны храниться в надежно запираемых шкафах или сейфах. При этом должны быть созданы надлежащие условия, обеспечивающие их сохранность.

6.6.6. Уничтожение или обезличивание части персональных данных, должно производиться способом, исключающим дальнейшую обработку этих персональных данных, с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

6.6.7. При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:

при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;

при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

6.9.8. Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на бумажном носителе, а если это не допускается техническими особенностями бумажного носителя, – путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

6.7. Ознакомление пользователей ИСПДн с правилами работы с ПДн осуществляется путем:

проведения руководителем структурного подразделения Финуправления, обрабатывающего ПДн, первичных инструктажей с вновь принятым работником по соблюдению установленных правил работы с ПДн;

проведения обучения пользователей ИСПДн администратором информационной безопасности правилам работы с используемыми средствами защиты информации;

путем самостоятельного изучения муниципальным служащим, работником Финуправления, непосредственно обрабатывающим ПДн, организационно-распорядительных документов, регламентирующих вопросы обеспечения безопасности ПДн.

При проведении первичного инструктажа новому пользователю ИСПДн должны быть разъяснены:

права и обязанности пользователя ИСПДн;

действия, которые запрещены при обработке ПДн;

возможные последствия и ответственность в случае нарушения правил работы с ПДн.

6.8. Допуск пользователей ИСПДн к ИСПДн Финуправления осуществляется только после прохождения первичного инструктажа и ознакомления с организационно-распорядительными документами Финуправления по вопросам обеспечения безопасности ПДн.

7. Передача персональных данных

7.1. Финуправление не предоставляет и не раскрывает сведения, содержащие персональные данные субъектов персональных данных, третьей стороне без письменного согласия субъекта персональных данных, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью, а также в случаях, установленных федеральными законами.

7.2. По мотивированному запросу, при наличии законных оснований, исключительно для выполнения возложенных законодательством функций и полномочий персональные данные субъекта персональных данных без его согласия могут быть переданы в:

- судебные органы, в связи с осуществлением правосудия;

- органы государственной безопасности;

- органы прокуратуры;

- органы полиции;

- следственные органы;

- налоговые органы;

- пенсионный Фонд РФ;

- Фонд социального страхования РФ;

- федеральную службу государственной статистики РФ;

- Фонд обязательного медицинского страхования РФ.

7.3. Финуправление в интересах и с согласия субъектов персональных данных в ходе своей деятельности может предоставлять персональные данные (только о субъектах, являющихся его сотрудниками) следующим организациям:

- негосударственным пенсионным фондам;

- негосударственным страховым компаниям;

- кредитным организациям;

- в иные органы и организации в случаях, установленных нормативными правовыми актами, обязательными для исполнения.

 7.4. Муниципальные служащие, работники, ведущие обработку персональных данных, не отвечают на вопросы, связанные с передачей персональных данных по телефону, электронной почте или факсу.

7.5. Передача ПДн может осуществляться в случаях:

наличия согласия в письменной форме субъекта персональных данных;

наличия договора на обработку ПДн субъекта ПДн третьей стороной, существенным условием которого является обязанность обеспечения указанной третьей стороной конфиденциальности ПДн и безопасности ПДн при их обработке;

предусмотренных федеральными законами, если это необходимо в целях защиты основ конституционного строя Российской Федерации, обеспечения обороны страны и безопасности государства;

исполнения договора, стороной которого является субъект ПДн;

защиты жизни, здоровья, иных жизненно важных интересов субъекта ПДн или других лиц при невозможности получения согласия в письменной форме субъекта ПДн.

7.6.При обнаружении нарушений передачи ПДн обработка ПДн приостанавливается и проводится разбирательство в соответствии с Положением о порядке выявления и реагирования на инциденты информационной безопасности в Финансовом управлении Администрации Белокалитвинского района.

