АДМИНИСТРАЦИЯ ИЗОБИЛЬНЕНСКОГО ГОРОДСКОГО ОКРУГА СТАВРОПОЛЬСКОГО КРАЯ

ПОСТАНОВЛЕНИЕ
от 10 апреля 2018 г. № 465

О МЕРАХ, НАПРАВЛЕННЫХ НА РЕАЛИЗАЦИЮ ПОСТАНОВЛЕНИЯ ПРАВИТЕЛЬСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ ОТ 21 МАРТА 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»

В соответствии с федеральными законами от 27 июля 2006 года № 152-ФЗ «О персональных данных», от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и защите информации», постановлением Правительства Российской Федерации от 21 марта 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», администрация Изобильненского городского округа Ставропольского края

ПОСТАНОВЛЯЕТ:

1. Утвердить прилагаемые:

1.1. Правила обработки персональных данных в администрации Изобильненского городского округа Ставропольского края.

1.2. Правила рассмотрения запросов субъектов персональных данных или их представителей в администрации Изобильненского городского округа Ставропольского края.

1.3. Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» в администрации Изобильненского городского округа Ставропольского края.

1.4. Правила работы с обезличенными данными в случае обезличивания персональных данных в администрации Изобильненского городского округа Ставропольского края.

1.5. Порядок доступа сотрудников администрации Изобильненского городского округа Ставропольского края в помещения, в которых ведется обработка персональных данных.

1.6. Перечень информационных систем персональных данных в администрации Изобильненского городского округа Ставропольского края.

1.7. Перечень персональных данных, обрабатываемых в администрации Изобильненского городского округа Ставропольского края в связи с реализацией служебных и трудовых отношений, а также в связи с оказанием муниципальных услуг и осуществлением государственных муниципальных функций.

1.8. Перечень должностей в администрации Изобильненского городского округа Ставропольского края, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных.

1.9. Перечень должностей администрации Изобильненского городского округа Ставропольского края, замещение которых предусматривает осуществление обработки персональных данных, либо осуществления доступа к персональным данным.

1.10. Инструкцию ответственного за организацию обработки и защиту персональных данных в администрации Изобильненского городского округа Ставропольского края.

1.11. Форму типового обязательства должностного лица администрации Изобильненского городского округа Ставропольского края, 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.

1.12. Типовую форму согласия на обработку персональных данных муниципальных служащих администрации Изобильненского городского округа Ставропольского края, а также иных субъектов персональных данных.

1.13. Типовую форму разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные.

1.14. Типовую форму обязательства о неразглашении персональных данных.

1.15. Отзыв согласия на обработку персональных данных.

2. Контроль за выполнением настоящего постановления оставляю за собой.

3. Настоящее постановление вступает в силу со дня его подписания.

Глава Изобильненского городского
округа Ставропольского края В.И.КОЗЛОВ

Утверждены
постановлением администрации
Изобильненского городского
округа Ставропольского края
от 10 апреля 2018 г. № 465

ПРАВИЛА ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В АДМИНИСТРАЦИИ ИЗОБИЛЬНЕНСКОГО ГОРОДСКОГО ОКРУГА СТАВРОПОЛЬСКОГО КРАЯ

1. Основные понятия

В настоящем документе используются следующие основные понятия:

автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники;

безопасность персональных данных – состояние защищённости персональных данных, при котором обеспечиваются их конфиденциальность, доступность и целостность при их обработке;

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

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 распространения без согласия субъекта персональных данных или наличия иного законного основания;

несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своим функциональному предназначению и техническим характеристикам;

обработка персональных данных – любое действие (операция) или совокупность действий, 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 (в том числе 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;

персональные данные – любая информация, относящаяся прямо или косвенно к определённому или определяемому физическому лицу (субъекту персональных данных);

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

распространение персональных данных – действия, направленные на раскрытие персональных данных неопределённому кругу лиц;

технические средства информационной системы персональных данных - средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приёма и обработки персональных данных (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 управления базами данных и т.п.), средства защиты информации;

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

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.

2. Общие положения

Настоящие правила разработаны для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных администрации Изобильненского городского округа Ставропольского края (далее – администрация), а также защиты прав и свобод граждан при обработке их персональных данных в администрации, в том числе право на неприкосновенность частной жизни, личную и семейную тайну, а также разъяснение ответственности должностных лиц, имеющих доступ к персональным данным, за невыполнение требований норм и правил, регулирующих обработку и защиту персональных данных.

Настоящие правила устанавливают порядок обработки персональных данных субъектов персональных данных в администрации и направлены на выявление, предотвращение и профилактику нарушений законодательства Российской Федерации в сфере персональных данных.

Субъектами персональных данных в администрации являются:

1) граждане, обратившиеся в администрацию;

Настоящие правила определяют необходимый минимальный объём мер, соблюдение которых позволяет предотвратить утечку сведений, относящихся к персональным данным. При необходимости могут быть введены дополнительные

меры, направленные на усиление защиты персональных данных.

Настоящие правила разработаны в соответствии со следующими нормативно-правовыми актами Российской Федерации:

1) Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных от 28 января 1981 года с поправками, одобренными Комитетом министров Совета Европы 15 июня 1999 года, ратифицированная Федеральным законом Российской Федерации от 19 декабря 2005 года № 160-ФЗ "О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных" в рамках, определяемых данным Федеральным законом, заявлений;

2) Конституция Российской Федерации;

3) Гражданский кодекс Российской Федерации;

4) Кодекс об административных правонарушениях Российской Федерации;

5) Трудовой кодекс Российской Федерации;

6) Уголовный кодекс Российской Федерации;

7) Федеральный закон от 27 июля 2004 года № 79-ФЗ "О государственной гражданской службе Российской федерации";

8) Федеральный закон от 27 июля 2006 года № 152-ФЗ "О персональных данных" (далее – Федеральный закон № 152-ФЗ);

9) Федеральный закон от 27 июля 2006 года № 149-ФЗ "Об информации, информационных технологиях и о защите информации";

10) Перечень сведений конфиденциального характера, утвержденный Указом Президента Российской Федерации от 06 марта 1997 г. № 188;

11) Положение об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации, утверждённое постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687;

12) Перечень 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, утверждённый постановлением Правительства Российской Федерации от 21 марта 2012 г. № 211;

13) Требования к защите персональных данных при их обработке в информационных системах персональных данных, утвержденные постановлением Правительства Российской Федерации от 01 ноября 2012 г. № 1119.

В соответствии с законодательством Российской Федерации об обработке и защите персональных данных персональные данные субъектов являются конфиденциальной информацией.

В случаях, предусмотренных действующим законодательством, сведения о доходах, об имуществе и обязательствах имущественного характера гражданского служащего, его супруги (супруга) и несовершеннолетних детей могут размещаться на официальном сайте администрации или предоставляться региональным средствам массовой информации по их запросам для последующего опубликования.

Порядок регистрации, учёта, оформления, тиражирования, хранения, использования и уничтожения документов и других материальных носителей персональных данных определяют законодательство Российской Федерации об обработке и защите персональных данных, а также действующие нормативные правовые акты администрации.

Администрация является оператором персональных данных субъектов,

указанных в настоящем документе. На основании соглашения (договора) администрация может поручать обработку персональных данных третьим лицам, с согласия субъекта персональных данных, а в случае если иное предусмотрено действующим законодательством Российской Федерации, то и без их согласия. Существенным условием соглашения (договора) по обработке персональных данных является обязанность обеспечения этими лицами конфиденциальности и безопасности персональных данных субъектов.

В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьёй 24 Конституции Российской Федерации, администрация вправе получать и обрабатывать данные о частной жизни муниципальных служащих и (или) сотрудников администрации только с их письменного согласия.

Администрация не имеет права получать и обрабатывать персональные данные субъекта о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных законодательством Российской Федерации.

Настоящие Правила вступают в силу со дня их утверждения и действуют до замены их новыми правилами обработки персональных данных.

Все изменения в правила вносятся постановлением администрации Изобильненского городского округа Ставропольского края.

3. Цель и содержание обработки персональных данных

Целями обработки персональных данных в администрации являются:

1) реализации полномочий, возложенных на орган местного самоуправления федеральным законодательством, законодательством Ставропольского края и нормативно-правовыми актами администрации.

Цель "реализации полномочий, возложенных на орган местного самоуправления федеральным законодательством, законодательством Ставропольского края и нормативно-правовыми актами администрации" достигается посредством обработки персональных данных следующих категорий для следующих субъектов:

1) граждане, обратившиеся в администрацию:

фамилия, имя, отчество, год рождения, дата рождения, место рождения, адрес, контактные сведения, паспортные данные, семейное положение, состав семьи, степень родства, имущественное положение, доходы, информация о трудовой деятельности, трудоспособность, СНИЛС, состояние здоровья, судимость, сведения о счете в банке, сведения об имуществе.

2) контрагенты (физические лица и представители лиц):

фамилия, имя, отчество, год рождения, адрес, контактные сведения, паспортные данные, ИНН, СНИЛС.

