|  |  |  |
| --- | --- | --- |
| **ХАЛЬМГ ТАҢҺЧИН****YСТИН РАЙОНА****МУНИЦИПАЛИН БYРДӘЦИН****АДМИНИСТРАЦИН****ЗААВР** | герб чб | **РАСПОРЯЖЕНИЕ****ГЛАВЫ АДМИНИСТРАЦИИ****ЮСТИНСКОГО РАЙОННОГО****МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ****РЕСПУБЛИКИ КАЛМЫКИЯ** |

359300, Республика Калмыкия, п. Цаган Аман Юстинского района, ул. Советская, 46 код /847 44/, тел. 9-24-00, факс 9-14-00,

E-mail: yurmo2010@yandex.ru

«12» января 2018 г. № 4-р Цаган Аман

В соответствии с Федеральным законом РФ от 27.07.2006г. №152 "О персональных данных", Федеральным законом РФ от 27.07.2006г. №149 “Об информации, и информационных технологиях и о защите информации”, Постановлением Правительства РФ от 17.11.2007 № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», Постановления Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Постановлением Правительства РФ от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей»:

1. Назначить ответственным за организацию обработки персональных данных в Администрации Юстинского РМО Республики Калмыкия заместителя главы Администрации Юстинского РМО Республики Калмыкия

Катаева М.Л.

2.Назначить администратором безопасности при обработке персональных данных в информационных системах ведущего специалиста - системного администратора Администрации Юстинского РМО Республики Калмыкия Горяева Б.В.

3.Утвердить Положение о порядке обработки персональных данных в Администрации Юстинского РМО Республики Калмыкия. (приложение №1)

4. Данное распоряжение вступает в силу со дня его подписания.

Глава Администрации

Юстинского РМО

Республики Калмыкия Ю.С.Очиров

Приложение №1

к Распоряжению от

«12» января 2018г. №4-р

Положение

о порядке обработки персональных данных

в Администрации Юстинского РМО Республики Калмыкия

.

1.ОБЩИЕ ПОЛОЖЕНИЯ

1..Настоящее Положение устанавливает процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также определяет для каждой цели обработки персональных данных содержание 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, регламентирует порядок работы с документами, электронными и магнитными носителями, содержащими персональные данные в «Администрации Юстинского РМО Республики Калмыкия» (далее – Организация), в целях реализации федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», Постановления Правительства Российской Федерации от 17.11.2007 № 781 «Об утверждении Положения об обеспечении безопасности 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 использования средств автоматизации», Постановления Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных».

2.ПОРЯДОК ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПРИ ОБРАБОТКЕ И ХРАНЕНИИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОСУЩЕСТВЛЯЕМЫХ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ

1. В целях обеспечения сохранности документов, содержащих персональные данные, все операции по оформлению, формированию, ведению и хранению данной информации должны выполняться сотрудниками Организации, осуществляющими данную работу в соответствии со своими служебными обязанностями, зафиксированными в их должностных регламентах (инструкциях) (согласно Приложению №1).

2. Документы с персональными данными, как и все остальные документы, поступающие в Организацию, обрабатываются в соответствии с утвержденной инструкцией по ведению делопроизводства в Организации. Документ выдается сотрудникам, допущенным к работе с персональными данными, в соответствии с перечнем должностей в Организации осуществляющих обработку персональных данных либо имеющих доступ к персональным данным (согласно Приложению №2).

3. Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных данных (далее -материальные носители), в специальных разделах или на специальных полях форм (бланков).

4. При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

5. Сотрудники Организации, осуществляющие обработку персональных данных без использования средств автоматизации, должны быть проинформированы о факте обработки ими персональных данных, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами.

6. Использование типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовая форма), возможно при соблюдении следующих условий:

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

б) типовая форма должна предусматривать информацию, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации, - при необходимости получения письменного согласия на обработку персональных данных (согласно Приложению №3);

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

г) типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

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:

а) 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;

б) 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.

8. Уничтожение части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление).

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

10. Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

11. Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей). Должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ, для этого документы должны находиться в закрываемых на замок шкафах, сейфах, иных шкафах, имеющих запираемые блок-секции, должен перечень лиц назначены ответственные за хранение документов, ответственные за помещения в которых хранятся документы.

12. Не допускается без согласования с руководителем Организации формирование и хранение баз данных (картотек, файловых архивов и др.), содержащих персональные данные.

13.Передача персональных данных не допускается с использованием средств телекоммуникационных каналов связи (телефон, телефакс, электронная почта и т.п.) без письменного согласия субъекта персональных данных, за исключением случаев, установленных законодательством Российской Федерации.

14.Ответы на запросы граждан и организаций обрабатываются в соответствии с Федеральным законом от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации» и предоставляются только при наличии обоснованной причины в соответствии с законодательством Российской Федерации, в том объеме, который позволяет не разглашать в ответах конфиденциальные данные (не относящиеся к запросу), за исключением данных, содержащихся в материалах запроса или опубликованных в общедоступных источниках.

15. Работа по защите персональных данных организовывается в соответствии с Планом мероприятий в Организации (согласно Приложению №4).

16. Проверки состояния защиты персональных данных организовывается в соответствии с план внутренних проверок режима защиты персональных данных(согласно Приложению №4).

3.ПОРЯДОК ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПРИ ОБРАБОТКЕ

И ХРАНЕНИИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОСУЩЕСТВЛЯЕМЫХ

С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ АВТОМАТИЗАЦИИ

1.Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных (согласно Приложению №5).

2. Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки персональных данных), а также используемые в информационной системе информационные технологии.

Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

3. Работы по обеспечению безопасности персональных данных при их обработке в информационных системах являются неотъемлемой частью работ по созданию информационных систем.

4. Обмен персональными данными при их обработке в информационных системах осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и (или) в случае необходимости путем применения технических средств.

5. Организация режима обеспечения безопасности, где размещено специальное оборудование, а также охрана помещений, в которых ведется работа с персональными данными, должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

6. Безопасность персональных данных при их обработке в информационной системе обеспечивает оператор или лицо, которому на основании приказа оператор поручает обработку персональных данных (далее - уполномоченное лицо). Существенным условием договора является обязанность уполномоченного лица обеспечить конфиденциальность и безопасность персональных данных при их обработке в информационной системе.

7. При обработке персональных данных в информационной системе должно быть обеспечено:

а) проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;

б) своевременное обнаружение фактов несанкционированного доступа к

персональным данным;

в) недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

г) возможность незамедлительного восстановления персональных данных,

модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

д) постоянный контроль за обеспечением уровня защищенности персональных данных.

8.Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах включают в себя:

а) определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;

б) разработку на основе модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем;

в) проверку готовности средств защиты информации к использованию с

составлением заключений о возможности их эксплуатации;

г) установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;

д) обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

е) учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;

ж) учет лиц, допущенных к работе с персональными данными в информационной системе;

з) контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

и) разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

к) описание системы защиты персональных данных;

л) оператор при необходимости может разработать дополнительные нормативные акты по защите персональных данных.

9. Для разработки и осуществления мероприятий по обеспечению безопасности персональных данных при их обработке в информационной системе оператором или уполномоченным лицом может назначаться структурное подразделение или должностное лицо (работник), ответственные за обеспечение безопасности персональных данных.

10. Лица, доступ которых к персональным данным, обрабатываемым в

информационной системе, необходим для выполнения служебных (трудовых) обязанностей, допускаются к соответствующим персональным данным на основании списка, утвержденного оператором или уполномоченным лицом.

11. Запросы пользователей информационной системы на получение персональных данных, а также факты предоставления персональных данных по этим запросам по возможности должны регистрироваться автоматизированными средствами информационной системы в электронном журнале обращений. Содержание электронного журнала обращений периодически проверяется соответствующими должностными лицами (работниками) оператора или уполномоченного лица.