8. Права субъектов персональных данных

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

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

подтверждение факта обработки персональных данных Оператором;

правовые основания и цели обработки персональных данных;

цели и применяемые оператором способы обработки персональных данных;

наименование и место нахождения оператора, сведения о лицах (за исключением работников Оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании Федерального закона № 152-ФЗ;

обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен Федеральным законом № 152-ФЗ;

сроки обработки персональных данных, в том числе сроки их хранения;

порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом № 152-ФЗ;

информацию об осуществленной или о предполагаемой трансграничной передаче данных;

наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;

иные сведения, предусмотренные действующим законодательством Российской Федерации в области персональных данных.

8.3. В целях обеспечения защиты персональных данных субъекты имеют право:

требовать от Оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав;

требовать предоставления сведений, указанных в пункте 8.2, от Оператора 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;

требовать предоставления сведений, указанных в пункте 8.2, от Оператора 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 оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных оператором, 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;

требовать исключения или исправления неверных или неполных персональных данных, а также данных, обработанных с нарушением законодательства;

заявить в письменной форме о своем несогласии, представив соответствующее обоснование (при отказе оператора или уполномоченного им лица исключить или исправить персональные данные субъекта);

требовать от Оператора или уполномоченного им лица уведомления всех лиц, которым ранее были сообщены неверные или неполные персональные данные субъекта, обо всех произведенных в них изменениях или исключениях из них;

обжаловать в суд любые неправомерные действия или бездействие оператора или уполномоченного им лица при обработке и защите персональных данных субъекта.

8.4. Субъект персональных данных или его законный представитель обязаны предоставлять персональные данные, соответствующие действительности.

8.5. Для реализации вышеуказанных прав субъект персональных данных, может в порядке, установленном ст. 14 Федерального закона № 152-ФЗ, обратиться в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности персональных данных (Роскомнадзор) с соответствующим запросом.

8.6. Если субъект персональных данных считает, что Оператор осуществляет обработку его персональных данных с нарушением требований Федерального закона № 152-ФЗ или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие Оператора в вышестоящий орган, в органы прокуратуры или в судебном порядке.

9. Правила рассмотрения запросов субъектов персональных данных или их представителей, запросов уполномоченного органа по защите прав субъектов персональных данных

9.1. Субъекты ПДн, персональные данные которых обрабатываются в Финуправлении в целях, определенных настоящим Положением, имеют право на получение информации, касающейся обработки их персональных данных, предусмотренной законодательством Российской Федерации.

9.2. При получении запроса субъекта персональных данных (его законного представителя), запроса уполномоченного органа по защите прав субъектов персональных данных Финуправления:

подтверждает наличие ПДн,

осуществляет ознакомление с ПДн,

производит уточнение ПДн,

производит уничтожение или отзыв согласия на обработку ПДн,

производит устранение нарушений законодательства, допущенных при обработке ПДн.

9.3. Субъекты персональных данных, вправе требовать от Оператора 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.

Сведения должны быть предоставлены субъекту ПДн Оператором в доступной форме. Указанные сведения не должны содержать персональные данные, относящиеся к другим субъектам ПДн, за исключением случаев наличия законных оснований для раскрытия таких персональных данных.

Сведения предоставляются субъекту ПДн (или его представителю) лицом, ответственным за организацию обработки персональных данных или руководителем Финуправления.

9.4. Запрос должен содержать:

номер основного документа, удостоверяющего личность субъекта ПДн или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе;

сведения о документе, подтверждающем, что субъект ПДн состоит в правоотношениях с Оператором (документ, подтверждающий прием документов на участие в конкурсе на замещение вакантных должностей муниципальной службы, иной документ), либо сведения, подтверждающие факты обработки персональных данных субъекта ПДн в Финуправлении;

подпись субъекта ПДн или его представителя.

Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

В случае неправильно составленного или неполного запроса, или при отсутствии документов, удостоверяющих личность субъекта ПДн (его законного представителя), муниципальный служащий, работник Финуправления осуществляющий обработку персональных данных вправе отказать в приеме запроса.