3) кандидаты для приёма на работу:

фамилия, имя, отчество, год рождения, дата рождения, место рождения, адрес, контактные сведения, паспортные данные, гражданство, сведения о воинском учёте, семейное положение, состав семьи, степень родства, социальное положение, имущественное положение, доходы, образование, профессия, информация о трудовой деятельности, трудоспособность, ИНН, СНИЛС, судимость.

4) сотрудники:

имущественное положение, год рождения, паспортные данные, социальное положение, доходы, адрес, сведения о воинском учёте, гражданство, информация о трудовой деятельности, контактные сведения, дата рождения, образование, фамилия, имя, отчество, семейное положение, профессия, состав семьи,

трудоспособность, место рождения, степень родства, ИНН, СНИЛС, состояние здоровья, судимость.

5) дети сотрудников:

фамилия, имя, отчество, год рождения, дата рождения, адрес, паспортные данные, доходы, информация о трудовой деятельности.

6) супруги сотрудников:

фамилия, имя, отчество, год рождения, дата рождения, место рождения, адрес, контактные сведения, паспортные данные, семейное положение, степень родства, имущественное положение, доходы, информация о трудовой деятельности.

7) лица, привлекаемые к административной ответственности:

фамилия, имя, отчество, год рождения, дата рождения, место рождения, адрес, контактные сведения, паспортные данные, информация о трудовой деятельности, гражданство, сведения о воинском учёте, семейное положение, состав семьи, степень родства, социальное положение, имущественное положение, образование, профессия, трудоспособность, состояние здоровья, судимость.

8) присяжные заседатели:

фамилия, имя, отчество, дата рождения, адрес.

9) сотрудники подведомственных учреждений и организаций:

фамилия, имя, отчество, год рождения, дата рождения, место рождения, адрес, контактные сведения, паспортные данные, гражданство, сведения о воинском учёте, семейное положение, состав семьи, степень родства, социальное положение, имущественное положение, доходы, образование, профессия, информация о трудовой деятельности, трудоспособность, ИНН, СНИЛС, состояние здоровья, судимость.

4. Правила обработки персональных данных

Все персональные данные субъектов администрация получает на законной основе.

Персональные данные ближайших родственников сотрудников (служащих), необходимые для ведения кадрового учёта, администрация получает от самих сотрудников.

Обработка персональных данных осуществляется в соответствии с действующим законодательством Российской Федерации на основании согласия субъекта персональных данных.

Субъект персональных данных принимает решение о предоставлении своих персональных данных и даёт согласие на их обработку своей волей и в своём интересе.

Администрация оставляет за собой право не осуществлять свои функции в отношении субъекта персональных данных в случае предоставления неполных или недостоверных персональных данных, а также в случае отказа дать письменное согласие на обработку персональных данных.

При установлении договорных отношений с субъектом персональных данных получение письменного согласия на обработку его персональных данных не требуется.

Получение персональных данных субъекта у третьих лиц возможно только при предварительном уведомлении субъекта и с его письменного согласия. Форма согласия утверждается отдельным постановлением.

Персональные данные субъектов администрации обрабатываются в структурных подразделениях в соответствии с исполняемыми функциями.

Доступ к персональным данным, обрабатываемым без использования средств автоматизации, осуществляется в соответствии со списком, утверждённым в порядке, определяемом в администрации.

Доступ к персональным данным, обрабатываемым в информационных системах персональных данных, осуществляется в соответствии со списком, утверждённым в порядке, определяемом в администрации.

Уполномоченные лица, допущенные к персональным данным субъектов администрации, имеют право получать только те персональные данные субъекта, которые необходимы для выполнения конкретных функций, в соответствии с должностными инструкциями указанных лиц.

Обработка персональных данных, осуществляемая без использования средств автоматизации, должна выполняться в соответствии с требованиями Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утверждённого постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687.

Персональные данные при такой их обработке, должны обособляться от иной информации, в частности путём фиксации их на отдельных материальных носителях персональных данных, в специальных разделах или на полях форм (бланков).

Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки.

Хранение материальных носителей персональных данных осуществляется в специально оборудованных шкафах и сейфах.

Персональные данные подлежат уничтожению либо обезличиванию в случаях достижения целей или в случае утраты необходимости в достижении этих целей, отзыва согласия субъекта персональных данных, выявления неправомерной обработки персональных данных, если иное не предусмотрено федеральным законом Российской Федерации.

В срок, не превышающий 7 рабочих дней со дня предоставления субъектом персональных данных или его законным представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, администрация вносит в них необходимые изменения, а также уведомляет субъекта о внесённых изменениях.

Уничтожение персональных данных осуществляется в срок, не превышающий 30 рабочих дней с момента достижения цели обработки персональных данных, если иное не предусмотрено федеральным законом Российской Федерации.

Уничтожение персональных данных осуществляется в срок, не превышающий 30 рабочих дней с момента отзыва согласия субъекта персональных данных.

Уничтожение персональных данных осуществляется в срок, не превышающий 7 рабочих дней с момента представления субъектом персональных данных или его законным представителем сведений, подтверждающих, что персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки.

Уничтожение персональных данных осуществляется в срок, не превышающий 10 рабочих дней с момента выявления неправомерной обработки персональных данных. Администрация уведомляет об этом субъекта или его законного представителя.

Уничтожение персональных данных на бумажных носителях осуществляет комиссия в составе руководителя и сотрудников структурного подразделения,

обрабатывавшего персональные данные субъекта и установившего необходимость уничтожения персональных данных под контролем руководителя этого структурного подразделения.

Способ уничтожения материальных носителей персональных данных определяется комиссией. Допускается применение следующих способов:

1) сжигание;

2) шредирование (измельчение);

При этом составляется «Акт об уничтожения персональных данных». Форма акта утверждается отдельным распоряжением.

При необходимости уничтожения большого количества материальных носителей или применения специальных способов уничтожения допускается привлечение специализированных организаций. В этом случае комиссия администрации должна присутствовать при уничтожении материальных носителей персональных данных. При этом к акту уничтожения необходимо приложить накладную на передачу материальных носителей персональных данных, подлежащих уничтожению, в специализированную организацию.

Уничтожение полей баз данных администрации, содержащих персональные данные субъекта, выполняется по заявке руководителя структурного подразделения, обрабатывавшего персональные данные субъекта и установившего необходимость их уничтожения.

Уничтожение полей баз данных администрации, содержащих персональные данные субъекта, осуществляет комиссия, в состав которой входят лица, ответственные за администрирование автоматизированных систем, которым принадлежат базы данных, сотрудники структурного подразделения, обрабатывавшего персональные данные субъекта и установившего необходимость их уничтожения.

Уничтожение полей баз данных администрации, содержащих персональные данные субъекта, достигается путём затирания информации на носителях информации (в том числе и резервных копиях) или путём механического нарушения целостности носителя информации, не позволяющего произвести считывание или восстановление персональных данных.

Уничтожение архивов электронных документов и протоколов электронного взаимодействия может не производиться, если ведение и сохранность их в течение определённого срока предусмотрены соответствующими нормативными и (или) договорными документами.

При невозможности осуществления затирания информации на носителях допускается проведение обезличивания путём перезаписи полей баз данных, которые позволяют определить субъекта, данными, исключающими дальнейшее определение субъекта.

Контроль выполнения процедур уничтожения персональных данных осуществляет ответственный за организацию обработки персональных данных в администрации.

Обработка биометрических персональных данных (фотография, отпечатки пальцев, сетчатки глаза и другое), в соответствии со статьёй 11 Федерального закона № 152-ФЗ, допускается при наличии согласия субъекта. Форма согласия утверждается отдельным распоряжением.

Решение, порождающее юридические последствия в отношении субъекта персональных данных или иным образом затрагивающее его права и законные интересы, может быть принято на основании исключительно автоматизированной обработки его персональных данных только при наличии согласия в письменной форме субъекта персональных данных.

Сотрудники (служащие) администрации должны быть ознакомлены под

роспись с требованиями законодательства Российской Федерации, касающимися обработки персональных данных, настоящими Правилами и другими документами администрации, устанавливающими порядок обработки персональных данных субъектов, а также права и обязанности в этой области.

5. Передача персональных данных третьим лицам

При обработке персональных данных субъекта должны соблюдаться следующие требования:

1) не сообщать персональные данные субъекта третьей стороне без письменного согласия субъекта. Допускается совмещение формы согласия субъекта с типовыми формами документов, содержащими персональные данные субъекта, при условии соблюдения требований статьи 9 Федерального закона № 152-ФЗ;

2) предупреждать лиц, получающих персональные данные субъекта, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные субъекта, обязаны соблюдать режим конфиденциальности в отношении этих данных.

При необходимости трансграничной передачи персональных данных на территорию иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных данных, администрация запрашивает согласие субъекта в письменной форме.