12. При обнаружении нарушений порядка предоставления персональных данных оператор или уполномоченное лицо незамедлительно приостанавливают предоставление персональных данных до выявления причин нарушений и устранения этих причин.

13. Средства защиты информации, предназначенные для обеспечения безопасности персональных данных при их обработке в информационных системах, подлежат учету с использованием индексов или условных наименований и регистрационных номеров.

14. Особенности обеспечения безопасности информации и конфиденциальности персональных данных, связанные с использованием конкретных автоматизированных информационных систем, определяются локальными нормативными документами Организации, регламентирующими порядок использования указанных информационных

систем, а также эксплуатационной и инструктивной документацией, касающейся технических средств обработки персональных данных в рамках конкретной автоматизированной информационной системы.

15. После изменения имеющихся файлов, а также для подготовки и передачи документа при необходимости файлы переносятся подготовившим их должностным лицом на маркированные носители, предназначенные для хранения персональных данных (с уничтожением их на автоматизированном средстве разработки документа в соответствии с действующим законодательством). Об уничтожении файлов необходимо

делать отметки в журнале, утвержденном приказом руководителя Организации.

16. При осуществлении обработки персональных данных с использованием средств автоматизации для информационных систем персональных данных должен быть назначен администратор системы безопасности. Техническое обслуживание оборудования должно осуществляться администратор системы безопасности.

17. Работа со съемными носителями информации проводится в соответствии с инструкцией по работе и учету электронных, магнитных и оптических носителей информации, на которых обрабатываются персональные данные и другая конфиденциальная информация в Организации. (согласно приложению№6).

18. В целях обеспечения антивирусной защиты работа с персональными данными проводится в соответствии с инструкцией «О применении средств антивирусной защиты информации в администрации Юстинского РМО Республики Калмыкия».

4.ПОРЯДОК УНИЧТОЖЕНИЯ ИНФОРМАЦИИ, СОДЕРЖАЩЕЙ

ПЕРСОНАЛЬНЫЕ ДАННЫЕ, ПРИ ДОСТИЖЕНИИ ЦЕЛЕЙ ОБРАБОТКИ ИЛИ ПРИ НАСТУПЛЕНИИ ИНЫХ ЗАКОННЫХ ОСНОВАНИЙ

1. Документы, дела, книги и журналы учета, содержащие персональные данные, при достижении целей обработки или при наступлении иных законных оснований (например, утратившие практическое значение, а также с истекшим сроком хранения), подлежат уничтожению в соответствии с действующим законодательством.

Уничтожение документов производится уполномоченными лицами по работе с персональными данными, которые несут персональную ответственность за правильность и полноту уничтожения.

Отобранные к уничтожению материалы измельчаются до степени, исключающей возможность прочтения текста и сжигаются.

После уничтожения материальных носителей подписывается акт в двух экземплярах(согласно Приложению №7).

2. Уничтожение информации на носителях необходимо осуществлять путем стирания информации с использованием программного обеспечения, установленного на ПЭВМ с гарантированным уничтожением (в соответствии с заданными характеристиками для установленного программного обеспечения с гарантированным уничтожением).

3. Информация, содержащая персональные данные, при достижении целей обработки или при наступлении иных законных оснований (например, утратившие практическое значение, с истекшим сроком хранения) в электронном виде подлежит уничтожению в соответствии с действующим законодательством.

Перед уничтожением информации исполнитель сообщает ответственному за организацию обработки персональных данных.

Приложение № 1

к Положению об обработке

персональных данных

**Должностной регламент**

лиц, имеющих доступ и осуществляющих обработку

персональных данных в Администрации Юстинского РМО РК

1. **Общие положения**

1.1. Должностной регламент лиц, имеющих доступ и осуществляющих

обработку персональных данных в Администрации Юстинского РМО Республики Калмыкия (далее Организация), осуществляющих обработку и допущенных к персональным данным, устанавливает требования по обеспечению получения, обработки, использования, хранения и гарантии конфиденциальности персональных данных физических лиц, необходимых для осуществления деятельности Организации.

1.2. Должностной регламент лиц, имеющих доступ и (или) осуществляющих обработку персональных данных в Организация разработан на основании Трудового кодекса Российской Федерации, Федерального закона от 27.06.2006 № 152-ФЗ "О персональных данных", постановлений Правительства Российской Федерации от 17.11.2007 № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» и от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без исполнения средств автоматизации».

2. **Действия при обработке персональных данных**

Должностные лица, имеющие доступ и осуществляющие обработку персональных данных (далее - должностные лица), обязаны:

2.1. Осуществлять обработку персональных данных исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

2.2. Получать все персональные данные непосредственно у субъекта

персональных данных.

Если персональные данные возможно получить только у третьей стороны, то должностные лица обязаны уведомить субъекта персональных данных об этом заранее, получить от него письменное согласие, сообщить о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа дать письменное согласие на их получение.

2.3. Не допускать получения и обработки персональных данных о политических, религиозных и иных убеждениях и частной жизни.

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

2.4. Не допускать получения и обработки персональных данных о членстве в общественных объединениях или профсоюзной деятельности, за исключением случаев, предусмотренных Трудовым Кодексом или иными федеральными законами.

2.5. Не сообщать персональные данные третьей стороне без письменного

согласия субъекта персональных данных, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью.

2.6. Не сообщать персональные данные в коммерческих целях без письменного согласия субъекта персональных данных, а также кому было ни было, если это не связано со служебной необходимостью.

2.7. Предупредить лиц, получающих персональные данные, 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.

2.8. Соблюдать режим секретности (конфиденциальности) при получении и обработке персональных данных.

2.9. Разрешать доступ к персональным данным только специально уполномоченным лицам, которые имеют право получать только те персональные данные, которые необходимы для выполнения конкретных функций.

2.10. Не запрашивать информацию о состоянии здоровья субъекта персональных данных, за исключением тех сведений, которые относятся к вопросу о возможности обучения или выполнения трудовой функции.

2.11. При фиксации персональных данных на материальных носителях не допускать фиксации на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы.

2.12. Для обработки различных категорий персональных данных,

осуществляемой без использования средств автоматизации, для каждой категории персональных данных использовать отдельный материальный носитель.

2.13. 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, принять меры по обеспечению раздельной обработки персональных данных, исключающее одновременное копирование иных персональных данных, не подлежащих распространению и использованию.

2.14. Не формировать и не хранить без согласования с лицом, ответственным за защиту персональных данных, базы данных (карточки, файловые архивы и т. п.), содержащие персональные данные.

2.15. Не передавать персональные данные по телефону, факсу, электронной почте за исключением случаев, установленных законодательством и действующими инструкциями по работе со служебными документами и обращениями граждан.

2.16. Ответы на запросы граждан и организаций давать в том объеме, который позволяет не разглашать в ответах конфиденциальные данные, за исключением данных, содержащихся в материалах заявителя или опубликованных в общедоступных источниках.

3. **Действия при обращении субъектов персональных данных и лиц, допущенных к персональным данным**

В целях обеспечения доступа субъекта персональных данных к своим

персональным данным должностные лица обязаны:

3.1. Предоставлять субъекту персональных данных полную информацию о его персональных данных, хранящихся у должностного лица, и обработке этих данных.

3.2. Предоставлять субъекту персональных данных свободный бесплатный доступ к своим персональным данным, в том числе выдавать копии любой записи, содержащей персональные данные субъекта, за исключением случаев, предусмотренных федеральным законом.

3.3. Регистрировать факт ознакомления субъекта персональных данных с его персональными данными, а также должностных лиц, допущенных к персональным данным в журнале по ознакомлению с персональными данными.