При отказе субъекта ПДн или его законного представителя переделать запрос, муниципальный служащий, работник Финуправления, осуществляющий обработку персональных данных делает об этом запись в «Журнале учета обращений граждан».

9.5. Запрос, предоставляемый субъектом ПДн, должен быть подготовлен в произвольной форме.

9.6. При получении запроса муниципальный служащий, работник Финуправления, осуществляющий обработку персональных данныхвыполняет следующие действия:

9.6.1. регистрирует запрос в «Журнале учета обращений граждан»;

9.6.2. сверяет сведения в запросе с предоставленными ему документами.

9.7. При получении запроса субъекта персональных данных или его представителя на наличие ПДн необходимо в течение 30 (тридцати) дней с даты получения запроса подтвердить обработку ПДн, в случае ее осуществления.

Если обработка ПДн субъекта не ведется, то в течение 30 (тридцати) дней с даты получения запроса необходимо отправить уведомление об отказе подтверждения обработки ПДн.

9.8. При получении запроса субъекта ПДн или его представителя на ознакомление с ПДн необходимо в течение 30 (тридцати) дней с даты получения запроса предоставить для ознакомления ПДн.

Если обработка ПДн субъекта ПДн не ведется, то в течение 30 (тридцати) дней с даты получения запроса необходимо отправить уведомление об отказе предоставления информации по ПДн.

9.9. При получении запроса субъекта персональных данных или его представителя на уточнение ПДн, необходимо внести в них изменения в срок, не превышающий 7 (семи) рабочих дней со дня предоставления субъектом ПДн или его представителем сведений, подтверждающих, что ПДн являются неполными, неточными или неактуальными.

После внесения изменений субъекту ПДн или его представителю отправляется уведомление о внесенных изменениях.

Если обработка ПДн субъекта ПДн не ведется, или не были предоставлены сведения, подтверждающие, что ПДн, которые относятся к соответствующему субъекту и обработку которых осуществляет Финуправление, являются неполными, неточными или неактуальными, то необходимо в течение 30 (тридцати) дней с даты получения такого запроса направить уведомление об отказе осуществления изменения ПДн.

9.10. При получении от субъекта ПДн запроса на отзыв согласия на обработку его ПДн, необходимо прекратить обработку ПДн субъекта ПДн, уничтожить ПДн субъекта ПДн в срок, не превышающий 30 (тридцати) дней с даты поступления указанного запроса за исключением случаев:

- если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн;

- если иное не предусмотрено соглашением между Финуправлением и субъектом ПДн;

- если Финуправление не вправе осуществлять обработку персональных данных субъекта ПДн без его согласия по основаниям, предусмотренным Федеральным законом № 152-ФЗ или другими федеральными законами.

9.11. При выявлении недостоверности ПДн при обращении или по запросу субъекта ПДн (его представителя) необходимо блокировать ПДн с момента такого обращения или получения такого запроса на период проверки.

Если факт недостоверности ПДн подтвержден на основании сведений, представленных субъектом ПДн или его представителем, либо уполномоченным органом по защите прав субъектов персональных данных, или на основании иных документов, необходимо уточнить персональные данные в течение 7 (семи) рабочих дней со дня представления такого запроса.

Если факт недостоверности ПДн не подтвержден, то необходимо отправить уведомление об отказе изменения ПДн.

9.12. При выявлении неправомерных действий Оператора при обращении или по запросу субъекта ПДн (его представителя) в срок, не превышающий 3 (трех) рабочих дней со дня этого выявления, Оператор обязан прекратить неправомерную обработку персональных данных.

В случае, если обеспечить правомерность обработки персональных данных невозможно, Оператор в срок, не превышающий 10 (десяти) рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные.

Об устранении допущенных нарушений или об уничтожении персональных данных Оператор обязан уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также и в указанный орган.