6. Права субъектов персональных данных

В целях обеспечения своих интересов субъекты имеют право:

1) получать полную информацию о своих персональных данных и обработке этих данных (в том числе автоматизированной);

2) осуществлять свободный бесплатный доступ к своим персональным данным, включая право получать копии любой записи, содержащей персональные данные субъекта, за исключением случаев, предусмотренных Федеральным законом;

3) требовать исключения или исправления неверных, или неполных персональных данных, а также данных, обработанных с нарушением Федерального закона № 152-ФЗ. Субъект персональных данных, при отказе администрации исключить или исправить персональные данные субъекта, имеет право заявлять в письменной форме о своём несогласии, обосновав соответствующим образом такое несогласие. Персональные данные оценочного характера субъект имеет право дополнить заявлением, выражающим его собственную точку зрения;

4) требовать от администрации уведомления всех лиц, которым ранее были сообщены неверные или неполные персональные данные субъекта, обо всех произведённых в них изменениях или исключениях из них;

5) обжаловать в суде любые неправомерные действия или бездействие администрации при обработке и защите персональных данных субъекта.

7. Порядок действий в случае запросов надзорных органов

В соответствии с частью 4 статьи 20 Федерального закона № 152-ФЗ администрация сообщает в уполномоченный орган по защите прав субъектов

персональных данных по его запросу информацию, необходимую для осуществления деятельности указанного органа, в течение тридцати дней с даты получения такого запроса.

Сбор сведений для составления мотивированного ответа на запрос надзорных органов осуществляет ответственный за организацию обработки персональных данных в администрации при необходимости с привлечением сотрудников (служащих) администрации.

В течение установленного законодательством срока ответственный за организацию обработки персональных данных в администрации подготавливает и направляет в уполномоченный орган мотивированный ответ и другие необходимые документы.

8. Защита персональных данных субъекта

Защиту персональных данных субъектов от неправомерного их использования или утраты администрация обеспечивает за счёт собственных средств в порядке, установленном законодательством Российской Федерации.

При обработке персональных данных должны быть приняты необходимые организационные и технические меры по обеспечению их конфиденциальности.

Технические меры защиты персональных данных при их обработке техническими средствами устанавливаются в соответствии с:

1) РД ФСТЭК России – «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденных приказом ФСТЭК России от 18 февраля 2013 года № 21;

2) специальными требованиями и рекомендациями по технической защите конфиденциальной информации (СТР-К), утвержденными приказом Гостехкомиссии России от 30 августа 2002 г. № 282;

3) внутренними документами администрации, действующими в сфере обеспечения информационной безопасности.

Защита персональных данных предусматривает ограничение к ним доступа.

Ответственные за организацию обработки персональных данных, администрирование средств и механизмов защиты, техническое обслуживание информационных систем персональных данных назначаются распоряжением администрации Изобильненского городского округа Ставропольского края.

Руководитель структурного подразделения администрации, осуществляющего обработку персональных данных:

1) несёт ответственность за организацию защиты персональных данных в структурном подразделении;

2) организует изучение уполномоченными сотрудниками нормативных правовых актов по защите персональных данных и требует их неукоснительного исполнения;

3) обеспечивает режим конфиденциальности в отношении персональных данных, обрабатываемых в структурном подразделении (отделе);

4) контролирует порядок доступа к персональным данным в соответствии с функциональными обязанностями сотрудников подразделения.

Сотрудники (служащие), допущенные к персональным данным дают письменное обязательство о неразглашении таких данных.

9. Обязанности лиц, допущенных к обработке персональных данных

Лица, допущенные к работе с персональными данными, обязаны:

1) знать законодательство Российской Федерации в области обработки и защиты персональных данных, нормативные документы администрации по защите персональных данных;

2) сохранять конфиденциальность персональных данных;

3) обеспечивать сохранность закреплённых за ними носителей персональных данных;

4) контролировать срок истечения действия согласий на обработку персональных данных и, при необходимости дальнейшей обработки персональных данных, обеспечивать своевременное получение новых согласий или прекращение обработки персональных данных;

5) докладывать своему непосредственному руководителю структурного подразделения обо всех фактах и попытках несанкционированного доступа к персональным данным и других нарушениях.

10. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных субъектов

Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, привлекаются к материальной, административной, уголовной и гражданско-правовой ответственности, а также к дисциплинарной ответственности в соответствии с действующим законодательством Российской Федерации.

К данным лицам могут быть применены следующие дисциплинарные взыскания:

1) замечание;

2) выговор;

3) увольнение с муниципальной службы.

Утверждены
постановлением администрации
Изобильненского городского
округа Ставропольского края
от 10 апреля 2018 г. № 465

ПРАВИЛА
РАССМОТРЕНИЯ ЗАПРОСОВ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ ИЛИ ИХ ПРЕДСТАВИТЕЛЕЙ В АДМИНИСТРАЦИИ ИЗОБИЛЬНЕНСКОГО ГОРОДСКОГО ОКРУГА СТАВРОПОЛЬСКОГО КРАЯ

При устном обращении, либо письменном запросе субъекта персональных данных или его законного представителя на доступ к персональным данным субъекта, администрация Изобильненского городского округа Ставропольского края (далее – администрация) руководствуется требованиями статей 14, 18 и 20 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», а так же Регламентом порядка действий сотрудников администрации Изобильненского городского округа Ставропольского края при обращении либо при получении запроса субъекта персональных данных или его законного представителя, а также уполномоченного органа по защите прав субъектов персональных данных утвержденным постановлением администрации Изобильненского городского округа Ставропольского края.

Доступ субъекта персональных данных или его законного представителя к персональным данным субъекта администрация предоставляет только под контролем ответственного за организацию обработки персональных данных в администрации.

Обращение субъекта персональных данных или его законного представителя фиксируется в журнале учёта обращений граждан по вопросам обработки персональных данных.

Запрос субъекта персональных данных или его законного представителя фиксируется в журнале учета запросов граждан по вопросам обработки персональных данных.

Ответственный за организацию обработки персональных данных принимает решение о предоставлении доступа субъекту персональных данных или его законному представителю к персональным данным указанного субъекта.

В случае, если данных, предоставленных субъектом или его законным представителем недостаточно для установления его личности или предоставление персональных данных нарушает конституционные права и свободы других лиц, ответственный за организацию обработки персональных данных подготавливает мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 Федерального закона от 27 июля 2006 года № 152-ФЗ "О персональных данных" или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий тридцати рабочих дней со дня обращения субъекта персональных данных или его законного представителя, либо от даты получения запроса субъекта персональных данных или его законного представителя.

Для предоставления доступа субъекта персональных данных или его

законного представителя к персональным данным субъекта ответственный за организацию обработки персональных данных привлекает сотрудника (сотрудников) структурного подразделения, обрабатывающего персональные данные субъекта по согласованию с руководителем этого структурного подразделения.

Сведения о наличии персональных данных администрации предоставляет субъекту персональных данных или его законному представителю в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных. Контроль предоставления сведений субъекту или его законному представителю осуществляет ответственный за организацию обработки персональных данных.

Сведения о наличии персональных данных должны быть предоставлены субъекту персональных данных или его законному представителю при ответе на запрос в течение тридцати дней от даты получения запроса субъекта персональных данных или его законного представителя.

Утверждены
постановлением администрации
Изобильненского городского
округа Ставропольского края
от 10 апреля 2018 г. № 465

ПРАВИЛА ОСУЩЕСТВЛЕНИЯ ВНУТРЕННЕГО КОНТРОЛЯ СООТВЕТСТВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ ТРЕБОВАНИЯМ К ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В АДМИНИСТРАЦИИ ИЗОБИЛЬНЕНСКОГО ГОРОДСКОГО ОКРУГА СТАВРОПОЛЬСКОГО КРАЯ

1. Общие положения

Настоящие правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в администрации Изобильненского городского округа Ставропольского края (далее - правила) разработаны в соответствии с положениями Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» и требованиями по соблюдению 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, утверждёнными постановлением Правительства Российской Федерации от 21 марта 2012 г. № 211, и определяют порядок организации и осуществления контроля выполнения соответствия обработки персональных данных требованиям к защите персональных данных в структурных подразделениях администрации Изобильненского городского округа Ставропольского края (далее – администрация).

Правила обязательны для исполнения всеми должностными лицами администрации, осуществляющими контроль состояния защиты персональных данных.

Контроль выполнения соответствия обработки персональных данных требованиям к защите персональных данных в структурных подразделениях администрации осуществляется с целью определения наличия несоответствий между требуемым уровнем защиты персональных данных и его фактическим состоянием, правильности обработки персональных данных ответственными лицами в структурных подразделениях, а также выработки мер по их устранению и недопущению в дальнейшем.

Контроль осуществляет ответственный за организацию обработки персональных данных в администрации.

Контроль проводится в форме плановых и внеплановых проверок. Внеплановые проверки могут быть контрольными и по частным вопросам.

Контрольные проверки проводятся для установления полноты выполнения рекомендаций плановых проверок.

Проверки по частным вопросам охватывают отдельные направления по защите персональных данных и могут проводиться в случаях, когда стали известны факты несанкционированного доступа, утечки либо утраты персональных данных субъектов или нарушения требований по обработке и защите персональных данных.

Проверки осуществляются ответственным за организацию обработки персональных данных в администрации, либо комиссией, образуемой Главой

Изобильненского городского округа Ставропольского края.

Сроки проведения контрольных проверок доводятся руководителям проверяемых структурных подразделений не позднее, чем за 24 часа до начала проверки.

Проверки по частным вопросам могут проводиться без уведомления руководителей проверяемых подразделений (отделов).