3.4. Исключать или исправлять неверные или неполные персональные данные, а также данные, обработанные с нарушением требований законодательства, в порядке, предусмотренном настоящим Регламентом.

4. **Действия при хранении персональных данных на съемных и материальных носителях.**

При хранении материальных носителей персональных данных должностное лицо обязано:

4.1. Соблюдать условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ.

4.2. Обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях, а также раздельно хранение съемных носителей с персональными данными с носителями открытой информации на рабочих столах.

4.3. Незамедлительно сообщать должностному лицу, ответственному за защиту персональных данных в Организации, об обнаружении фактов несанкционированного доступа к персональным данным.

4.4. Принять меры для незамедлительного восстановления персональных

данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

4.5. Не допускать воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование.

4.6. Не оставлять материальные носители с персональными данными без

присмотра в незапертом помещении и не представлять их на хранение другим лицам.

4.7. Уничтожение съемных носителей персональных данных, пришедших в негодность, или отслуживших установленный срок, осуществлять по акту уполномоченной комиссией.

4.8. Немедленно ставить известность руководителя соответствующего

структурного подразделения о фактах утраты съемных носителей, содержащих персональные данные, либо о разглашения содержащихся в них сведений. На утраченные носители составлять акт, соответствующие отметки вносить в журнал учета съемных носителей персональных данных.

5. **Действия при ведении и использование типовых форм и журналов учета**.

При использовании и ведении типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных, должностное лицо обязано:

5.1. Использовать только типовую форму или связанные с ней документы (инструкция по её заполнению, карточки, реестры и журналы), которые:

- должны содержать сведения о цели обработки персональных данных,

осуществляемой без использования средств автоматизации, имя (наименование) и адрес Организации, фамилию, имя, отчество, и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых Организацией способов обработки персональных данных;

- должны быть составлены таким образом, чтобы каждый из субъектов

персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;

- должны исключать объединение полей, предназначенных для внесения

персональных данных, цели обработки которых заведомо не совместимы.

5.2. Получать согласие субъекта персональных данных на обработку

персональных данных, осуществляемую без использования средств автоматизации, при необходимости, в виде отметки в специальном поле типовой формы документа.

5.3. Не допускать копирования содержащихся в таких журналах (реестрах, книгах) информации.

6. **Действия при уничтожении или уточнении персональных данных.**

6.1. В случае достижения цели обработки уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, производить способом, исключающим обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе, (удаление, вымарывание).

6.2. Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производить путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях, либо путем изготовления нового материального носителя с уточнением персональных данных.

6.3. Известить всех лиц, которым ранее были сообщены неверные или неполные персональные данные субъекта персональных данных, обо всех произведенных в них исключениях, исправлениях или дополнениях.

7. **Ответственность**

Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, привлекаются к дисциплинарной и материальной, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

ОБЯЗАТЕЛЬСТВО

О НЕРАЗГЛАШЕНИИ ИНФОРМАЦИИ,

СОДЕРЖАЩЕЙ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

Я,\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ сотрудник «Администрации Юстинского РМО Республики Калмыкия» исполняющий(ая) должностные обязанности по должности \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(должность, наименование структурного подразделения)

предупрежден(а) о том, что на период исполнения должностных обязанностей в соответствии с должностным регламентом мне будет предоставлен допуск к информации, содержащей персональные данные субъектов персональных данных.

Настоящим добровольно принимаю на себя обязательства:

1. Не осуществлять незаконную передачу персональных данных и не

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

2. В случае попытки третьих лиц незаконно получить от меня информацию, содержащую персональные данные, сообщать об этом

непосредственному руководителю.

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

4. Не разглашать и не передавать третьим лицам известную мне информацию, содержащую персональные данные, в том числе и после

прекращения права на допуск к информации, содержащей персональные данные.

5. В случае расторжения со мной трудового договора обязуюсь прекратить обработку персональных данных, ставших известными мне в связи с исполнением должностных обязанностей.

Я предупрежден(а) о том, что в случае нарушения данного обязательства,

а также положений, предусмотренных нормами Трудового кодекса Российской Федерации, Федерального закона «О персональных данных», буду привлечен(а) к дисциплинарной и/или иной юридической ответственности в соответствии с законодательством Российской Федерации.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (фамилия, инициалы) (подпись)

"\_\_\_" \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ г.

Приложение №2

к Положению об обработке

персональных данных

П Е Р Е Ч Е Н Ь

должностей в Администрации Юстинского РМО РК

предусматривающий осуществление обработки персональных данных

либо осуществление доступа к персональным данным

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № п/п | Наименование должности | Место хранения материальных носителей персональных данных | Категория персональных данных | Замещение должности предусматривает |
| 1 | Глава Администрации Юстинского РМО РК |  | персональные данные обрабатываемые:* в связи с реализацией трудовых отношений;
* в связи с оказанием муниципальных услуг и осуществлением муниципальных функций;
* в обращениях граждан,

в конкурсах; | осуществление доступак персональным данным |
| 2 | Заместитель главы Администрации Юстинского РМО РК |  |
| 3 | Заместитель главы Администрации Юстинского РМО РК |  |
| 4 | Начальник отдела организационной и кадрово-правовой работы, документационного и материально-технического обеспечения | Рабочий кабинет:-сейф-шкаф |
| 5 | Главный специалист отдела организационной и кадрово-правовой работы, документационного и материально-технического обеспечения | Рабочий кабинет:-сейф-шкаф |
| 6 | Эксперт-консультант-главный бухгалтер Администрации Юстинского РМО РК | Рабочий кабинет:-сейф-шкаф |
| 7 | Эксперт-консультант-архитектор Администрации Юстинского РМО РК |  |
| 8 | Ведущий специалист-системный администратор отдела организационной и кадрово-правовой работы, документационного и материально-технического обеспечения |  |
| 9 | Начальник отдела по земельным и имущественным отношениям |  |
| 10 | Иные сотрудники Администрации Юстинского РМО РК |  |

Приложение №3

к Положению об обработке

персональных данных

СОГЛАСИЕ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ

Я, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

Фамилия, имя, отчество субъекта персональных данных

зарегистрированный (ая) по адресу:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

документ, удостоверяющий личность:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

вид документа, № документа, когда и кем выдан

даю согласие на обработку моих персональных данных Администрацией Яшкульского РМО РК, (далее оператор).

Перечень персональных данных, на обработку которых дается согласие[[1]](#footnote-1):

* + 1. Паспортные данные;
		2. Идентификационный номер налогоплательщика;
		3. Банковские реквизиты;
		4. Контактный телефон.
		5. фамилия, имя, отчество; число, месяц, год рождения;
		6. данные страхового свидетельства обязательного пенсионного страхования;
		7. начисления по заработной плате; данные о вычетах и взносах; номера лицевых счетов;
		8. сведения о детях; сведения о льготах;
		9. социальный пакет.

Перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки:

* + - 1. Получение персональных данных у субъекта персональных данных, а также у третьих лиц, в случае дополнительного согласия субъекта;
			2. Хранение персональных данных (в электронном виде и на бумажном носителе);
			3. Уточнение (обновление, изменение) персональных данных;
			4. Использование персональных данных Администрацией Яшкульского РМО РК для осуществления муниципальных услуг и функций.
			5. Передача персональных данных субъекта в порядке, предусмотренном законодательством РФ.

Обработка вышеуказанных персональных данных будет осуществляться путем смешанной обработки персональных данных (сбор, систематизация, накопление, хранение, уточнение (обновление, изменение использования, распространение), в том числе передача), уничтожение персональных данных).

Срок, действия настоящего согласия с момента заключения трудового договора и до момента его прекращения.

Порядок отзыва настоящего согласия ***по личному заявлению субъекта персональных данных***.