9.13. При достижении целей обработки ПДн Оператор обязан незамедлительно прекратить обработку ПДн, и уничтожить соответствующие ПДн в срок, не превышающий 30 (тридцати) дней с даты достижения цели обработки ПДн, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, иным соглашением между Финуправлением и субъектом ПДн.

9.14. В случае поступления Запроса Уполномоченного органа по защите прав субъекта ПДн по персональным данным необходимо выполнить следующие действия:

зарегистрировать запрос в «Журнале учета обращений граждан»;

в течение тридцати дней предоставить информацию, необходимую для осуществления деятельности указанного органа;

при выявлении недостоверных ПДн при обращении или по запросу уполномоченного органа по защите прав субъекта ПДн необходимо их блокировать с момента такого обращения или получения такого запроса на период проверки. Если факт недостоверности ПДн подтвержден на основании документов, предоставленных субъектом ПДн или его законным представителем, необходимо в течении 7 (семи) рабочих дней уточнить ПДн и снять их блокирование. Если факт недостоверности ПДн не подтвержден, то необходимо отправить уведомление об отказе изменения и снять блокирование ПДн;

при выявлении неправомерных действий с ПДн Орган власти при обращении или по запросу уполномоченного органа по защите прав субъекта ПДн необходимо прекратить неправомерную обработку в срок, не превышающий 3 (трех) рабочих дней, с момента такого обращения или получения такого запроса на период проверки. В случае невозможности обеспечения правомерности обработки ПДн Финуправление в срок, не превышающий десяти рабочих дней с даты выявления неправомерности действий с ПДн, необходимо уничтожить ПДн и отправить уведомление об уничтожении ПДн.

9.15. В случае, если информация об обрабатываемых персональных данных была предоставлена субъекту ПДн по его запросу, он вправе обратиться повторно в Финуправление или направить повторный запрос в целях получения указанных сведений не ранее, чем через 30 (тридцать) дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн.

9.16. Субъект ПДн вправе обратиться повторно в Финуправление или направить повторный запрос до истечения срока, указанного в пункте 9.15. настоящего Положения, в случае, если такие необходимые сведения были ему предоставлены не в полном объеме по результатам рассмотрения первоначального обращения.

Повторный запрос должен содержать обоснование направления повторного запроса.

9.17. Оператор вправе отказать субъекту ПДн в выполнении повторного запроса, не соответствующего условиям, предусмотренным пунктом 9.4 настоящего Положения. Такой отказ должен быть мотивированным.

9.18. Право субъекта ПДн 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.

10. Лица, ответственные за выполнение требований по обработке и обеспечению безопасности персональных данных в Финуправлении

10.1. Ответственность за выполнение требований в области информационной безопасности персональных данных в Финуправлении возлагается:

10.1.1. за организацию обработки персональных данных - на заместителя начальника Финуправления;

10.1.2. за координацию деятельности в сфере защиты персональных данных в Финуправлении - на постоянно действующую техническую комиссию (далее – ПДТК);

10.1.3. за обработку персональных данных - на руководителей структурных подразделений Финуправления, обрабатывающих персональные данные;

10.1.4. за выполнение требований по безопасности персональных данных при осуществлении обработки персональных данных ~~-~~ на муниципальных служащих, работников структурных подразделений Финуправления, обрабатывающих персональные данные;

10.1.5. за неразглашение персональных данных, ставших им известными в процессе трудовой деятельности – на лиц, имеющих доступ к персональным данным;

10.1.6. за контроль над выполнением требований по безопасности ПДн, непосредственное осуществление мероприятий по обеспечению защиты ПДн в Финуправлении - на администратора информационной безопасности.