Периодичность и сроки проведения плановых проверок подразделений администрации устанавливаются планом, утверждаемым Главой Изобильненского городского округа Ставропольского края. Сроки проведения плановых проверок доводятся руководителям проверяемых структурных подразделений (отделов) не позднее, чем за 10 суток до начала проверки.

2. Порядок подготовки к проверке

Проверка проводится на основании распоряжения администрации Изобильненского городского округа Ставропольского края. Ответственный за организацию обработки персональных данных в администрации подготавливает предложения по составу комиссии. Проект распоряжения о проверке подготавливает ответственный за организацию обработки персональных данных в администрации.

Проверяющие лица обязаны получить у руководителей проверяемых структурных подразделений информацию об условиях обработки персональных данных, необходимую для достижения целей проверки. Перед началом проверки они должны изучить материалы предыдущих проверок данного структурного подразделения.

3. Порядок проведения проверки

По прибытии в структурное подразделение для проведения проверки председатель комиссии прибывает к руководителю проверяемого структурного подразделения администрации, представляется ему и представляет других прибывших на проверку лиц.

Руководитель проверяемого структурного подразделения обязан оказывать содействие комиссии по проверке и в случае необходимости определяет должностное лицо, ответственное за сопровождение проверки.

На период проведения контрольных мероприятий обработку персональных данных необходимо по возможности прекращать. Допуск проверяющих лиц к конкретным информационным ресурсам, защищаемым сведениям и техническим средствам должен исключать ознакомление проверяющих лиц с конкретными персональными данными.

Общий порядок проведения проверки включает следующее:

1) получение документов о распределении обязанностей по обработке и защите персональных данных, выявление ответственных за обработку и защиту персональных данных и установление факта ознакомления сотрудников проверяемого структурного подразделения со своей ответственностью;

2) получение при содействии сотрудников проверяемого структурного подразделения документов, касающихся обработки и защиты персональных данных в данном структурном подразделении;

3) анализ полученной документации;

4) непосредственная проверка выполнения установленного порядка обработки и защиты персональных данных и требований законодательства Российской Федерации в области защиты персональных данных.

При этом согласовываются конкретные вопросы по объёму, содержанию, срокам проведения проверки, а также каких должностных лиц структурного подразделения необходимо привлечь к проверке и какие объекты следует посетить.

В ходе осуществления контроля выполнения требований по обработке и защите персональных данных в проверяемом структурном подразделении администрации рассматриваются в частности следующие показатели:

1) в части общей организации работ по обработке персональных данных:

а) соответствие информации, указанной в уведомлении об обработке персональных данных и в положении о порядке обработки персональных данных администрации, реальному положению дел;

б) соответствие обрабатываемой и собираемой информации (персональных данных), их полнота, в соответствии с нормативными правовыми актами и локальными актами, принятыми в администрации;

в) наличие нормативных документов по защите персональных данных;

г) знание нормативных документов сотрудниками, имеющими доступ к персональным данным;

д) полнота и правильность выполнения требований нормативных документов администрации сотрудниками, имеющими доступ к персональным данным;

е) наличие документов, определяющих состав сотрудников, ответственных за организацию защиты персональных данных в подразделении, соответствие этих документов реальному штатному составу подразделения, а также подтверждение факта ознакомления ответственных сотрудников с данными документами;

ж) уровень подготовки сотрудников, ответственных за организацию защиты персональных данных в подразделении;

з) наличие согласий на обработку персональных данных субъектов персональных данных. Соответствие объёма персональных данных и сроков обработки целям обработки персональных данных.

2) в части защиты персональных данных в информационных системах персональных данных (далее - ИСПДн):

а) соответствие средств вычислительной техники ИСПДн показателям, указанным в документации на ИСПДн;

б) структура и состав локальных вычислительных сетей, организация разграничения доступа пользователей к сетевым информационным ресурсам, порядок защиты охраняемых сведений при передаче (обмене) персональных данных в сети передачи данных;

в) соблюдение установленного порядка использования средств вычислительной техники ИСПДн;

г) наличие и эффективность применения средств и методов защиты персональных данных, обрабатываемых на средствах вычислительной техники;

д) соблюдение требований, предъявляемых к паролям на информационные ресурсы;

е) соблюдение требований и правил антивирусной защиты средств вычислительной техники;

ж) контроль журналов учёта носителей персональных данных. Сверка основного журнала с дублирующим (если требуется ведение дублирующего учёта носителей);

з) тестирование реализации правил фильтрации межсетевого экрана, процесса регистрации, процесса идентификации и аутентификации запросов, процесса идентификации и аутентификации администратора межсетевого экрана, процесса регистрации действий администратора межсетевого экрана, процесса

контроля за целостностью программной и информационной части, процедуры восстановления настроек межсетевого экрана.

3) в части защиты информационных ресурсов и помещений:

а) правильность отнесения обрабатываемой информации к персональным данным;

б) правильность установления уровня защищенности персональных дынных в информационной системе;

в) закрепление гражданско-правовой ответственности в сфере информационной безопасности и соблюдения режима конфиденциальности персональных данных в правилах внутреннего трудового распорядка, положениях о структурных подразделениях администрации, должностных инструкциях сотрудников (служащих) и трудовых договорах;

г) порядок передачи персональных данных органам государственной власти, местного самоуправления и сторонним организациям (контрагентам);

д) действенность принимаемых мер по защите охраняемых сведений в ходе подготовки материалов к открытому опубликованию и при изготовлении рекламной продукции;

е) состояние конфиденциального делопроизводства, соблюдение установленного порядка подготовки, учёта, использования, хранения и уничтожения документов, содержащих персональные данные;

ж) выполнение требований по правильному оборудованию защищаемых помещений и предотвращению утечки охраняемых сведений при проведении мероприятий конфиденциального характера;

з) соответствие защищаемых помещений их техническим паспортам.

Более подробно вопросы, подлежащие проверке, могут раскрываться в отдельных документах (методических рекомендациях, технологических картах, памятках и т.п.).

Во время проведения проверки, выявленные нарушения требований по обработке и защите персональных данных должны быть по возможности устранены. Проверяющие лица могут дать рекомендации по устранению на месте отмечаемых нарушений и недостатков.

Недостатки, которые не могут быть устранены на месте, включаются в итоговый документ по результатам проверки.

4. Оформление результатов проверки

Результаты проверки оформляются:

1) актом - при проведении проверки комиссией;

2) служебной запиской - при проведении проверки назначенными специалистами.

Акт и/или служебная записка составляется в двух экземплярах и подписывается членами комиссии.

Один экземпляр хранится у ответственного за организацию обработки персональных данных администрации. Второй экземпляр хранится в администрации в установленном порядке. Копия акта о проверке остается в проверяемом структурном подразделении.

Результаты проверок структурных подразделений периодически обобщаются ответственным за организацию обработки персональных данных в администрации и доводятся до руководителей структурных подразделений. При необходимости принятия решений по результатам проверок структурных подразделений на имя главы Изобильненского городского округа Ставропольского края готовятся соответствующие служебные записки

Утверждены
постановлением администрации
Изобильненского городского
округа Ставропольского края
от 10 апреля 2018 г. № 465

ПРАВИЛА
РАБОТЫ С ОБЕЗЛИЧЕННЫМИ ДАННЫМИ В СЛУЧАЕ ОБЕЗЛИЧИВАНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ В АДМИНИСТРАЦИИ ИЗОБИЛЬНЕНСКОГО ГОРОДСКОГО ОКРУГА СТАВРОПОЛЬСКОГО КРАЯ

1. Правила работы с обезличенными данными в случае обезличивания персональных данных в администрации Изобильненского городского округа Ставропольского края (далее – Правила) устанавливают порядок проведения мероприятий в администрации Изобильненского городского округа Ставропольского края (далее – администрация) по обезличиванию персональных данных, порядок и условия работы с обезличенными данными, в случае обезличивания персональных данных.

2. Обезличивание персональных данных и работа с обезличенными данными в администрации поселения осуществляется в соответствии с Федеральным законом от 27 июля 2006 года № 152 «О персональных данных» (далее - Федеральный закон «О персональных данных»), постановлением Правительства Российской Федерации от 21 марта 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», настоящими Правилами и другими нормативными правовыми актами, касающимися обработки персональных данных.

3. Основные понятия и термины, используемые в настоящих Правилах, применяются в том же значении, что и в Федеральном законе «О персональных данных».

4. Целью обезличивания персональных данных в администрации является обеспечение защиты персональных данных граждан 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.

5. Обезличивание персональных данных может быть проведено для решения следующих задач:

получения статистических данных;

снижения ущерба от разглашения защищаемых персональных данных;

снижения класса используемых информационных систем персональных данных.

Кроме того, обезличивание персональных данных может быть проведено по достижении сроков обработки или в случае утраты необходимости в достижении целей обработки, если иное не предусмотрено законодательством Российской Федерации.

5.1. В случае достижения целей обработки персональных данных или в случае утраты необходимости в их достижении должностное лицо администрации поселения, обрабатывающее персональные данные, обязано:

незамедлительно прекратить обработку персональных данных;

обезличить соответствующие персональные данные в срок, не превышающий 30 дней с даты достижения целей обработки персональных данных или утраты необходимости достижения этих целей.