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

подпись расшифровка подписи

«\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_\_

Приложение №4

к Положению об обработке

персональных данных

Инструкция

по организации парольной защиты

Данная инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в ИСПДн, а также контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями.

1. Организационное и техническое обеспечение процессов генерации, использование и прекращение действия паролей во всех подсистемах ИСПДН и контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями возлагается на сотрудников отдела информационных технологий.

2. Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями ИСПДН самостоятельно с учетом следующих требований:

- длина пароля должна быть не менее 8 символов;

- в числе символов пароля обязательно должны присутствовать латинские буквы и цифры;

- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, даты рождения, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);

- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 позициях;

- личный пароль пользователь не имеет права сообщать никому.

Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены о дисциплинарной ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

3. При наличии технологической необходимости в случае возникновения нештатных ситуаций, форс-мажорных обстоятельств и т.п. использования имен и паролей некоторых сотрудников (исполнителей) в их отсутствие, сотрудники обязаны сразу же сменить свой пароль.

4. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в квартал.

5. Внеплановая смена личного пароля или удаление учетной записи пользователя автоматизированной системы в случае прекращения его полномочий (увольнение, переход на другую работу и т.п.) должна производиться уполномоченными сотрудниками отдела информационных технологий немедленно после окончания последнего сеанса работы данного пользователя с системой.

6. В случае компрометации личного пароля пользователя ИСПДН должны быть немедленно предприняты меры в соответствии с п. 5 настоящей Инструкции в зависимости от полномочий владельца скомпрометированного пароля.

7. Хранение сотрудником (исполнителем) значений своих паролей на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе (возможно вместе с персональными ключевыми дискетами и идентификатором Touch Memory).

8. Контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на ответственных за информационную безопасность в подразделениях (руководителей подразделений), периодический контроль - возлагается на сотрудников обеспечения безопасности информации - администраторов средств парольной защиты.

С инструкцией ознакомлен:

Ответственный за обработку

персональных данных \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(ФИО, роспись, дата)

Приложение №5

к Положению об обработке

персональных данных

План

мероприятий по защите персональных данных

в Администрации Юстинского РМО РК

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Мероприятия | Срок выполнения | Ответственный исполнитель |
| 1 | Инвентаризация действующих в Администрации информационных систем персональных данных (далее - ИСПДн): контроль состояния и организации защиты, выявление новых информационных систем (далее - ИС). Инвентаризация проводится с целью выявления и обработки в ИС персональных данных (далее - ПДн) | Раз в год | Заместитель главы Юстинского РМО РКВедущий специалист-системный администратор Администрации Юстинского РМО РК  |
| 2 | Поддержание в актуальном состоянии правовых и организационных документов по защите информации ограниченного доступа в Администрации  | Раз в год  | Заместитель главы Юстинского РМО РКВедущий специалист-системный администратор Администрации Юстинского РМО РК  |
| 3 | Проведение методических занятий по соблюдению правил работы в ИСПДн | Раз в полгода | Заместитель главы Юстинского РМО РКВедущий специалист-системный администратор Администрации Юстинского РМО РК  |
| 4 | Контроль состояния и организации защиты информации в ИСПДн: носители информации, журналы, технические средства защиты информации, средства криптографической защиты информации, допуск и доступ к информации | Раз в год  | Заместитель главы Юстинского РМО РКВедущий специалист-системный администратор Администрации Юстинского РМО РК  |
| 5 | Смена паролей | Раз в год  | Ведущий специалист-системный администратор Администрации Юстинского РМО РК |
| 6 | Обновление антивирусных средств защиты информации | Постоянно | Ведущий специалист-системный администратор Администрации Юстинского РМО РК |

План

внутренних проверок режима защиты персональных данных в

Администрации Юстинского РМО Республики Калмыкия

|  |  |  |  |
| --- | --- | --- | --- |
| №п/п | Мероприятие | Периодичность | Исполнитель |
| 1 | Контроль над соблюдением режима обработки ПДн | Раз в год  | Заместитель главы Юстинского РМО РКВедущий специалист-системный администратор Администрации Юстинского РМО РК  |
| 2 | Контроль над выполнением антивирусной защиты | Постоянно | Ведущий специалист-системный администратор Администрации Юстинского РМО РК |
| 3 | Контроль над соблюдением режима защиты при подключении к сетям общего пользования | Постоянно | Ведущий специалист-системный администратор Администрации Юстинского РМО РК |
| 4 | Проведение внутренних проверок на предмет выявления изменений в режиме обработки и защиты ПДн | Раз в год  | Заместитель главы Юстинского РМО РК |
| 5 | Контроль за обновлениями программного обеспечения и единообразия применяемого ПО на всех элементах ИСПДн | Постоянно | Ведущий специалист-системный администратор Администрации Юстинского РМО РК |
| 6 | Поддержание в актуальном состоянии нормативно-организационных документов | Раз в год  | Заместитель главы Юстинского РМО РК |

Приложение № 6

к Положению об обработке

персональных данных

ИНСТРУКЦИЯ

по учету и работе с электронными, магнитными и оптическими носителями

информации, на которых обрабатываются персональные данные и другая

конфиденциальная информация в Администрации Юстинского РМО РК.

1. Общие положения

Настоящая инструкция определяет общие положения по учету электронных, магнитных, оптических носителей информации на которых обрабатываются

персональные данные и другая конфиденциальная информация в Администрации Юстинского РМО РК (далее Организация) в соответствии с Федеральным законом «О персональных данных» № 152-ФЗ, постановлением Правительства Российской Федерации от 17.11.2007 № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», Приказом ФСТЭК России от 5 февраля 2010 г. N 58 «Об утверждении положения о методах и способах защиты в информационных системах персональных данных».

2. Порядок работы

При исполнении своих служебных обязанностей пользователи информационной системы персональных данных (далее ИСПДн) должны соблюдать следующие основные правила:

- все электронные, магнитные и оптические носители информации (далее носители) - мобильные шасси для жестких магнитных дисков, флеш накопители информации, компакт диски, накопители на гибких магнитных дисках и иные магнитные оптические или магнитооптические диски, используемые в технологическом процессе обработки информации в ИСПДн, подлежат обязательному учету в ведомости «по учету электронных и магнитных носителей, на которых обрабатываются персональные данные (наименование организации)»;

- сотрудник Организации, ответственный за хранение и выдачу носителей, а также список пользователей, работающих с носителями - утверждаются нормативным актом Организации;

- раз в квартал проводить проверку целостности носителей с использованием стандартных средств операционной системы, установленных на ПЭВМ;

- временно не используемые носители должны храниться пользователями и сотрудником Организации, ответственным за их хранение и выдачу носителей, в местах, недоступных для посторонних лиц, исключающих их хищение, подмену, уничтожение;

- временно не используемые носители пользователи по окончанию работы с ними сдают сотруднику Организации, ответственному за их хранение и выдачу;

- учет и выдачу съемных носителей персональных данных по утвержденной форме осуществляют работники структурных подразделений, на которых возложены функции хранения носителей персональных данных. Выдача осуществляется только сотрудникам, допущенным к работе с персональными

данными (далее ПДн) в соответствии с нормативным актом Организации;

- запись ПДн и другой конфиденциальной информации в обязательном порядке осуществляется на учтенные носители;

- обмен ПДн и другой конфиденциальной информацией между организациями должен осуществляться в соответствии с нормативно-правовыми актами (соглашения, договора, заключенных Организацией, согласия субъектов, и Федеральными законами Российской Федерации), на учтенных носителях, с учетом допуска исполнителей к передаваемой информации;

- для обмена информацией на носителях создаются каталоги (папка файловой системы) экспорта данных, после завершения выгрузки информации необходимо производить очистку каталога;

- все находящиеся на хранении и в обращении съемные магнитные и электронные носители (далее – съемный носитель) с персональными данными

подлежат учёту. Каждый съемный носитель с записанными на нем персональными данными должен иметь этикетку или надпись, на которой указывается – Ф.И.О. владельца, дату выдачи, подпись сотрудника ответственного за хранение;

- запрещается передавать носители третьим лицам;

- информацию по различным ИСПДн хранить на носителях в отдельных системных файловых папках.