10.2. Лицо, ответственное за организацию обработки персональных данных в Финуправлении в целях обеспечения информационной безопасности персональных данных обязано:

контролировать выполнение работ по информационной безопасности в Финуправлении, которые должны соответствовать требованиям законодательства Российской Федерации, руководящих и методических документов Федеральной службы по техническому и экспортному контролю (далее – ФСТЭК России) и Федеральной службой безопасности Российской Федерации (далее - ФСБ России), организационно-распорядительных документов Финуправления, а также настоящего Положения;

контролировать работу администратора информационной безопасности;

контролировать состав и сроки исполнения работ по обеспечению безопасности ПДн в Финуправлении в соответствии с требованиями законодательства Российской Федерации, руководящих и методических документов ФСТЭК России и ФСБ России, организационно-распорядительных документов Финуправления, а также настоящего Положения;

осуществлять координацию и руководство работой ПДТК;

инициировать проверки по фактам обнаружения инцидентов ИБ;

принимать решение по проведению расследования инцидентов ИБ;

согласовывать проекты организационно – распорядительной документации Финуправления, касающейся вопросов обеспечения безопасности персональных данных;

инициировать приостановку обработки персональных данных пользователями ИСПДн при обнаружении нарушений порядка обработки персональных данных;

инициировать проведение служебных проверок по фактам несоблюдения условий, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности ПДн.

10.3. Лицо, ответственное за обработку персональных данных Финуправления обязано:

осуществлять контроль за соблюдением пользователями ИСПДн требований организационно-распорядительных документов Финуправления;

соблюдать требования законодательства Российской Федерации, руководящих и методических документов, организационно-распорядительных документов Финуправления в области обеспечения безопасности ПДн, а также настоящего Положения;

осуществлять контроль за соответствием Перечня реальному штатному расписанию Финуправления, своевременно вносить в него изменения;

инициировать внесение изменений в состав ИСПДн при возникновении служебной необходимости;

своевременно информировать администратора информационной безопасности о любых нарушениях в работе ИСПДн или подозрениях на возникновение инцидента ИБ;

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;

принимать необходимые меры по восстановлению нарушенных прав субъектов персональных данных;

осуществлять взаимодействие по обеспечению безопасности персональных данных с администратором информационной безопасности.

10.4. Лицо, ответственное за контроль над выполнением требований по безопасности ПДн, непосредственное осуществление мероприятий по обеспечению защиты ПДн в Финуправлении (администратор информационной безопасности) осуществляет:

анализ и выявление возможных каналов утечки информации и воздействия на информационные ресурсы и процессы на объектах информатизации;

классификацию информационных систем персональных данных;

выполнение организационно-технических мер защиты информации на объектах информатизации;

контроль за эксплуатацией средств защиты информации ИСПДн;

разработку на базе руководящих и методических документов по технической защите информации организационно-распорядительных документов, определяющих порядок и мероприятия по защите информации на АРМ ИСПДн;

контроль выполнения требований по защите информации при эксплуатации АРМ ИСПДн;

организацию парольной защиты;

организацию учета средств защиты информации, эксплуатационной и технической документации к ним;

инструктаж пользователей ИСПДн о порядке и правилах использования средств защиты информации, включая средства антивирусной защиты;

администрирование средств и систем защиты персональных данных в ИСПДн, включая средства антивирусной защиты;

учет лиц, допущенных к работе с персональными данными в ИСПДн;

учет электронных носителей персональных данных, используемых в ИСПДн;

обработку ПДн муниципальных служащих и работников Финуправления для изготовления сертификатов проверки ключей электронной подписи, необходимых в ходе служебной деятельности;

организацию принятия правовых, организационных и технических мер для обеспечения защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных;

доведение до сведения пользователей ИСПДн положений законодательства Российской Федерации в области персональных данных, организационно-распорядительных документов Финуправления по вопросам обработки персональных данных, требований к защите персональных данных.