5.2. Персональные данные не обезличиваются в случаях, если:

договором (соглашением), стороной которого либо выгодоприобретателем или поручителем, по которому 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.

5.3. В случае выявления недостоверности персональных данных, неправомерности действий с персональными данными должностное лицо администрации поселения, обрабатывающее персональные данные, обязано осуществить незамедлительное блокирование указанных персональных данных и в срок, не превышающий 3 рабочих дней с даты такого выявления, устранить допущенные нарушения.

В случае подтверждения факта недостоверности персональных данных должностное лицо администрации, обрабатывающее персональные данные, 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.

5.4. В случае невозможности устранения допущенных нарушений должностное лицо администрации, обрабатывающее персональные данные, в срок, не превышающий 10 рабочих дней с даты выявления неправомерности действий с персональными данными, обезличивает персональные данные.

Об устранении допущенных нарушений или об обезличивании персональных данных должностное лицо администрации поселения, обрабатывающее персональные данные, уведомляет субъекта персональных данных (его законного представителя) по форме уведомления об устранении допущенных нарушений или уведомления об уничтожении согласно приложениям 1, 2 и (или) уполномоченный орган по защите прав субъектов персональных данных по форме уведомления об устранении допущенных нарушений или уведомления об уничтожении согласно приложениям 3, 4.

5.5. В случае отзыва субъектом персональных данных согласия на обработку своих персональных данных должностное лицо администрации, обрабатывающее персональные данные, обязано прекратить обработку персональных данных и обезличить их в срок, не превышающий 30 рабочих дней с даты поступления указанного отзыва, если иное не предусмотрено законодательством, договором или соглашением между администрацией и субъектом персональных данных. Об обезличивании персональных данных должностное лицо администрации поселения, обрабатывающее персональные данные, уведомляет субъекта персональных данных (его законного представителя).

6. Способы обезличивания:

6.1. К способам обезличивания персональных данных при условии дальнейшей обработки персональных данных относятся:

уменьшение перечня обрабатываемых сведений;

замена части сведений условными обозначениями;

обобщение (понижение) точности некоторых сведений;

деление сведений на части и обработка их в разных информационных системах;

другие способы.

6.2. К способам обезличивания персональных данных в случае достижения целей обработки или в случае утраты необходимости в достижении этих целей относятся:

сокращение перечня персональных данных;

уничтожение персональных данных.

6.3. 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 материальном носителе (закрашиванием, вырезанием и т.д.).

7. Правила работы с обезличенными данными:

7.1. Обезличенные персональные данные не подлежат разглашению и нарушению конфиденциальности.

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

7.3. При обработке обезличенных персональных данных с использованием средств автоматизации необходимо:

использование паролей;

использование антивирусных программ;

соблюдение правил доступа в помещения, в которых ведется обработка персональных данных.

7.4. При обработке обезличенных персональных данных без использования средств автоматизации необходимо соблюдение:

хранения бумажных носителей в условиях, исключающих доступ к ним посторонних лиц;

соблюдение правил доступа в помещения, в которых ведется обработка персональных данных.

Приложение 1
к Правилам работы с обезличенными данными в случае обезличивания персональных данных в администрации Изобильненского городского округа Ставропольского края, утвержденными постановлением администрации Изобильненского городского округа Ставропольского края
от 10 апреля 2018 г. № 465

Уведомление об устранении допущенных нарушений

Уважаемый (ая)_____,
(Ф.И.О.)
в связи с _____ сообщаем Вам, что все допущенные нарушения при обработке Ваших персональных данных устранены.

_____ _____ _____
(должность) (подпись) (Ф.И.О.)

«____» _____ 20___ г.

Приложение 2
к Правилам работы с обезличенными данными в случае обезличивания персональных данных в администрации Изобильненского городского округа Ставропольского края, утвержденными постановлением администрации Изобильненского городского округа Ставропольского края
от 10 апреля 2018 г. № 465

Уведомление об уничтожении

Уважаемый (ая) _____,
(Ф.И.О.)
в связи с _____ сообщаем Вам, что Ваши персональные данные _____
(указать персональные данные)
_____
уничтожены.

_____ _____ _____
(должность) (подпись) (Ф.И.О.)

«____» _____ 20___ г.

Приложение 3
к Правилам работы с обезличенными данными в случае обезличивания персональных данных в администрации Изобильненского городского округа Ставропольского края, утвержденными постановлением администрации Изобильненского городского округа Ставропольского края
от 10 апреля 2018 г. № 465

Уведомление об устранении допущенных нарушений

Настоящим уведомлением сообщаем Вам, что допущенные нарушения при обработке персональных данных, а именно _____
(указать допущенные нарушения)
_____,
устранены.

_____ _____ _____
(должность) (подпись) (Ф.И.О.)

«____» _____ 20___ г.

Приложение 4
к Правилам работы с обезличенными данными в случае обезличивания персональных данных в администрации Изобильненского городского округа Ставропольского края, утвержденными постановлением администрации Изобильненского городского округа Ставропольского края от 10 апреля 2018 г. № 465

В _____
(указать уполномоченный орган)

Уведомление об уничтожении

Настоящим уведомлением сообщаем Вам, что в связи с _____
_____
персональные данные_____
(указать, чьи персональные данные)
уничтожены.

_____ _____ _____
(должность) (подпись) (Ф.И.О.)

«____» _____ 20___ г.

Утвержден
постановлением администрации
Изобильненского городского
округа Ставропольского края
от 10 апреля 2018 г. № 465

ПОРЯДОК ДОСТУПА СЛУЖАЩИХ АДМИНИСТРАЦИИ ИЗОБИЛЬНЕНСКОГО ГОРОДСКОГО ОКРУГА СТАВРОПОЛЬСКОГО КРАЯ В ПОМЕЩЕНИЯ, В КОТОРЫХ ВЕДЁТСЯ ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Общие положения

Настоящий порядок разработан в целях обеспечения безопасности персональных данных, средств вычислительной техники информационных систем персональных данных, материальных носителей персональных данных, а также обеспечения внутриобъектового режима.

Документ устанавливает правила доступа в помещения в рабочее и нерабочее время, а также в нештатных ситуациях.

Объектами охраны администрации Изобильненского городского округа Ставропольского края (далее – администрация) являются:

1) помещения, в которых происходит обработка персональных данных, как с использованием средств автоматизации, так и без таковых, в том числе серверные помещения;

2) помещения, в которых хранятся материальные носители персональных данных и резервные копии персональных данных;

3) помещения, в которых установлены криптографические средства, предназначенные для шифрования персональных данных, в том числе носители ключевой информации (далее спецпомещения).

Бесконтрольный доступ посторонних лиц в указанные помещения исключён.

Посторонними лицами считаются сотрудники администрации, не допущенные к обработке персональных данных и лица, не являющиеся сотрудниками администрации.

К спецпомещениям, предъявляются дополнительные требования по безопасности, указанные в разделе 4.

Ответственность за соблюдение положений настоящего порядка несут сотрудники структурных подразделений, допущенные в помещения, являющиеся объектами охраны, а также их руководители.

Контроль соблюдения требований настоящей инструкции обеспечивает сотрудник, назначенный ответственным за организацию обработки персональных данных в администрации.

Ограждающие конструкции объектов охраны должны предполагать существенные трудности для нарушителя по их преодолению.

Например: металлические решётки на окнах, металлическая дверь, система контроля и управления доступа и так далее.

2. Правила доступа в помещения, в которых ведётся обработка персональных данных

Доступ посторонних лиц в помещения, в которых ведется обработка персональных данных, а также хранятся материальные носители персональных данных и резервные копии персональных данных, должен осуществляется только ввиду служебной необходимости и под контролем сопровождающего лица, из числа сотрудников, допущенных к обработке персональных данных.

При этом должны быть приняты меры, исключающие ознакомление посторонних лиц с персональными данными. Пример: мониторы повернуты в сторону от посетителей, документы убраны в стол, либо находятся в непрозрачной папке (накрыты чистыми листами бумаги).

При возникновении чрезвычайных ситуаций природного и техногенного характера, аварий, катастроф, стихийных бедствий, а также ситуаций, которые могут создавать угрозу жизни и здоровью граждан, в целях оказания помощи гражданам, предотвращения, ликвидации предпосылок и последствий нештатной ситуации, может осуществляться доступ в помещения, в которых ведется обработка персональных данных лиц из числа сотрудников администрации, не допущенных к обработке персональных данных.

В нерабочее время все окна и двери в помещениях (в том числе в смежные помещения), в которых ведется обработка персональных данных, должны быть надежно закрыты, материальные носители персональных данных должны быть убраны в запираемые шкафы (сейфы), компьютеры выключены либо заблокированы.

Доступ сотрудников в помещения, в которых ведется обработка персональных данных в нерабочее время, допускается по распоряжению руководства администрации.

3. Правила доступа в серверные помещения

Доступ в серверные помещения, в которых ведётся обработка персональных данных, осуществляется в соответствии со списком, утверждённым в администрации.

Уборка серверных помещений происходит только под контролем лица, из указанных в утверждённом списке.