- резервное копирование информации содержащейся на носителях производит ответственный за работу с носителем по необходимости (можно сразу после записи, если была записана важная информация, утеря которой приведет к

негативным последствиям для организации т.д.), в каталог (папка файловой

системы, ссылка на каталог указывается администратором безопасности), но не реже одного раза в неделю;

- по окончании работ пользователь сдает съемный носитель для хранения уполномоченному должностному лицу, о чем делается соответствующая запись в

ведомости «по учету электронных и магнитных носителей, на которых обрабатываются персональные данные (наименование организации)».

- при необходимости (например информация на носителе далее не нужна) по окончании обработки информации пользователь обязан произвести стирание

остаточной информации на несъёмных носителях (жестких дисках) и в оперативной памяти, одним из способов стирания остаточной информации в

оперативной памяти является перезагрузка ПЭВМ. Перед уничтожением информации необходимо согласовать это действие с сотрудниками, ответственными за обработку и уничтожение информации в Организации;

- перед использованием носителя необходимо провести антивирусный контроль устройства в соответствии с инструкцией по антивирусной защите.

Не допускается:

- хранение съемных носителей с персональными данными вместе с носителями открытой информации, на рабочих столах, либо оставление их без присмотра или передача на хранение другим лицам;

- вынос съемных носителей с персональными данными из служебных помещений для работы с ними на дому, в гостиницах и т. д.

На носители для отправки и передачи записываются только предназначенные адресатам персональные данные. Отправка персональных данных адресатам на съемных носителях осуществляется на учтенных носителях с отметкой в журнале учета носителей об отправке. Вынос съемных носителей персональных данных для непосредственной передачи адресату осуществляется только с письменного разрешения руководителя соответствующего структурного подразделения Организации.

О фактах утраты съемных носителей, содержащих персональные данные, либо разглашения содержащихся на них сведений немедленно ставится в известность руководитель соответствующего структурного подразделения Организации и руководитель Организации.

На утраченные носители составляется акт. Соответствующие отметки вносятся в журналы учета съемных носителей персональных данных.

Съемные носители персональных данных, пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению в соответствии с

действующим законодательством. Также можно съемные носители оставить на

длительный срок хранения до утраты актуальности сведений хранящихся на этих

носителях. После уничтожения материальных носителей членами комиссии

подписывается акт в трех экземплярах и в журналах их учета и регистрации, а также в номенклатурах и описях дел проставляется отметка «Уничтожено. Акт №\_\_(дата)».

Уничтожение носителей осуществляется соответствующей комиссией, состав которой утверждается приказом руководителя Организации. По результатам уничтожения носителей составляется акт утвержденной формы.

Ответственный за обработку

персональных данных \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Приложение № 7

к Положению об обработке

персональных данных

Типовая форма

акта об уничтожении носителей, содержащих персональные данные

Акт № \_\_\_\_\_

об уничтожении носителей, содержащих персональные данные

Я, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

Ответственный за организацию обработки персональных данных провел(а) отбор бумажных, электронных, магнитных и оптических носителей персональных данных и другой конфиденциальной информации (далее носители) и установил(а), что в соответствии с требованиями руководящих документов по защите информации указанные носители и информация записанная на них в процессе эксплуатации, в соответствии с действующим законодательством Российской Федерации, подлежит гарантированному уничтожению и составил(а) настоящий акт о том, что произведено уничтожение носителей персональных данных в составе:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| №п/п | Дата | Тип носителя | Учетный номер носителя | Категория информации  | Примечание |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Всего носителей \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(цифрами и прописью количество)

Перечисленные носители ПДн уничтожены путем

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

(сжигания/размагничивания/физического уничтожения/ механического уничтожения / иного способа)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(фамилия, инициалы) (подпись)

"\_\_\_" \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ г.

Приложение № 8

к Положению об обработке

персональных данных

ДОЛЖНОСТНАЯ ИНСТРУКЦИЯ

ответственного за организацию обработки персональных данных

в Администрации Юстинского РМО Республики Калмыкия

1. Общие положения

1.1. Должностная инструкция ответственного за организацию обработки персональных данных в Администрации Юстинского РМО Республики Калмыкия (далее – должностная инструкция) определяет основные обязанности и права ответственного за организацию обработки персональных данных в администрации Юстинского РМО Республики Калмыкия (далее – Администрация).

1.2. Должностная инструкция регулирует отношения и порядок взаимодействия между ответственным за организацию обработки персональных данных в Администрации и ответственными Администрации, которые обрабатывают персональные данные, в связи с реализацией трудовых отношений, в связи с оказанием муниципальных услуг и осуществлением муниципальных функций, а также в соответствии с действующим законодательством Российской Федерации, за исключением случаев, перечисленных в части 2 статьи 1 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных».

1.3. Ответственный за организацию обработки персональных данных в Администрации в своей деятельности руководствуется действующим законодательством Российской Федерации, муниципальными правовыми актами, а также настоящей должностной инструкцией.

1. Должностные обязанности

Ответственный за организацию обработки персональных данных в Администрации обязан:

2.1 организовывать работу в Администрации по разработке и принятию муниципальных правовых актов, правил обработки персональных данных в Администрации, которые определяют:

- порядок доступа к персональным данным в Администрации;

- организацию приема и обработки в Администрации обращений и запросов субъектов персональных данных или их представителей;

- процедуры, направленные на предотвращение и выявление в Администрации нарушений действующего законодательства Российской Федерации о персональных данных и устранение последствий таких нарушений;

2.2 обеспечивать своевременное размещение на официальном сайте

Администрации муниципальных правовых актов, устанавливающих правила обработки персональных данных в Администрации, в течение 10 дней после их утверждения главой администрации Юстинского РМО Республики Калмыкия, если иной срок размещения не установлен муниципальным правовым актом;

2.3 организовывать ознакомление сотрудников Администрации, непосредственно осуществляющих обработку персональных данных, с действующим законодательством Российской Федерации о персональных данных и муниципальными правовыми актами, определяющими правила обработки персональных данных в Администрации и требования по защите персональных данных;

2.4 руководить осуществлением принятия необходимых правовых, организационных и технических мер для защиты персональных данных в Администрации в соответствии с действующим законодательством Российской Федерации о персональных данных;

2.5 осуществлять согласование мероприятий при создании в Администрации новых информационных систем персональных данных;

2.6 координировать работу в органах Администрации по формированию и ведению перечней:

- должностей сотрудников Администрации, замещение которых предусматривает осуществление обработки персональных данных;

- персональных данных, обрабатываемых в Администрации;

- информационных систем персональных данных Администрации;

2.7 организовывать и руководить проведением внутренних проверок организации состояния работ по вопросам информационной безопасности в Администрации для осуществления периодического контроля:

- условий обработки персональных данных в Администрации и их соответствие требованиям действующего законодательства Российской Федерации о персональных данных и принятыми в соответствии с ним муниципальными правовыми актами;

- организации приема и обработки в Администрации обращений и запросов субъектов персональных данных или их представителей;

- выполнения установленных в соответствии с действующим законодательством Российской Федерации и муниципальными правовыми актами требований к защите персональных данных, обрабатываемых в Администрации;