10.5. Муниципальные служащие, работники структурных подразделений Финуправления, обрабатывающие персональные данные - пользователи ИСПДн, обязаны:

знать и выполнять требования законодательства Российской Федерации, руководящих и методических документов и организационно-распорядительных документов Финуправления в области обеспечения безопасности ПДн;

осуществлять обработку персональных данных только после получения разрешения;

использовать для обработки ПДн только учтенные съемные машинные носители информации;

соблюдать утвержденную разрешительную систему доступа к ИСПДн Финуправления;

знать и уметь правильно использовать то аппаратно-программное обеспечение, которое установлено на его автоматизированной рабочем месте, а также строго выполнять правила работы со средствами защиты информации, установленными на них;

хранить в тайне свой пароль (пароли).

10.6. Лица, имеющие доступ к персональным данным обязаны хранить в тайне персональные данные, ставшие им известными в процессе трудовой деятельности.

11. Правила работы с обезличенными персональными данными

11.1. В соответствии со статьей 3 Федерального закона № 152-ФЗ под обезличиванием персональных данных понимаются действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

11.2. Обезличивание персональных данных может быть проведено с целью ведения статистических данных, снижения ущерба от разглашения защищаемых персональных данных, снижения класса ИСПДн и по достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральными законами.

11.3. Обезличивание персональных данных осуществляется в соответствии с требованиями и методами по обезличиванию персональных данных, утвержденных приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 05.09.2013 № 996.

11.4. Методы обезличивания должны обеспечивать требуемые свойства обезличенных данных, соответствовать предъявляемым требованиям к их характеристикам (свойствам), быть практически реализуемыми в различных программных средах и позволять решать поставленные задачи обработки персональных данных.

11.5. Лица, на которых возложены обязанности за проведение мероприятий по обезличиванию обрабатываемых персональных данных в Финуправлении, указаны в приказе «О перечне должностей финансового управления Администрации Белокалитвинского района, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных».

 11.6. Обезличенные персональные данные могут обрабатываться с использованием и без использования средств автоматизации.

12. Блокирование, обезличивание и уничтожение

персональных данных

12.1. В случае достижения целей обработки персональных данных или в случае утраты необходимости в их достижении уполномоченное должностное лицо обязано:

незамедлительно прекратить обработку персональных данных;

уничтожить либо обезличить соответствующие персональные данные в срок, не превышающий 30 дней с даты достижения целей обработки персональных данных.

Персональные данные не уничтожаются (не обезличиваются) в случаях, если:

договором, соглашением стороной которого, выгодоприобретателем или поручителем является субъект персональных данных, предусмотрен иной порядок обработки персональных данных;

законодательством установлены сроки обязательного архивного хранения материальных носителей персональных данных;

в иных случаях, прямо предусмотренных законодательством.

12.2. Обезличивание или уничтожение части персональных данных, если это допускается материальным носителем, производится способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных персональных данных, зафиксированных на этом же материальном носителе.

12.3. В случае выявления недостоверности персональных данных, неправомерности действий с персональными данными осуществляется немедленное блокирование указанных персональных данных.

В срок, не превышающий трех рабочих дней с даты такого выявления, допущенные нарушения устраняются.

В случае подтверждения факта недостоверности персональных данных лицо, обрабатывающее ПДн в Финуправлении уточняет персональные данные и снимает с них блокирование на основании документов, представленных:

субъектом персональных данных (его законным представителем);

уполномоченным органом по защите прав субъектов персональных данных;

иными лицами.

12.4. В случае невозможности устранения допущенных нарушений лицо, ответственное за обработку персональных данных в срок, не превышающий десяти рабочих дней с даты выявления неправомерности действий с персональными данными, уничтожает персональные данные.

Об устранении допущенных нарушений или об уничтожении персональных данных лицо, ответственное за обработку персональных данных уведомляет субъекта персональных данных (его законного представителя) и (или) уполномоченный орган по защите прав субъектов персональных данных.