Доступ в серверные помещения посторонних лиц допускается по согласованию с ответственным за обеспечение безопасности информационных систем обработки персональных данных.

Нахождение в серверных помещениях посторонних лиц без сопровождающего запрещено.

При возникновении чрезвычайных ситуаций природного и техногенного характера, аварий, катастроф, стихийных бедствий, а также других ситуаций, которые могут создавать угрозу жизни и здоровью граждан, доступ в серверные помещения, в целях оказания помощи гражданам, предотвращения, ликвидации предпосылок и последствий нештатной ситуации, может осуществляться без согласования с ответственным за обеспечение безопасности информационных систем персональных.

Доступ сотрудников в серверные помещения в нерабочее время допускается по распоряжению руководства администрации.

4. Правила доступа в спецпомещения

Спецпомещения выделяют с учётом размеров контролируемых зон, регламентированных эксплуатационной и технической документацией к криптосредствам. Помещения должны иметь прочные входные двери с замками, гарантирующими надёжное закрытие помещений в нерабочее время. Окна помещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в спецпомещения посторонних лиц, необходимо оборудовать металлическими решётками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в спецпомещения.

Расположение спецпомещения, специальное оборудование и организация режима в спецпомещениях должны исключить возможность неконтролируемого проникновения или пребывания в них посторонних лиц, а также просмотра посторонними лицами ведущихся там работ.

Для предотвращения просмотра извне спецпомещений их окна должны быть защищены.

Спецпомещения должны быть оснащены входными дверьми с замками. Должно быть обеспечено постоянное закрытие дверей спецпомещений на замок и открытие только для санкционированного прохода, а также опечатывание спецпомещений по окончании рабочего дня или оборудование спецпомещений соответствующими техническими устройствами, сигнализирующими о несанкционированном вскрытии спецпомещений.

Доступ в спецпомещения осуществляется в соответствии с перечнем лиц, имеющих право доступа в помещения, где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ, утверждённым распоряжением администрации Изобильненского городского округа Ставропольского края.

Доступ иных лиц в спецпомещения может осуществляться под контролем лиц, имеющих право допуска в спецпомещения.

При возникновении чрезвычайных ситуаций природного и техногенного характера, аварий, катастроф, стихийных бедствий, а также ситуаций, которые могут создавать угрозу жизни и здоровью граждан, в целях оказания помощи гражданам, предотвращения, ликвидации предпосылок и последствий нештатной ситуации, может осуществляться доступ в спецпомещения иных лиц их числа сотрудников администрации.

Сотрудники органов МЧС и аварийных служб, врачи «скорой помощи» допускаются в спецпомещения для ликвидации нештатной ситуации, иных чрезвычайных ситуаций или оказания медицинской помощи в сопровождении руководителя структурного подразделения администрации.

При утрате ключа от входной двери в спецпомещение замок необходимо заменить или переделать его секрет с изготовлением к нему новых ключей с документальным оформлением.

Доступ сотрудников в спецпомещения в нерабочее время допускается на основании служебных записок (или иных видов разрешающих документов), подписанных Главой Изобильненского городского округа Ставропольского края.

Нахождение в спецпомещениях посторонних лиц в нерабочее время запрещается.

Утвержден
постановлением администрации
Изобильненского городского
округа Ставропольского края
от 10 апреля 2018 г. № 465

ПЕРЕЧЕНЬ
ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ АДМИНИСТРАЦИИ ИЗОБИЛЬНЕНСКОГО ГОРОДСКОГО ОКРУГА СТАВРОПОЛЬСКОГО КРАЯ (ДАЛЕЕ - ИСПДН)

№	Наименование ИСПДн	Категория ИСПДн	Уровень защищенности персональных данных	Использование СКЗИ для обеспечения безопасности персональных данных
1	2	3	4	5
1.	Кадры	ИСПДн-Д	четвертый	не используются
2.	Бухгалтерия	ИСПДн-Д	четвертый	используются
3.	Обращения граждан	ИСПДн-Д	четвертый	используются
4.	Услуги	ИСПДн-Д	четвертый	используются
5.	Юристы	ИСПДн-Д	четвертый	не используются
6.	КДН, опека и попечительство	ИСПДн-И	четвертый	не используются

Утвержден
постановлением администрации
Изобильненского городского
округа Ставропольского края
от 10 апреля 2018 г. № 465

ПЕРЕЧЕНЬ
ПЕРСОНАЛЬНЫХ ДАННЫХ, ОБРАБАТЫВАЕМЫХ В АДМИНИСТРАЦИИ ИЗОБИЛЬНЕНСКОГО ГОРОДСКОГО ОКРУГА СТАВРОПОЛЬСКОГО КРАЯ В СВЯЗИ С РЕАЛИЗАЦИЕЙ СЛУЖЕБНЫХ И ТРУДОВЫХ ОТНОШЕНИЙ, А ТАКЖЕ В СВЯЗИ С ОКАЗАНИЕМ МУНИЦИПАЛЬНЫХ УСЛУГ И ОСУЩЕСТВЛЕНИЕМ МУНИЦИПАЛЬНЫХ ФУНКЦИЙ

1. ПЕРЕЧЕНЬ
персональных данных, обрабатываемых в администрации Изобильненского городского округа Ставропольского края в связи с оказанием муниципальных услуг и осуществлением муниципальных функций

1. Фамилия, имя, отчество.
2. Год рождения.
3. Дата рождения.
4. Место рождения.
5. Адрес.
6. Паспортные данные.
7. СНИЛС.

2. ПЕРЕЧЕНЬ
персональных данных, обрабатываемых в администрации Изобильненского городского округа Ставропольского края в связи с реализацией трудовых отношений

1. Фамилия, имя, отчество, дата и место рождения, гражданство.

2. Прежние фамилия, имя, отчество, дата, место и причина изменения (в случае изменения).

3. Владение иностранными языками и языками народов Российской Федерации.

4. Образование (когда и какие образовательные учреждения закончил, номера дипломов, направление подготовки или специальность по диплому, квалификация по диплому).

5. Послевузовское профессиональное образование (наименование образовательного или научного учреждения, год окончания), учёная степень, учёное звание (когда присвоены, номера дипломов, аттестатов).

6. Выполняемая работа с начала трудовой деятельности (включая военную

службу, работу по совместительству, предпринимательскую деятельность).

7. Классный чин федеральной государственной гражданской службы, гражданской службы субъекта Российской Федерации, муниципальной службы, дипломатический ранг, воинское, специальное звание, классный чин правоохранительной службы (кем и когда присвоены).

8. Государственные награды, иные награды и знаки отличия (кем награждён и когда).

9. Степень родства, фамилии, имена, отчества, даты рождения близких родственников (отца, матери, братьев, сестёр и детей), а также мужа (жены).

10. Места рождения, места работы и домашние адреса близких родственников (отца, матери, братьев, сестёр и детей), а также мужа (жены).

11. Фамилии, имена, отчества, даты рождения, места рождения, места работы и домашние адреса бывших мужей (жён).

12. Пребывание за границей (когда, где, с какой целью).

13. Близкие родственники (отец, мать, братья, сестры и дети), а также муж (жена), в том числе бывшие, постоянно проживающие за границей и (или) оформляющие документы для выезда на постоянное место жительства в другое государство (фамилия, имя, отчество, с какого времени проживают за границей).

14. Адрес регистрации и фактического проживания.

15. Дата регистрации по месту жительства.

16. Паспортные данные (серия, номер, кем и когда выдан).

17. Данные документа, удостоверяющего личность гражданина Российской Федерации за пределами Российской Федерации (серия, номер, кем и когда выдан).

18. Номер телефона.

19. Отношение к воинской обязанности, сведения по воинскому учёту (для граждан, пребывающих в запасе, и лиц, подлежащих призыву на военную службу).

20. Идентификационный номер налогоплательщика.

21. Номер страхового свидетельства обязательного пенсионного страхования.

22. Наличие (отсутствие) судимости.

23. Допуск к государственной тайне, оформленный за период работы, службы, учёбы (форма, номер и дата).

24. Наличие (отсутствие) заболевания, препятствующего поступлению на государственную гражданскую службу Российской Федерации или её прохождению, подтверждённого заключением медицинского учреждения.

25. Результаты обязательных предварительных (при поступлении на работу) и периодических медицинских осмотров (обследований), а также обязательного психиатрического освидетельствования.

26. Сведения о доходах, имуществе и обязательствах имущественного характера, а также о доходах, об имуществе и обязательствах имущественного характера членов семьи.

27. Сведения о последнем месте государственной или муниципальной службы.