- соотношения оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения действующего законодательства Российской Федерации о персональных данных и принимаемых Администрацией мер, направленных на обеспечение выполнения обязанностей, предусмотренных действующим законодательством Российской Федерации и муниципальными правовыми актами;

2.8 представлять доклады главе Администрации Юстинского РМО Республики Калмыкия о результатах проведенных внутренних проверок организации состояния работ по вопросам информационной безопасности в Администрации и мерах, необходимых для устранения выявленных нарушений;

2.9 координировать работу в Администрации на принятие мер, направленных на совершенствование защиты персональных данных, обрабатываемых в Администрации;

2.11 осуществлять методическое руководство при разработке условий обработки персональных данных и эффективности мер по защите персональных данных в Администрации;

1. Права

Ответственный за организацию обработки персональных данных в Администрации имеет право:

3.1 запрашивать в органах Администрации, в которых ведется обработка персональных данных или планируется ведение обработки персональных данных, любые сведения, необходимые для организации условий обработки персональных данных и принятия необходимых правовых, организационных и технических мер для защиты персональных данных в Администрации;

3.2 принимать участие в рассмотрении жалоб и обращений граждан или юридических лиц по вопросам, связанным с обработкой персональных данных в Администрации, а также вырабатывать предложения для принятия в пределах своих полномочий решений по результатам рассмотрения указанных жалоб и обращений;

3.3 участвовать в расследовании нарушений в области защиты персональных данных в Администрации и разрабатывать предложения по устранению недостатков и предупреждению подобного рода нарушений;

3.4 требовать от органов Администрации уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных, при обращении (запросе) субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных либо по результатам проведенной внутренней проверки организации состояния работ по вопросам информационной безопасности в Администрации;

3.5 принимать меры по приостановлению или прекращению обработки персональных данных в Администрации, осуществляемой с нарушением требований действующего законодательства Российской Федерации о персональных данных;

3.6 вносить предложения о совершенствовании нормативного правового регулирования обработки и защиты персональных данных в Администрации.

1. Взаимоотношения (связи по должности)

Ответственный за организацию обработки персональных данных в Администрации взаимодействует:

4.1 с отделом по мобилизационной работе, работе с правоохранительными органами и информационной безопасности Администрации – по вопросам организации и контроля защиты персональных данных в Администрации;

4.2 с должностными лицами органов Администрации и других организаций всех организационно-правовых форм – по вопросам организации и выполнения условий обработки и защиты персональных данных в Администрации;

4.3 с территориальными органами федеральных органов, обеспечивающими защиту прав субъектов персональных данных, контроль организации работы с персональными данными и эффективность защиты персональных данных в Администрации, в соответствии со своими полномочиями.

1. Ответственность

Ответственный за организацию обработки персональных данных в Администрации несет ответственность за ненадлежащее выполнение возложенных на него обязанностей, прописанных в настоящей должностной инструкции, в соответствии с действующим законодательством Российской Федерации и муниципальными правовыми актами.

1. Заключительные положения

Должностная инструкция подлежит пересмотру в случае изменения законодательства Российской Федерации о персональных данных, определяющего должностные обязанности ответственного за организацию обработки персональных данных в Администрации.

ОЗНАКОМЛЕН:

Ответственный за организацию

обработки персональных данных в

Администрации Юстинского РМО РК

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/

 (подпись) (ФИО)

Приложение № 9

к Положению об обработке

персональных данных

Перечни

персональных данных, обрабатываемых в администрации Юстинского

 РМО Республики Калмыкия, в связи с реализацией трудовых отношений,

а также в связи с оказанием муниципальных услуг и осуществлением муниципальных функций

1. В состав персональных данных работников Администрации входят документы, содержащие следующую информацию: ФИО (в том числе прежние), дата, месяц, год, место рождения, семейное положение, адрес (адрес по месту регистрации, адрес по месту фактического проживания), фотографическое изображение, образование, профессия, доходы, имущественное положение, национальная принадлежность, состояние здоровья, паспортные данные, данные заграничного паспорта, ИНН; данные свидетельства государственного пенсионного страхования; данные полиса обязательного медицинского страхования; данные документа об образовании; квалификация и специализация по документу; сведения об аттестации, квалификационном чине, сведения о повышении квалификации; сведения о переподготовке кадров; сведения о наградах, поощрениях; контактная информация (номер домашнего телефона, номер рабочего телефона, номер мобильного телефона, e-mail); сведения о воинском учете; данные трудовой книжки; сведения о трудовом стаже, судимости, сведения о предыдущих местах работы, пребывание за границей, допуску к государственной тайне, ученой степени, звании.

2. Комплект документов, сопровождающий процесс оформления трудовых отношений работника и Администрации при его приеме, переводе, увольнении, конкурсе.

Информация, представляемая работником при поступлении на работу в Администрацию, должна иметь документальную форму. При заключении трудового договора в соответствии со статьей 65 Трудового кодекса Российской Федерации лицо, поступающее на работу, предъявляет работодателю:

- Анкету (утвержденную распоряжением Правительства РФ от 26 мая 2005 г. №667-р, согласно Приложения);

- паспорт или иной документ, удостоверяющий личность;

- трудовую книжку, за исключением случаев, когда трудовой договор заключается впервые или работник поступает на работу на условиях совместительства;

- страховое свидетельство государственного пенсионного страхования;

- документ об образовании, о квалификации или наличии специальных знаний - при поступлении на работу, требующую специальных знаний или специальной подготовки;

- документы воинского учета (для военнообязанных).

А также свидетельство о присвоении ИНН (при его наличии у работника). При поступлении на муниципальную службу субъект персональных данных дополнительно предъявляет Администрации документы, предусмотренные Федеральным законом от 02.03.2007 №25-ФЗ «О муниципальной службе в Российской Федерации».

В отдельных случаях, с учетом специфики работы, Трудовым Кодексом РФ, иными федеральными законами, Указами Президента Российской Федерации и постановлениями Правительства Российской Федерации может предусматриваться необходимость предъявления при заключении трудового договора дополнительных документов.

Запрещается требовать от лица, поступающего на работу, документы помимо предусмотренных Трудовым Кодексом РФ, иными федеральными законами, указами Президента Российской Федерации и постановлениями Правительства Российской Федерации.

3. В Администрации создаются и хранятся следующие группы документов, содержащие данные о работниках в единичном или сводном виде:

1) документы, содержащие персональные данные работников (комплексы документов, сопровождающие процесс оформления трудовых отношений при приеме на работу, переводе, увольнении; комплекс материалов по анкетированию, тестированию; проведению собеседований с кандидатом на должность; подлинники и копии распоряжений по личному составу; личные дела и трудовые книжки работников; дела, содержащие основания к распоряжениям по личному составу; дела, содержащие материалы аттестации и присвоения классных чинов муниципальным служащим; служебных расследований; справочно - информационный банк данных по персоналу (картотеки, журналы); подлинники и копии отчетных, аналитических и справочных материалов, реестров направляемых Администрацией в государственные органы статистики, налоговые инспекции, вышестоящие органы управления и другие учреждения);

2) документация по организации работы (положения, должностные инструкции работников, постановления, распоряжения, указания главы Администрации); документы по планированию, учету, анализу и отчетности в части работы с кадрами в Администрации.

4. В Администрации создаются и хранятся следующие группы документов, содержащие персональные данные граждан, связанные с оказанием муниципальных услуг и осуществлением муниципальных функций:

документы, содержащие персональные данные граждан, сопровождающие процесс предоставления муниципальных услуг (комплекты документов, сопровождающие процесс оформления предоставления муниципальной услуги, информационный банк данных по опекунам, опекаемым и приемным семьям, неблагополучных семьях, реестр награжденных, подлинники и копии отчетных, аналитических и справочных материалов, реестров направляемых Администрацией в целях предоставления муниципальных услуг в государственные органы статистики, налоговые инспекции, вышестоящие органы управления и другие учреждения).

Утверждена

распоряжением Правительства

Российской Федерации

от 26 мая 2005 г. № 667-р

*(в ред. от 16 октября 2007 г.)*

**АНКЕТА**

(заполняется собственноручно)

|  |  |  |  |
| --- | --- | --- | --- |
| 1. Фамилия |  |  | Местодляфотографии |
| Имя |  |  |
| Отчество |  |  |

|  |  |
| --- | --- |
| 2. Если изменяли фамилию, имя или отчество, то укажите их, а также когда,где и по какой причине изменяли |  |
| 3. Число, месяц, год и место рождения(село, деревня, город, район, область, край, республика, страна) |  |
| 4. Гражданство (если изменяли, то укажите, когда и по какой причине, если имеете гражданство другого государства — укажите) |  |
| 5. Образование (когда и какие учебные заведения окончили, номера дипломов)Направление подготовки или специальность по дипломуКвалификация по диплому |  |
| 6. Послевузовское профессиональное образование: аспирантура, адъюнктура, докторантура (наименование образовательного или научного учреждения, год окончания)Ученая степень, ученое звание (когда присвоены, номера дипломов, аттестатов) |  |
| 7. Какими иностранными языками и языками народов Российской Федерации владеете и в какой степени (читаете и переводите со словарем, читаете и можете объясняться, владеете свободно) |  |

|  |  |
| --- | --- |
| 8. Классный чин федеральной гражданской службы, дипломатический ранг, воинское или специальное звание, классный чин правоохранительной службы, классный чин гражданской службы субъекта Российской Федерации, квалификационный разряд государственной службы, квалификационный разряд или классный чин муниципальной службы (кем и когда присвоены) |  |
| 9. Были ли Вы судимы, когда и за что (заполняется при поступлении на государственную гражданскую службу Российской Федерации) |  |
| 10. Допуск к государственной тайне, оформленный за период работы, службы, учебы, его форма, номер и дата (если имеется) |  |

11. Выполняемая работа с начала трудовой деятельности (включая учебу в высших и средних специальных учебных заведениях, военную службу, работу по совместительству, предпринимательскую деятельность и т. п.).

При заполнении данного пункта необходимо именовать организации так, как они назывались в свое время, военную службу записывать с указанием должности и номера воинской части.

|  |  |  |
| --- | --- | --- |
| Месяц и год | Должность с указанием организации | Адрес организации(в т. ч. за границей) |
| поступления | ухода |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

12. Государственные награды, иные награды и знаки отличия

|  |
| --- |
|  |
|  |
|  |

13. Ваши близкие родственники (отец, мать, братья, сестры и дети), а также муж (жена), в том числе бывшие.

Если родственники изменяли фамилию, имя, отчество, необходимо также указать их прежние фамилию, имя, отчество.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Степень родства | Фамилия, имя, отчество | Год, число, месяц и место рождения | Место работы (наименование и адрес организации), должность | Домашний адрес(адрес регистрации, фактического проживания) |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

14. Ваши 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 они проживают за границей) |
|  |

|  |  |
| --- | --- |
| 15. Пребывание за границей (когда, где, с какой целью) |  |
|  |
|  |
|  |
| 16. Отношение к воинской обязанности и воинское звание |  |
|  |

17. Домашний адрес (адрес регистрации, фактического проживания), номер телефона (либо

|  |  |
| --- | --- |
| иной вид связи) |  |
|  |
|  |
|  |
|  |
| 18. Паспорт или документ, его заменяющий |  |
|  | (серия, номер, кем и когда выдан) |
|  |
|  |

|  |  |
| --- | --- |
| 19. Наличие заграничного паспорта |  |
|  | (серия, номер, кем и когда выдан) |
|  |
|  |

20. Номер страхового свидетельства обязательного пенсионного страхования (если имеется)

|  |
| --- |
|  |

|  |  |
| --- | --- |
| 21. ИНН (если имеется) |  |

22. Дополнительные сведения (участие в выборных представительных органах, другая ин-

|  |  |
| --- | --- |
| формация, которую желаете сообщить о себе) |  |
|  |
|  |
|  |

23. Мне известно, что сообщение о себе в анкете заведомо ложных сведений и мое несоответствие квалификационным требованиям могут повлечь отказ в участии в конкурсе и приеме на должность, поступлении на государственную гражданскую службу Российской Федерации или на муниципальную службу в Российской Федерации.

На проведение в отношении меня проверочных мероприятий согласен (согласна).

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| « |  | » |  | 20 |  | г. Подпись |  |

|  |  |
| --- | --- |
| М. П. | Фотография и данные о трудовой деятельности, воинской службе и об учебе оформляемого лица соответствуют документам, удостоверяющим личность, записям в трудовой книжке, документам об образовании и воинской службе. |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| « |  | » |  | 20 |  | г. |  |
|  |  | (подпись, фамилия работника кадровой службы) |

Приложение № 10

к Положению об обработке

персональных данных

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, категории субъектов, персональные данные которых

обрабатываются, сроки их обработки и хранения, порядок

уничтожения при достижении целей обработки или при наступлении

иных законных оснований) в Администрации Юстинского РМО РК.

1. Обработка персональных данных должна осуществляться на законной основе.

2. Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

3. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

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

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

6. При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.

7. Меры, направленные на выявление и предотвращение нарушений, предусмотренных законодательством:

1) осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных Федеральному закону от 27.07.2006г. №152-Ф3 (далее - Федеральный закон);

2) ознакомление работников оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных

данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.

8. Обеспечение безопасности персональных данных достигается, в частности:

1) определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

2) применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

3) применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

4) оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

5) учетом машинных носителей персональных данных;

6) обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;

7) восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

8) установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных.

9. Целями обработки персональных данных работников являются:

1) обеспечение соблюдения законов и иных нормативных правовых актов;

2) учет работников;

3) соблюдение порядка и правил приема сотрудников;

4) использование в уставной деятельности с применением средств автоматизации или без таких средств, включая хранение этих данных в архивах и размещение в информационно-телекоммуникационных сетях с целью предоставления доступа к ним;

5) с оказанием муниципальных услуг и осуществлением муниципальных функций

6) обеспечение личной безопасности работников.

10. Хранение персональных данных должно осуществляться 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 достижении целей

обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

11. В случае выявления неправомерной обработки персональных данных,

осуществляемой оператором или лицом, действующим по поручению оператора, оператор в срок, не превышающий 3 (трех) рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению

оператора. 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 или обеспечить их уничтожение. 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 указанный орган.

12. В случае достижения цели обработки персональных данных оператор обязан прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в срок, не превышающий 30 (тридцати) дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом.

13. В случае отзыва субъектом персональных данных согласия на обработку своих персональных данных оператор обязан прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий 3-х дней с даты получения указанного отзыва, если иное не предусмотрено соглашением между оператором и субъектом персональных данных. Об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных.

14. В случае отсутствия возможности уничтожения персональных данных в течение сроков, указанных выше, оператор осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и обеспечивает

уничтожение персональных данных в срок не более чем 6 (шесть) месяцев, если иной срок не установлен федеральными законами.

Приложение № 11

к Положению об обработке

персональных данных

ПРАВИЛА

рассмотрения запросов субъектов персональных данных

в Администрации Юстинского РМО Республики Калмыкия

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящие Правила разработаны в соответствии с Федеральным законом «О персональных данных» от 27.07.2006г. № 152-ФЗ и Трудовым Кодексом Российской Федерации и определяют порядок обработки поступающих в Администрацию Юстинского РМО Республики Калмыкия (далее Администрация).

2. ПРАВА СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. В соответствии с действующим законодательством субъект ПДн имеет право на получение при обращении или при получении запроса информации, касающейся обработки его персональных данных, в том числе содержащей:

2.1.1. подтверждение факта обработки персональных данных Администрации, а также цель такой обработки;

2.1.2. способы обработки персональных данных, применяемые Администрацией;

2.1.3. сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;

2.1.4. перечень обрабатываемых персональных данных и источник их получения;

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

2.1.6. сведения о том, какие юридические последствия для субъекта персональных данных может повлечь за собой обработка его персональных данных.

2.2. Право субъекта персональных данных на доступ к своим персональным данным ограничивается в случае, если:

2.2.1. обработка персональных данных, в том числе персональных данных, полученных в результате оперативно-розыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;

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

2.2.3. предоставление персональных данных нарушает конституционные права и свободы других лиц.

2.3. Если субъект персональных данных считает, что Администрация 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 Администрации в уполномоченном органе по защите прав субъектов персональных данных или в судебном порядке.

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

3. ПОРЯДОК РАБОТЫ С ОБРАЩЕНИЯМИ СУБЪЕКТОВ

3.1. При поступлении обращения субъекта, необходимо зарегистрировать его в Журнале учета обращений субъектов персональных данных.

3.2. Администрация обязана сообщить субъекту персональных данных или его законному представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с ними при обращении субъекта персональных данных или его законного представителя либо в течение десяти рабочих дней с даты получения запроса субъекта персональных данных или его законного представителя.

3.3. В случае отказа в предоставлении субъекту персональных данных или его законному представителю при обращении либо при получении запроса субъекта персональных данных или его законного представителя информации о наличии персональных данных о соответствующем субъекте персональных данных, а также таких персональных данных Департамент обязан дать в письменной форме мотивированный ответ в срок, не превышающий семи рабочих дней со дня обращения субъекта персональных данных или его законного представителя либо с даты получения запроса субъекта персональных данных или его законного представителя.

3.4. Администрация обязана безвозмездно предоставить субъекту персональных данных или его законному представителю возможность ознакомления с персональными данными, относящимися к соответствующему субъекту персональных данных, а также внести в них необходимые изменения, уничтожить или блокировать соответствующие

персональные данные по предоставлении субъектом персональных данных или его законным представителем сведений, подтверждающих, что персональные данные, которые относятся к соответствующему субъекту и обработку которых осуществляет Департамент, являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки. О внесенных изменениях и предпринятых мерах Администрация обязана уведомить субъекта персональных данных или его законного представителя и третьих лиц, которым персональные данные этого субъекта были переданы.

Приложение № 12

к Положению об обработке

персональных данных

ПРАВИЛА

осуществления внутреннего контроля соответствия обработки персональных

данных требованиям к защите персональных данных Администрации Юстинского РМО Республики Калмыкия.

ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящие Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных Администрации Юстинского РМО Республики Калмыкия (далее Администрация) разработаны с учетом Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и 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».

1.2. Настоящие Правила определяют порядок осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных и действуют постоянно.

2. ТЕМАТИКА ВНУТРЕННЕГО КОНТРОЛЯ

2.1. Тематика проверок обработки персональных данных с использованием средств автоматизации:

2.1.1. соответствие полномочий пользователя матрице доступа;

2.1.2. соблюдение пользователями информационных систем персональных данных Администрации парольной политики;

2.1.3. соблюдение пользователями информационных систем персональных данных Администрации антивирусной политики;

2.1.4. соблюдение пользователями информационных систем персональных данных Администрации правил работы со съемными носителями персональных данных;

2.1.5. соблюдение ответственными за криптографические средства защиты информации правил работы с ними;

2.1.6. соблюдение порядка доступа в помещения Администрации, где расположены элементы информационных систем персональных данных;

2.1.7. соблюдение порядка резервирования баз данных и хранения резервных копий;

2.1.8. соблюдение порядка работы со средствами защиты информации;

2.1.9. знание пользователей информационных систем персональных данных о своих действиях во внештатных ситуациях.

2.2. Тематика проверок обработки персональных данных без использования средств автоматизации:

2.2.1. хранение бумажных носителей с персональными данными;

2.2.2. доступ к бумажным носителям с персональными данными;

2.2.3. доступ в помещения, где обрабатываются и хранятся бумажные носители с персональными данными.

3. ПОРЯДОК ПРОВЕДЕНИЯ ВНУТРЕННИХ ПРОВЕРОК

3.1. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям Администрация организует проведение периодических проверок условий обработки персональных данных.

3.2. Проверки осуществляются ответственным за организацию обработки

персональных данных (далее Ответственный) либо комиссией, образуемой руководителем Администрации.

3.3. Внутренние проверки проводятся по необходимости в соответствии с поручением руководителя Администрации.

3.4. Проверки осуществляются Ответственным либо комиссией непосредственно на месте обработки персональных данных путем опроса либо, при необходимости, путем осмотра рабочих мест сотрудников, участвующих в процессе обработки персональных данных.

3.5. Для каждой проверки составляется Протокол проведения внутренней проверки.

Форма Протокола приведена в Приложении к настоящим Правилам.

3.6. При выявлении в ходе проверки нарушений, Ответственным либо Председателем комиссии в Протоколе делается запись о мероприятиях по устранению нарушений и сроках исполнения.

3.7. Протоколы хранятся у Ответственного либо Председателя комиссии в течение текущего года. Уничтожение Протоколов проводится Ответственным либо комиссией самостоятельно в январе следующего за проверочным годом.

3.8. О результатах проверки и мерах, необходимых для устранения нарушений, руководителю Департамента докладывает Ответственный либо Председатель комиссии.

Приложение

АКТ

проведения внутренней проверки условий обработки персональных данных

Администрации Юстинского РМО Республики Калмыкия

Настоящий Акт составлен в том, что \_\_.\_\_.201\_ ответственным за организацию обработки персональных данных по внутреннему контролю проведена проверка

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

тема проверки

Проверка осуществлялась в соответствии с требованиями

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

название документа

В ходе проверки проверено:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Выявленные нарушения:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Меры по устранению нарушений:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Срок устранения нарушений: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

Должность Ответственного \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ И.О. Фамилия

Журнал

проведения внутренней проверки условий обработки персональных

данных Администрации Юстинского РМО Республики Калмыкия

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № п/п | Цель проверки  | ФИОдолжностного лица осуществляющегопроверку | Подпись |  Дата  |
| 1 |  |  |  |  |
| 2 |  |  |  |  |

/ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /Должность/

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ / ФИО должностного лица

Лист ознакомлений

с положением «О порядке обработки персональных данных»

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Фамилия, имя, отчество  | Дата ознакомления  | Роспись  |
| 1 |  |  |  |
| 2 |  |  |  |
| 3 |  |  |  |
| 4 |  |  |  |
| 5 |  |  |  |
| 6 |  |  |  |
| 7 |  |  |  |
| 8 |  |  |  |
| 9 |  |  |  |
| 10 |  |  |  |
| 11 |  |  |  |
| 12 |  |  |  |
| 13 |  |  |  |
| 14 |  |  |  |
| 15 |  |  |  |
| 16 |  |  |  |
| 17 |  |  |  |
| 18 |  |  |  |
| 19 |  |  |  |
| 20 |  |  |  |
| 21 |  |  |  |
| 22 |  |  |  |
| 23 |  |  |  |
| 24 |  |  |  |
| 25 |  |  |  |
| 26 |  |  |  |
| 27 |  |  |  |
| 28 |  |  |  |
| 29 |  |  |  |
| 30 |  |  |  |

1. Для обработки персональных данных, содержащихся в согласии в письменной форме субъекта на обработку его персональных данных, дополнительное согласие не требуется.

 [↑](#footnote-ref-1)