12.5. В случае отзыва субъектом персональных данных согласия на обработку своих персональных данных лицо, ответственное за обработку персональных данных обязано прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий тридцати рабочих дней с даты поступления указанного отзыва, если иное не предусмотрено законодательством, договором или соглашением между Оператором и субъектом персональных данных. Об уничтожении персональных данных лицо, ответственное за обработку персональных данных уведомляет субъекта персональных данных (его законного представителя).

12.6. Документы, содержащие персональные данные, утратившие свое практическое значение и не подлежащие архивному хранению, уничтожаются.

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

13. Порядок доступа в помещения, в которых

осуществляется обработка персональных данных

13.1. Обеспечение безопасности помещений, где расположены ИСПДн и ведется обработка персональных данных (далее - помещения), направлено на исключение возможности несанкционированного доступа к техническим средствам ИСПДн, их хищения и нарушения работоспособности, хищения носителей информации.

13.2.Распоряжением \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ определены границы контролируемой зоны, на территории которой исключено бесконтрольное пребывание посторонних лиц.

13.3. Реализация режима безопасности помещений возлагается на лиц, работающих в данных помещениях.

13.4. Помещения должны соответствовать следующим требованиям:

обеспечивать сохранность технических средств;

исключать возможность бесконтрольного проникновения в помещения;

исключать возможность визуального просмотра обрабатываемой информации посторонними лицами.

13.5. Допуск в помещения обслуживающего персонала для выполнения хозяйственных и ремонтных работ, осуществляется только в присутствии муниципальных служащих, работников Финуправления, обрабатывающих персональные данные и имеющих автоматизированные рабочие места ИСПДн в данных помещениях.

При этом должна быть исключена возможность бесконтрольного доступа в помещения и непосредственно к ИСПДн, несанкционированного ознакомления, обзора обрабатываемых персональных данных, обеспечена гарантированная сохранность элементов ИСПДн, накопителей и носителей информации.

13.6. По окончании рабочего времени помещения запираются на ключ и пломбируются печатью.

Печати выдаются Администратором безопасности (?) под роспись в журнале учета печатей, согласно Перечню.

13.8. Вскрытие и закрытие (опечатывание) помещений осуществляется муниципальными служащими, работниками Финуправления, обрабатывающими персональные данные и имеющими автоматизированные рабочие места ИСПДн в данных помещениях.

13.8.1. Перед уходом по окончании рабочего времени лица, непосредственно обрабатывающие персональные данные, обязаны:

убрать бумажные и электронные носители, содержащие персональные данные, в запираемые шкафы или сейфы;

отключить технические средства обработки информации и электроприборы от сети.

Лицо, покидающее помещение последним, обязано:

закрыть окна;

выключить освещение;

закрыть двери помещения;

опечатать помещение.

13.8.2. Перед открытием помещения первый прибывший муниципальный служащий, работник, имеющий автоматизированное рабочее место ИСПДн в данном помещении, обязан:

провести внешний осмотр двери и дверного замка и опечатывающего устройства с целью установления их целостности;

открыть дверь и осмотреть помещение;

проверить наличие и целостность замков на запираемых шкафах и сейфах.

13.8.3. При обнаружении факта взлома двери (дверного замка) и (или) нарушения целостности печати в опечатывающем устройстве помещения необходимо:

не вскрывая помещение, незамедлительно сообщить о данном факте лицу, ответственному за обработку персональных данных;

вызвать работников охраны здания;

в присутствии не менее двух лиц и лица, ответственного за обработку персональных данных, вскрыть помещение и осмотреть его;

составить акт о факте взлома двери (дверного замка) и (или) нарушения целостности печати в опечатывающем устройстве и передать его лицу, ответственному за организацию обработки персональных данных в Финуправлении.

13.9. В случае необходимости принятия экстренных мер при авариях в системах энерго-, водо- и теплоснабжения в выходные или нерабочие праздничные дни помещения вскрываются лицом, имеющим доступ к данному помещению в присутствии сотрудника охраны \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

При этом незамедлительно ставятся в известность лица, ответственные за организацию обработки персональных данных, за обработку персональных данных и администратор информационной безопасности.