Утвержден
постановлением администрации
Изобильненского городского
округа Ставропольского края
от 10 апреля 2018 г. № 465

ПЕРЕЧЕНЬ
ДОЛЖНОСТЕЙ В АДМИНИСТРАЦИИ ИЗОБИЛЬНЕНСКОГО ГОРОДСКОГО ОКРУГА СТАВРОПОЛЬСКОГО КРАЯ, ОТВЕТСТВЕННЫХ ЗА ПРОВЕДЕНИЕ МЕРОПРИЯТИЙ ПО ОБЕЗЛИЧИВАНИЮ ОБРАБАТЫВАЕМЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ

№ п/п	Структурное подразделение (отдел)	Должность служащего
1	2	3
1.	Общий отдел	заместитель начальника отдела

Утвержден
постановлением администрации
Изобильненского городского
округа Ставропольского края
от 10 апреля 2018 г. № 465

ПЕРЕЧЕНЬ
ДОЛЖНОСТЕЙ СЛУЖАЩИХ АДМИНИСТРАЦИИ ИЗОБИЛЬНЕНСКОГО ГОРОДСКОГО ОКРУГА СТАВРОПОЛЬСКОГО КРАЯ, ЗАМЕЩЕНИЕ КОТОРЫХ ПРЕДУСМАТРИВАЕТ ОСУЩЕСТВЛЕНИЕ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ЛИБО ОСУЩЕСТВЛЕНИЕ ДОСТУПА К ПЕРСОНАЛЬНЫМ ДАННЫМ

№ п/п	Структурное подразделение (отдел)	Должность служащего
1	2	3
1.	Руководство	Глава Изобильненского городского округа, первый заместитель главы, заместитель главы, главный специалист
2.	Общий отдел	начальник, заместитель начальника, главный специалист, ведущий специалист
3.	Отдел правового и кадрового обеспечения	начальник, заместитель начальника, консультант, главный специалист, ведущий специалист
4.	Отдел по обеспечению организационной деятельности и связям с общественностью	заместитель начальника
5.	Отдел по безопасности и профилактике правонарушений	начальник, главный специалист
6.	Отдел экономического развития, стратегического планирования и статистики	ведущий специалист
7.	Отдел планирования и закупок	начальник, заместитель начальника, консультант
8.	Отдел сельского хозяйства, охраны окружающей среды, пищевой и перерабатывающей промышленности и торговли	заместитель начальника, главный специалист, ведущий специалист
9.	Отдел строительства, жилищно-коммунального и дорожного хозяйства	начальник, заместитель начальника, консультант, главный специалист, ведущий специалист, специалист 1 категории

10.	Отдел социального развития и туризма	начальник, главный специалист, ведущий специалист, специалист 1 категории, специалист
11.	Отдел по работе с территориями	начальник, главный специалист, специалист 1 категории
12.	Архивный отдел	начальник, главный специалист, специалист 1 категории

Утверждена
постановлением администрации
Изобильненского городского
округа Ставропольского края
от 10 апреля 2018 г. № 465

ИНСТРУКЦИЯ ОТВЕТСТВЕННОГО ЗА ОРГАНИЗАЦИЮ ОБРАБОТКИ И ЗАЩИТУ ПЕРСОНАЛЬНЫХ ДАННЫХ В АДМИНИСТРАЦИИ ИЗОБИЛЬНЕНСКОГО ГОРОДСКОГО ОКРУГА СТАВРОПОЛЬСКОГО КРАЯ

1. Общие положения

1.1. Ответственный за организацию обработки и защиту персональных данных в администрации Изобильненского городского округа Ставропольского края (далее соответственно – администрации, ответственный за организацию обработки и защиту персональных данных) назначается распоряжением администрации.

1.2. Ответственный за организацию обработки и защиту персональных данных в своей деятельности руководствуется Трудовым кодексом Российской Федерации, Федеральным законом «О персональных данных», постановлениями Правительства Российской Федерации от 15 сентября 2008г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствие с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», настоящей должностной инструкцией.

1.3. Ответственный за организацию обработки и защиту персональных данных является уполномоченным на поддержание достигнутого уровня защиты информационных систем персональных данных и ее ресурсов на этапах эксплуатации.

1.4. Ответственный за организацию обработки и защиту персональных данных осуществляет методическое руководство сотрудниками администрации, имеющими доступ к персональным данным, по вопросам обеспечения безопасности персональных данных. Требования ответственного за организацию обработки и защиту персональных данных, связанные с выполнением им своих должностных обязанностей, обязательны для исполнения всеми сотрудниками администрации, имеющими доступ к персональным данным.

2. Задачи ответственного за организацию обработки и защиту персональных данных

2.1. На ответственного за организацию обработки и защиту персональных данных возложены следующие задачи:

1) уведомление органа по защите прав субъектов персональных данных (Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор)) об обработке персональных данных или в случае изменения сведений, указанных в Уведомлении (части 3 статьи 22 Федерального закона «О персональных данных»), а также в случае прекращения обработки персональных данных;

2) организация приёма и обработки обращений и запросов субъектов персональных данных или их законных представителей и осуществление контроля за приёмом и обработкой таких обращений и запросов;

3) осуществление внутреннего контроля за соблюдением требований законодательства Российской Федерации сотрудниками администрации при обработке персональных данных в администрации, в том числе, требований к защите персональных данных;

4) доведение до сведения сотрудников администрации, имеющих доступ к персональным данным, положений законодательства Российской Федерации о персональных данных, локальных актов администрации по вопросам обработки персональных данных, требований к защите персональных данных;

5) организация комплексной защиты объектов информатизации администрации, а именно:

информационных ресурсов, представленных в виде документированной информации на магнитных, оптических носителях, информативных физических полей, информационных массивов и баз данных, содержащие персональные данные субъектов администрации;

средств и систем информатизации (средства вычислительной техники, информационно-вычислительные комплексы, локальные вычислительные сети и корпоративные информационные системы), программных средств (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение), автоматизированных систем управления информационными, управленческими и технологическими процессами, систем связи и передачи данных, технических средства приёма, передачи и обработки информации (звукозаписи, звукоусиления, звуковоспроизведения, переговорные устройства и другие технические средства обработки графической, смысловой и буквенно-цифровой информации), используемых для реализации процессов ведения деятельности, обработки информации, содержащих персональные данные субъектов администрации;

6) организация защиты персональных данных субъектов администрации;

7) разработка организационных мероприятий, обеспечивающих безопасность объектов защиты администрации, своевременное выявление и устранение возможных каналов утечки информации;

8) организация постоянного контроля за обеспечением уровня защищенности персональных данных;

9) организация проведения работ по технической защите информации на объектах информатизации, в информационно-вычислительных сетях, системах и средствах связи и телекоммуникаций администрации;

10) реализация технических мер, обеспечивающих своевременное выявление возможных технических каналов утечки информации в подразделениях;

11) методическое руководство системой обеспечения информационной безопасности администрации;

12) организация контроля состояния и оценки эффективности системы

обеспечения информационной безопасности и реализация мер по её совершенствованию;

13) внедрение в информационную инфраструктуру администрации современных методов и средств обеспечения информационной безопасности.

3. Права и функции ответственного за организацию обработки и защиту персональных данных

3.1. Для решения поставленных задач ответственный за организацию обработки и защиту персональных данных осуществляет следующие функции:

1) контроль за организацией доступа и учет сотрудников администрации, имеющим доступ к персональным данным;

2) разработка и внедрение организационных мероприятий и технических мер по комплексной защите персональных данных;

3) обеспечение соблюдения режима конфиденциальности при обработке персональных данных;

4) планирование работы по защите персональных данных в администрации;

5) контроль за выполнением мероприятий по защите персональных данных, анализ материалов контроля, выявление недостатков и нарушений, в том числе разработка и реализация мер по их устранению;

6) обеспечение взаимодействия с контрагентами по вопросам организации и проведения проектно-изыскательских, научно-исследовательских, опытно-конструкторских и других работ по защите информации;

7) участие в разработке технических заданий на выполняемые исследования и работы;

8) контроль за выполнением плановых заданий, договорных обязательств, а также сроков, полноты и качества работ по защите персональных данных, выполняемых контрагентами;

9) разработка и принятие мер по обеспечению финансирования работ по защите персональных данных, в том числе выполняемых по договорам;

10) проведение работ по технической защите информации в администрации, в том числе, оценка эффективности принятых мер по технической защите информации;

11) организация мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным или передачи их лицам, не имеющим права доступа к такой информации;

12) выявление демаскирующих признаков, возможных каналов утечки информации, в том числе по техническим каналам, разработка мер по их устранению и предотвращению;

13) постоянный контроль за обеспечением уровня защищенности персональных данных;

14) контроль за обеспечением функционирования и безопасности криптосредств;

15) обеспечение соответствия проводимых работ по защите персональных данных технике безопасности, правилам и нормам охраны труда.

3.2. Ответственный за организацию обработки и защиту персональных данных имеет право:

1) осуществлять контроль за деятельностью структурных подразделений администрации по выполнению ими требований по защите персональных данных и других вопросов, входящих в компетенцию ответственного за организацию обработки и защиту персональных данных. При выявлении нарушений требований по защите персональных данных составлять акты, докладные

записки, отчёты для рассмотрения руководством администрации;

2) принимать необходимые меры при обнаружении несанкционированного доступа к персональным данным, как внутри администрации, так и извне, и докладывать о принятых мерах главе округа с представлением информации о субъектах, нарушивших режим доступа;

3) вносить на рассмотрение Главы Изобильненского городского округа предложения, акты, заключения о приостановлении работ в случае обнаружения каналов утечки (или предпосылок к утечке) информации ограниченного доступа;

4) давать структурным подразделениям администрации, а также отдельным сотрудникам обязательные для исполнения указания по вопросам, входящим в свою компетенцию;

5) запрашивать и получать от всех структурных подразделений сведения, справочные и другие материалы, необходимые для осуществления своей деятельности;

6) составлять акты и другую техническую документацию о степени защищенности объектов информатизации;

7) готовить предложения о привлечении к проведению работ по оценке эффективности защиты персональных данных на объектах администрации (на договорной основе) учреждений и организаций, имеющих лицензию на соответствующий вид деятельности, а также предложения о закупке необходимых технических средств защиты и другой спецтехники, имеющих в обязательном порядке сертификат качества;

8) вносить предложения по заключения договора на проведение работ по защите персональных данных;

9) рассматривать применяемые и предлагаемые методы защиты информации, промежуточных и конечных результатов исследований и разработок;

10) осуществлять визирование договоров с контрагентами с целью правового обеспечения передачи им персональных данных субъектов администрации в ходе выполнения работ по этим договорам;

11) представлять интересы администрации при осуществлении государственного контроля и надзора за обработкой персональных данных Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

4. Взаимоотношения (служебные связи)

4.1. Ответственный за организацию обработки и защиту персональных данных выполняет свои задачи в контакте со всеми структурными подразделениями администрации.

4.2. Для выполнения своих функций и реализации предоставленных прав ответственный за организацию обработки и защиту персональных данных взаимодействует с территориальными и региональными подразделениями Федеральной службы по техническому и экспортному контролю, ФСБ России, МВД России, другими представителями исполнительной власти и организациями, предоставляющими услуги и выполняющими работы в области защиты персональных данных на законном основании.

5. Ответственность

5.1. Ответственный за организацию обработки и защиту персональных данных несёт персональную ответственность за надлежащее и своевременное

выполнение функций, предусмотренных настоящей Инструкцией.

5.2. На ответственного за организацию обработки и защиту персональных данных возлагается персональная ответственность за:

обеспечение сохранности программных, технических и других материальных средств;

соблюдение правил пожарной безопасности;

своевременное, а также качественное исполнение документов и поручений руководства администрации, ведение делопроизводства в соответствии с действующими правилами и инструкциями;

обеспечение сохранности принимаемой и достоверность передаваемой информации;

недопущение использования информации в неслужебных целях;

надлежащий контроль за режимом доступа к персональным данным;

соблюдение им трудовой и производственной дисциплины;

качество проводимых им работ по контролю за соблюдением администрации и его сотрудниками, имеющими доступ к персональным данным, законодательства Российской Федерации, в том числе требований к защите персональных данных, локальных актов администрации по вопросам обработки персональных данных, состояние и поддержание установленного уровня защиты информационных систем персональных данных.

Утверждено
постановлением администрации
Изобильненского городского
округа Ставропольского края
от 10 апреля 2018 г. № 465

ТИПОВОЕ ОБЯЗАТЕЛЬСТВО ДОЛЖНОСТНОГО ЛИЦА АДМИНИСТРАЦИИ ИЗОБИЛЬНЕНСКОГО ГОРОДСКОГО ОКРУГА СТАВРОПОЛЬСКОГО КРАЯ, 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

Я, _____,
(фамилия, имя, отчество)

обязуюсь прекратить обработку персональных данных, ставших мне известными в связи с исполнением должностных обязанностей, в случае расторжения со мной служебного контракта.

В соответствии со статьей 7 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» я уведомлен (а) о том, что операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

Ответственность, предусмотренная законодательством Российской Федерации, мне разъяснена.

_____ _____
(дата) (подпись)

Утверждена
постановлением администрации
Изобильненского городского
округа Ставропольского края
от 10 апреля 2018 г. № 465

ТИПОВАЯ ФОРМА СОГЛАСИЯ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ МУНИЦИПАЛЬНЫХ СЛУЖАЩИХ АДМИНИСТРАЦИИ ИЗОБИЛЬНЕНСКОГО ГОРОДСКОГО ОКРУГА СТАВРОПОЛЬСКОГО КРАЯ, А ТАКЖЕ ИНЫХ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

Я, _____
(фамилия, имя, отчество)
зарегистрированный (ая) по адресу: _____
(почтовый индекс, адрес места жительства)
_____

документ, удостоверяющий личность, _____
(вид документа)
серия номер _____
кем и когда выдан документ
_____

в соответствии со статьёй 9 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» своей волей и в своем интересе даю согласие оператору – администрации Изобильненского муниципального района Ставропольского края, на автоматизированную, а также без использования средств автоматизации обработку моих персональных данных, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

А именно:

1) анкетных и биографических данных, включая адрес места жительства и проживания;

2) паспортных данных или данных иного документа, удостоверяющего личность и гражданство, включая серию, номер, дату выдачи, наименование органа, выдавшего документ);

3) сведений об образовании, квалификации и о наличии специальных знаний или специальной подготовки;

4) сведений о трудовой деятельности, опыте работы, занимаемой должности, трудовом стаже, повышения квалификации и переподготовки;

5) сведений о составе семьи и наличии иждивенцев, сведений о месте работы или учёбы членов семьи;

6) сведений о состоянии здоровья и наличии заболеваний (когда это необходимо в случаях, установленных законом);

7) сведений о доходах, об имуществе и обязательствах имущественного характера, в том числе членов семьи;

Если мои персональные данные можно получить только у третьей стороны, то я должен быть уведомлен об этом заранее с указанием целей, предполагаемых источников и способов получения персональных данных, также должно быть получено на это согласие.

Мне разъяснены мои права и обязанности, связанные с обработкой персональных данных, в том числе, моя обязанность проинформировать оператора в случае изменения моих персональных данных; мое право в любое время отозвать свое согласие путем направления соответствующего письменного заявления оператору.

Согласие вступает в силу со дня его подписания и действует в течение неопределенного срока до достижения цели обработки персональных данных или его отзыва в письменной форме.

" ____ " _____ 20_____г. _____ _____

(подпись) (расшифровка подписи)

Утверждена
постановлением администрации
Изобильненского городского
округа Ставропольского края
от 10 апреля 2018 г. № 465

ТИПОВАЯ ФОРМА РАЗЪЯСНЕНИЯ СУБЪЕКТУ ПЕРСОНАЛЬНЫХ ДАННЫХ ЮРИДИЧЕСКИХ ПОСЛЕДСТВИЙ ОТКАЗА ПРЕДОСТАВИТЬ СВОИ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

В соответствии со статьей 26 Федерального закона от 02 марта 2007 года № 25-ФЗ «О муниципальной службе в Российской Федерации», статьями 65,86 Трудового кодекса Российской Федерации определен перечень персональных данных, который субъект персональных данных обязан предоставить в связи с поступлением или прохождением муниципальной службы (работы).

Без представления субъектом персональных данных обязательных для заключения служебного контракта (трудового договора) сведений служебный контракт (трудовой договор) не может быть заключен.

На основании пункта 11 статьи 77 Трудового кодекса Российской Федерации служебный контракт (трудовой договор) прекращается вследствие нарушения установленных обязательных правил его заключения, если это нарушение исключает возможность замещения должности (продолжения работы).

Мне_____
(фамилия, имя, отчество)

разъяснены юридические последствия отказа предоставить свои персональные данные.

"____" _____ 20___ г. _____ _____

Утверждена
постановлением администрации
Изобильненского городского
округа Ставропольского края
от 10 апреля 2018 г. № 465

ТИПОВАЯ ФОРМА
ОБЯЗАТЕЛЬСТВА О НЕРАЗГЛАШЕНИИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Я,_____
(ФИО сотрудника)
_____
Паспорт серия номер выдан_____
_____
Исполняющий (ая) должностные обязанности_____
_____
(должность)

предупрежден(а), что на период исполнения должностных обязанностей мне будет предоставлен допуск к персональным данным. Настоящим добровольно принимаю на себя обязательства:

1. Не разглашать третьим лицам персональные данные, которые мне доверены (будут доверены) или станут известными в связи с выполнением должностных обязанностей.

2. В случае попытки третьих лиц получить от меня персональные данные, сообщать непосредственному руководителю.

3. Не использовать персональные данные с целью получения выгоды.

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

5. После прекращения права на допуск к персональным данным не разглашать и не передавать третьим лицам известные мне персональные данные.

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

(Фамилия, Имя, Отчество) (Дата) (Подпись)

Утвержден
постановлением администрации
Изобильненского городского
округа Ставропольского края
от 10 апреля 2018 г. № 465

Главе Изобильненского городского
округа Ставропольского края
В.И. Козлову
От
Паспорт серия номер

(когда и кем выдан)

Проживающий по адресу:

Контактный номер телефона

Отзыв согласия на обработку персональных данных

« ___» _____ 201__ г.

Настоящим во исполнение положений Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» я, _____

(фамилия, имя, отчество)

(серия, номер паспорта, кем выдан)

(место регистрации)

отзываю у администрации Изобильненского городского округа Ставропольского края свое согласие на обработку персональных данных. Прошу прекратить обработку персональных данных не позднее трех рабочих дней с даты поступления настоящего Отзыва, а также уничтожить всю персональную информацию, касающуюся меня лично.

_____ _____

Ф.И.О. подпись