13.10. Запрещается передавать ключи от помещений третьим лицам.

13.11. Ответственность и контроль за соблюдением порядка доступа в помещения возлагается на лиц, ответственных за обработку персональных данных.

14. Гарантии конфиденциальности

14.1. Информация, относящаяся к персональным данным, является конфиденциальной и охраняется законом.

14.2. Муниципальные служащие, работники Финуправления, получившие доступ к персональным данным, несут персональную дисциплинарную, административную, гражданско-правовую или уголовную ответственность в случае нарушения норм и требований действующего законодательства Российской Федерации, регулирующего правила обработки и защиты персональных данных.

15. Контроль эффективности защиты ПДн

15.1. Контроль эффективности средств (систем) защиты информации предусматривает инструментальную проверку функционирования технических средств на соответствие установленным требованиям и нормам безопасности персональных данных.

Контроль заключается в проверке выполнения требований нормативных документов по защите информации, а также в оценке обоснованности и эффективности принятых мер.

15.2. Осуществляемые в Финуправлении контрольно-проверочные мероприятия должны включать:

систематическую проверку технического состояния средств защиты, а также мер, предотвращающих несанкционированный доступ к ним и нарушение режимов их эксплуатации;

**Лист ознакомления**

с Положением об обработке персональных данных в

финансовом управлении Администрации Белокалитвинского района

(утв. приказом от \_\_\_\_\_\_\_\_\_\_\_\_ N \_\_\_\_\_\_\_)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № | ФИО | Должность | Дата ознакомления | Подпись |
| 1 | Самойлова О.В. | Заместитель начальника – начальник бюджетного отдела | \_\_\_.\_\_\_.2022 |  |
| 2 | Паршина Т.М. | Главный специалист | \_\_\_.\_\_\_.2022 |  |
| 3 | Минаева Е.И. | Главный специалист | \_\_\_.\_\_\_.2022 |  |
| 4 | Колесникова С.Н. | Главный специалист | \_\_\_.\_\_\_.2022 |  |
| 5 | Мигулина Н.В. | Ведущий специалист | \_\_\_.\_\_\_.2022 |  |
| 6 | Шляхтина А.А. | Ведущий специалист | \_\_\_.\_\_\_.2022 |  |
| 7 | Голотвина А.В. | Главный специалист | \_\_\_.\_\_\_.2022 |  |
| 8 | Сусел С.И. | Начальник отдела учета исполнения бюджета – главный бухгалтер | \_\_\_.\_\_\_.2022 |  |
| 9 | Дьяконов А.В. | Главный специалист | \_\_\_.\_\_\_.2022 |  |
| 10 | Багаева С.А. | Ведущий специалист | \_\_\_.\_\_\_.2022 |  |
| 11 | Склярова В.В. | Ведущий специалист | \_\_\_.\_\_\_.2022 |  |
| 12 | Алексеева И.В. | Ведущий специалист | \_\_\_.\_\_\_.2022 |  |
| 14 | Кнурева Т.И. | Начальник отдела прогнозирования доходов и налоговой политики | \_\_\_.\_\_\_.2022 |  |
| 15 | Романова Л.И. | Главный специалист | \_\_\_.\_\_\_.2022 |  |
| 16 | Михеева И.А. | Главный специалист | \_\_\_.\_\_\_.2022 |  |
| 17 | Кроликова Ю.Г. | Ведущий специалист | \_\_\_.\_\_\_.2022 |  |
| 18 | Ившин А.М. | Начальник сектора информатизации | \_\_\_.\_\_\_.2022 |  |
| 19 | Казьмин Э.В. | Главный специалист | \_\_\_.\_\_\_.2022 |  |
| 20 | Ткаченко Ю.М. | Старший инспектор | \_\_\_.\_\_\_.2022 |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |