Приложение № 1

Утверждено
приказом Министерства
земельных и имущественных
отношений Республики Тыва
от 26.04.2021 г. № 16-од

Правила обработки персональных данных в Министерстве земельных и имущественных отношений Республики Тыва

1. Общие положения

Настоящие Правила обработки персональных данных в Министерстве земельных и имущественных отношений Республики Тыва (далее – Правила) направлены на предотвращение нарушений законодательства Российской Федерации, регулирующего обработку персональных данных (далее – ПДн), а также определяющие содержание обрабатываемых ПДн, категории субъектов, ПДн которых обрабатываются, сроки их обработки и хранения, порядок уничтожения ПДн при достижении целей обработки ПДн.

Настоящим Правилом определяется порядок обработки сведений, относящихся к персональным данным субъектов персональных данных в Министерстве земельных и имущественных отношений Республики Тыва (далее - Министерство) осуществляемым с использованием средств автоматизации, в том числе в информационно телекоммуникационных сетях, или без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру действий совершаемых с персональными данными с использованием средств автоматизации.

Правила разработаны в соответствии с федеральными законами от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 27.07.2006 г. № 152-ФЗ «О персональных данных», Трудовым кодексом Российской Федерации, постановлениями Правительства Российской Федерации от 21.03.2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», от 15.09.2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», нормативными и методическими документами по технической защите информации ФСТЭК России и ФСБ России.

2. Основные термины и понятия

В настоящем Положении используются следующие термины и понятия, применяемые в значениях, предусмотренных Федеральным законом «О персональных данных»:

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

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

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

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

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

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

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

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

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

10) *конфиденциальность персональных данных* - обязательное для соблюдения Минземимуществом Республики Тыва или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания;

11) *общедоступные персональные данные* - персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

3. Категории субъектов персональных данных

В Министерстве земельных и имущественных отношений Республики Тыва осуществляется обработка персональных данных следующих субъектов персональных данных:

– граждан, направляющих обращения в Министерство земельных и имущественных отношений Республики Тыва;

– контрагентов по исполнению договоров;

– работников Министерства земельных и имущественных отношений Республики Тыва;

– кандидатов, участвующих в конкурсе на замещение вакантных должностей государственной службы, на включение в кадровый резерв;

– граждан, включенных в кадровый резерв государственной службы;

– награждаемых юридических и физических лиц.

4. Принципы обработки ПДн

Обработка ПДн в Министерстве земельных и имущественных отношений Республики Тыва должна осуществляться на законной и справедливой основе и ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка ПДн, несовместимая с целями сбора ПДн.

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

Содержание и объем обрабатываемых ПДн должны соответствовать заявленным целям обработки. Обрабатываемые ПДн не должны быть избыточными по отношению к заявленным целям их обработки.

При обработке ПДн должны быть обеспечены точность ПДн, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки ПДн. Должны приниматься необходимые меры по удалению или уточнению не полных или неточных данных.

Хранение ПДн должно осуществляться в форме, позволяющей определить субъект ПДн, не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен федеральным законом или иным нормативным правовым актом. Обрабатываемые в Министерстве земельных и имущественных отношений Республики Тыва ПДн подлежат уничтожению, либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

5. Цели обработки ПДн

Цели обработки ПДн должны быть четко определены и соответствовать:

– заявленным в положении (уставе) о Министерстве земельных и имущественных отношений Республики Тыва основным полномочиям и правам;

– задачам и функциям Министерства земельных и имущественных отношений Республики Тыва.

Цели обработки ПДн определяют:

– содержание и объем обрабатываемых ПДн;

– категории субъектов ПДн;

– сроки их обработки и хранения;

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

Цели обработки ПДн должны быть конкретны, заранее определены, законны и заявлены.

Обработка ПДн в Министерстве земельных и имущественных отношений Республики Тыва осуществляется для исполнения наделенных полномочий, организации кадровой работы, финансовой деятельности в соответствии с действующим положением.

6. Способы и правила обработки ПДн

5.1. В Министерстве земельных и имущественных отношений Республики Тыва применяется два способа обработки ПДн:

– обработка ПДн без использования средств автоматизации;

– обработка ПДн с использованием средств автоматизации.

5.2. Правила обработки ПДн без использования средств автоматизации

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

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

При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них ПДн (далее – типовая форма), должны соблюдаться следующие условия:

– типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки ПДн, осуществляемой без использования средств автоматизации;

– имя (наименование) и адрес оператора;

– фамилию, имя, отчество и адрес субъекта ПДн;

– источник получения ПДн;

– сроки обработки ПДн;

– перечень действий с ПДн, которые будут совершаться в процессе их обработки;

– общее описание используемых оператором способов обработки ПДн;

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

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

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

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

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

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

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

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

5.3. Обработка ПДн с использованием средств автоматизации в Министерстве земельных и имущественных отношений Республики Тыва допускается в следующих случаях:

– обработка ПДн осуществляется с согласия субъекта ПДн на обработку его ПДн;

– обработка ПДн необходима для достижения целей, предусмотренных законом, осуществления и выполнения, возложенных на Министерство земельных и имущественных отношений Республики Тыва полномочий и обязанностей;

– обработка ПДн необходима для исполнения договора, стороной которого является субъект ПДн, а также для заключения договора по инициативе субъекта ПДн;

– обработка ПДн необходима для предоставления государственных услуг гражданам и организациям;

– обработка ПДн необходима для осуществления прав и законных интересов Министерства земельных и имущественных отношений Республики

Тыва или третьих лиц, либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта ПДн;

– осуществляется обработка ПДн, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

Обработка ПДн средствами автоматизации должна осуществляться на основании правил, инструкций, руководств, регламентов и иных документов, определяющих технологический процесс обработки информации, содержащей такие данные.

6. Обработка ПДн с согласия субъекта ПДн

Оператор перед обработкой ПДн получает у субъектов обработки ПДн согласие на обработку ПДн.

Согласие на обработку ПДн может быть дано субъектом ПДн или его представителем только в письменной форме. Равнозначным содержащему собственноручную подпись субъекта ПДн согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с действующим законодательством электронной подписью.

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

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

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

Согласие на обработку ПДн может быть отозвано субъектом ПДн путем направления запроса в Министерство земельных и имущественных отношений Республики Тыва.

7. Обработка ПДн без согласия субъекта ПДн

Обработка ПДн без получения согласия на такую обработку от субъекта ПДн в Министерство земельных и имущественных отношений Республики Тыва может осуществляться при наличии оснований, предусмотренных пунктами 2 - 11 части 1 статьи 6 Федерального закона от 27.07.2006 г. № 152-ФЗ.

8. Правила обработки ПДн при поручении обработки ПДн другому лицу

Министерство земельных и имущественных отношений Республики Тыва вправе поручить обработку ПДн другому лицу:

– с согласия субъекта ПДн, если иное не предусмотрено федеральным законом;

– на основании заключаемого с этим лицом договора;

– путем принятия соответствующего акта (далее – поручение оператора).

Лицо, осуществляющее обработку ПДн по поручению Министерства земельных и имущественных отношений Республики Тыва, обязано соблюдать принципы и правила обработки ПДн.

В случае, если Министерство земельных и имущественных отношений Республики Тыва поручит обработку ПДн другому лицу, ответственность перед субъектом ПДн за действия указанного лица несет Министерство земельных и имущественных отношений Республики Тыва. Лицо, осуществляющее обработку ПДн по поручению Министерство земельных и имущественных отношений Республики Тыва, несет ответственность перед Министерством земельных и имущественных отношений Республики Тыва.

В случае необходимости получения согласия на обработку ПДн от субъекта ПДн обязанность получения такого согласия возлагается на Министерство.

9. Правила обработки общедоступных ПДн

Общедоступные ПДн физических лиц, полученные из сторонних общедоступных источников ПДн, обрабатываются в исключительных случаях в сроки, не превышающие необходимые для их использования. При этом совместно с такими данными должны собираться реквизиты их источника и подтверждение согласия субъекта ПДн на включение такой информации в общедоступные источники ПДн, так как в случае обработки общедоступных ПДн обязанность доказывания того, что обрабатываемые ПДн являются общедоступными, возлагается на Министерство.

По достижению целей обработки общедоступных ПДн они подлежат немедленному уничтожению.

С целью информационного обеспечения и осуществления взаимодействия со сторонними физическими и юридическими лицами в Министерстве могут создаваться общедоступные источники ПДн. Создание общедоступного источника ПДн осуществляется по решению руководителя Министерства.

В решении о создании общедоступного источника ПДн должны быть указаны:

– цель создания общедоступного источника ПДн;

– ссылка на нормативный акт, устанавливающий необходимость создания общедоступного источника ПДн (при наличии);

– перечень персональных данных, которые вносятся в общедоступный источник ПДн;

– порядок включения ПДн в общедоступный источник ПДн;

– порядок уведомления пользователей общедоступного источника ПДн;

– порядок получения письменного согласия субъекта ПДн на включение ПДн в общедоступный источник ПДн.

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

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

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

10. Правовое основание обработки ПДн

10.1. Правовое основание обработки ПДн в Министерстве включает в себя:

- определение законности целей обработки ПДн;
- оценку вреда, который может быть причинен субъекту ПДн в случае нарушения требований по обработке и обеспечению безопасности ПДн;
- определение заданных характеристик безопасности ПДн;
- определение сроков обработки, в т.ч. хранения ПДн, осуществление контроля за соблюдением сроков обработки ПДн и фактов достижения целей обработки ПДн.

10.2. Определение законности целей обработки ПДн

Заявляемые цели обработки ПДн должны быть законны, а также должны рассматриваться и соответственно иметь правовое основание особые правила обработки ПДн (такие как специальные и биометрические категории ПДн, и др.).

При определении правовых оснований обработки ПДн должны определяться реквизиты федеральных законов, а также иных подзаконных актов и документов, которые требуют обработки ПДн или иных документов, являющихся такими основаниями.

Обработка ПДн без документально определенного и оформленного правового основания обработки ПДн в Министерстве не допускается.

10.3. Оценка вреда, который может быть причинен субъектам ПДн в случае нарушения требований по обработке и обеспечению безопасности ПДн.

Оценкой вреда, который может быть причинен субъекту ПДн в случае нарушения требований по обработке и обеспечению безопасности ПДн, является определение юридических или иным образом затрагивающих права и законные интересы последствий в отношении субъекта ПДн, которые могут возникнуть в случае нарушения требований по обработке и обеспечению безопасности ПДн.

К юридическим последствиям относятся случаи возникновения, изменения или прекращения личных, либо имущественных прав граждан или иным образом затрагивающих его права, свободы и законные интересы.

При обработке ПДн должны определяться и документально оформляться все возможные юридические или иным образом затрагивающие права и законные интересы последствия в отношении субъекта ПДн, которые могут возникнуть в случае нарушения требований по обработке и обеспечению безопасности ПДн.

Определение таких юридических последствий необходимо для недопущения нарушения и обеспечения защиты прав и свобод человека и гражданина при обработке его ПДн, в т.ч. защиты прав на неприкосновенность частной жизни, личную и семейную тайну, а также определения соотношения

вреда, который может быть причинен субъектам ПДн в случае нарушения требований по обработке и обеспечению безопасности ПДн и принимаемых мер.

Обработка ПДн в Министерстве без принятия мер по обеспечению безопасности ПДн не допускается.

10.4. Заданные характеристики безопасности ПДн.

Всеми работниками Министерства, получающими доступ к ПДн, должна обеспечиваться конфиденциальность таких данных.

Конфиденциальность персональных данных – это обязательное для соблюдения Министерства требование не раскрывать третьим лицам и не распространять ПДн без согласия субъекта ПДн, если иное не предусмотрено федеральным законом.

Вне зависимости от необходимости обеспечения конфиденциальности ПДн, при обработке ПДн должно определяться наличие требований по обеспечению иных характеристик безопасности ПДн, отличных от нее.

К таким характеристикам относятся требования:

– по обеспечению защищенности от уничтожения ПДн;

– по обеспечению защищенности от изменения ПДн;

– по обеспечению защищенности от блокирования ПДн;

– по обеспечению защищенности от иных несанкционированных действий.

Обеспечение указанных характеристик безопасности ПДн устанавливается федеральными законами и иными нормативными правовыми актами.

Обработка ПДн без документально определенного и оформленного решения по определению характеристик безопасности ПДн не допускается.

10.5. Определение сроков обработки, в т.ч. хранения ПДн, осуществление контроля за соблюдением сроков обработки ПДн и фактов достижения целей обработки ПДн.

На основании определенных целей обработки ПДн, способов обработки и образующихся в процессе такой обработки различных видов документов устанавливаются сроки такой обработки ПДн, в том числе хранения.

Определение сроков хранения осуществляется в соответствии с требованиями законодательства Российской Федерации, в т. ч. в соответствии с перечнями типовых архивных документов с указанием сроков их хранения.

При использовании документов, содержащих ПДн, в различных целях, определение сроков обработки, в т.ч. хранения, таких документов устанавливается по максимальному сроку, предусмотренному федеральным законом. При этом в случае наличия ПДн в таких документах, обработка которых более не требуется, производятся действия по уничтожению таких данных.

Обработка ПДн без документально определенных и оформленных сроков обработки, в том числе хранения ПДн, не допускается.

С целью выполнения требования по уничтожению, либо обезличиванию ПДн по достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом, в Министерстве может создаваться комиссия, определяющая факт достижения целей обработки ПДн и достижение предельных сроков хранения документов, содержащих ПДн.

11. Действия (операции) с ПДн

Обработкой ПДн называется любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств, включая: сбор, запись, систематизацию, накопление, хранение, уточнение, извлечение, использование, передачу, обезличивание, блокирование, удаление, уничтожение персональных данных.

Обработка ПДн без определенных и документально оформленных действий (операций), совершаемых с ПДн, не допускается.

12. Осуществление сбора ПДн

12.1. Способы сбора ПДн и источники их получения

В Министерстве применяются следующие способы получения ПДн субъектов ПДн:

- заполнение субъектом ПДн соответствующих форм;
- получение ПДн от третьих лиц;
- получение данных на основании запроса третьим лицам;
- сбор данных из общедоступных источников.

12.2. Правила сбора ПДн

Если предоставление ПДн является обязательным в соответствии с федеральными законами, иными нормативными правовыми документами, Министерство обязано разъяснить субъекту ПДн юридические последствия отказа предоставить его ПДн.

Если основания на обработку ПДн без согласия отсутствуют, то необходимо получение согласия субъекта ПДн на обработку его ПДн. Обработка ПДн без получения такого согласия запрещается.

Если ПДн получены не от субъекта ПДн Министерство до начала обработки таких ПДн обязано предоставить субъекту ПДн следующую информацию:

- наименование оператора или его представителя;
- сведения о цели обработки ПДн и ее правовое основание;
- сведения о предполагаемых пользователях ПДн;
- сведения об установленных правах субъекта ПДн;
- сведения об источниках получения ПДн.

Министерство освобождается от обязанности предоставлять субъекту ПДн сведения в случаях, если:

- субъект ПДн уведомлен об осуществлении обработки его ПДн соответствующим оператором;
- ПДн получены на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн;
- персональные данные сделаны общедоступными субъектом ПДн или получены из общедоступного источника;
- предоставление субъекту ПДн сведений нарушает права и законные интересы третьих лиц.

13. Осуществление систематизации, накопления, уточнения и использования ПДн

Систематизация, накопление, уточнение, использование ПДн в Министерстве осуществляются законными способами в соответствии с правилами, инструкциями, руководствами, регламентами и иными документами, определяющими технологический процесс обработки информации.

Уточнение персональных данных в Министерстве производиться только на основании законно полученной в установленном порядке информации.

Решение об уточнении ПДн субъекта ПДн принимается лицом, ответственным за организацию обработки ПДн.

Использование персональных данных в Министерстве осуществляться исключительно в заявленных целях. Использование ПДн в заранее не определенных и не оформленных установленным образом целях не допускается.

14. Осуществление передачи ПДн

Передача персональных данных в Министерстве осуществляется с соблюдением настоящих Правил и действующего законодательства Российской Федерации.

В Министерство приняты следующие способы передачи ПДн субъектов ПДн:

– передача ПДн на электронных и бумажных носителях информации нарочно;

– передача ПДн на электронных и бумажных носителях посредством почтовой связи;

– передача ПДн по электронным каналам.

Перед осуществлением передачи ПДн проверяется основание на осуществление такой передачи и наличие согласия на передачу ПДн в согласии субъекта ПДн на обработку ПДн или наличие иных законных оснований.

Передача ПДн должна осуществляться на основании:

– договора с третьей стороной, которой осуществляется передача ПДн;

– запроса, полученного от третьей стороны, которой осуществляется передача ПДн;

– исполнения возложенных законодательством Российской Федерации на Министерство функций, полномочий и обязанностей.

15. Осуществление хранения ПДн

Хранение ПДн в Министерстве осуществляется в форме документов, зафиксированной на материальном носителе информации (содержащей ПДн) с реквизитами, позволяющими ее идентифицировать и определить субъекта ПДн.

При этом в Министерстве предусматриваются следующие виды документов:

– изобразительный документ – документ, содержащий информацию, выраженную посредством изображения какого-либо объекта;

– фотодокумент – изобразительный документ, созданный фотографическим способом;

– письменный документ – текстовой документ, информация которого зафиксирована любым типом письма;

– рукописный документ – письменный документ, при создании которого знаки письма наносят от руки;

– машинописный документ – письменный документ, при создании которого знаки письма наносят техническими средствами;

– документ на машинном носителе – документ, созданный с использованием носителей и способов записи, обеспечивающих обработку его информации электронно-вычислительной машиной.

Хранение ПДн в Министерстве осуществляется в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен федеральным законом, иным нормативным документом.

Хранение ПДн в Министерстве осуществляется на таких материальных носителях информации и с применением такой технологии ее хранения, которые обеспечивают защиту этих данных от неправомерного или случайного: доступа к ним; их уничтожения; изменения; блокирования; копирования; предоставления; распространения.

16. Осуществление блокирования ПДн

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

Блокирование ПДн конкретного субъекта ПДн осуществляться во всех информационных системах ПДн, обслуживаемых Министерством.

Блокирование ПДн осуществляется:

– в случае выявления неправомерной обработки ПДн при обращении субъекта ПДн или его представителя, либо по запросу субъекта ПДн или его представителя, либо уполномоченного органа по защите прав субъектов ПДн с момента такого обращения или получения указанного запроса на период проверки;

– в случае отсутствия возможности уничтожения ПДн в установленные сроки до их уничтожения.

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

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

17. Осуществление обезличивания ПДн

Обезличивание персональных данных при обработке ПДн с использованием средств автоматизации осуществляется на основании нормативных правовых

актов, правил, инструкций, руководств, регламентов и иных документов для достижения заранее определенных и заявленных целей.

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

18. Осуществление уничтожения ПДн

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

Уничтожение ПДн в Министерстве производится в следующих случаях:

– обрабатываемые ПДн подлежат уничтожению, либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом;

– ПДн являются незаконно полученными или не являются необходимыми для заявленной цели обработки;

– в случае выявления неправомерной обработки ПДн, если обеспечить правомерность обработки ПДн невозможно;

– в случае достижения цели обработки ПДн;

– в случае отзыва субъектом ПДн согласия на обработку его ПДн и в случае, если сохранение ПДн более не требуется для целей обработки ПДн.

При уничтожении ПДн необходимо:

– убедиться в необходимости уничтожения ПДн;

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

– уничтожить ПДн подходящим способом в соответствии с настоящими Правилами или способом, указанным в соответствующем требовании или распорядительном документе;

– проверить необходимость уведомления об уничтожении ПДн;

– при необходимости уведомить об уничтожении ПДн требуемых лиц.

При уничтожении ПДн применяются следующие способы:

– измельчение в бумагорезательной (бумагоуничтожительной) машине – для документов, исполненных на бумаге;

– физическое уничтожение частей носителей информации – разрушение или сильная деформация для носителей информации на жестком магнитном диске (уничтожению подлежат внутренние диски и микросхемы);

– CD (DVD)-дисках, USB- и Flash-носителях (уничтожению подлежат модули и микросхемы долговременной памяти);

– стирание с помощью сертифицированных средств уничтожения информации – для записей в базах данных и отдельных документов на машинном носителе.

При необходимости уничтожения части ПДн допускается уничтожать материальный носитель одним из указанных в настоящих Правилах способов,

с предварительным копированием сведений, не подлежащих уничтожению, способом, исключающим одновременное копирование ПДн, подлежащих уничтожению.

По факту уничтожения ПДн в Министерстве составляется акт об уничтожении ПДн, который подписывается лицами, производившими уничтожение, заверяется лицом, ответственным за организацию обработки ПДн, присутствовавшим при уничтожении, и утверждается руководителем Министерства.

Хранение актов об уничтожении ПДн осуществляется в течение срока исковой давности, если иное не установлено нормативными правовыми актами Российской Федерации.

19. Права и обязанности субъекта ПДн и Министерства земельных и имущественных отношений Республики Тыва при обработке ПДн

19.1. Права субъекта ПДн

Субъект персональных данных, чьи ПДн обрабатываются в Министерстве имеет право:

– на получение сведений о подтверждении факта обработки ПДн Министерстве;

– на получение сведений о правовых основаниях и целях обработки ПДн;

– на получение сведений о лицах (за исключением сведений о государственных служащих и сотрудниках Министерства, которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании служебного контракта (трудового договора) или на основании федерального закона;

– на получение сведений об обрабатываемых ПДн, относящихся к соответствующему субъекту ПДн, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

– на получение сведений о сроках обработки ПДн, в т.ч. сроках их хранения;

– на получение сведений о порядке осуществления субъектом ПДн своих прав, предусмотренных законодательством в области ПДн;

– на получение информации об осуществленной или о предполагаемой трансграничной передаче данных;

– на получение сведений о наименовании и адресе лица, осуществляющего обработку ПДн по поручению Министерства, если обработка поручена или будет поручена такому лицу;

– на получение иных сведений, предусмотренных законодательством в области ПДн и другими федеральными законами;

– требовать от Министерства уточнения его ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки;

– принимать предусмотренные законом меры по защите своих прав;

– требовать от Министерства предоставления ему ПДн в доступной форме;

– повторного обращения и запроса в целях получения сведений и ознакомления с его персональными данными;

– заявить возражение против принятия решения на обработку ПДн, порождающего юридические последствия в отношении субъекта ПДн или иным образом затрагивающего его права и законные интересы;

– обжаловать действия или бездействие Министерства в уполномоченный орган по защите прав субъектов ПДн или в судебном порядке, если субъект ПДн считает, что Министерство осуществляет обработку его ПДн с нарушением требований федерального закона или иным образом нарушает его права и свободы;

– на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке;

– требовать предоставления безвозмездно субъекту ПДн или его представителю возможности ознакомления с персональными данными, относящимися к этому субъекту ПДн;

– принимать решение о предоставлении его ПДн и давать согласие на их обработку свободно, своей волей и в своем интересе;

– отзывать согласие на обработку ПДн.

19.2. Обязанности субъекта ПДн

Субъект персональных данных, чьи ПДн обрабатываются в Министерстве, обязан:

– предоставлять свои ПДн в случаях, когда федеральными законами предусматриваются случаи обязательного предоставления субъектом ПДн своих персональных данных;

– с целью соблюдения его законных прав и интересов подавать только достоверные ПДн.

Кроме указанных обязанностей в вопросах обработки его ПДн на субъекта ПДн налагаются иные обязанности, предусмотренные действующим законодательством Российской Федерации.

19.3. Права Министерства при обработке ПДн субъектов ПДн

Министерство земельных и имущественных отношений Республики Тыва при обработке ПДн субъектов ПДн имеет право:

– обрабатывать ПДн в соответствии с действующим законодательством Российской Федерации;

– поручить обработку ПДн другому лицу с согласия субъекта ПДн, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, в том числе государственного контракта, либо путем принятия соответствующего акта;

– мотивированно отказать субъекту ПДн в выполнении повторного запроса в целях получения сведений, касающихся обработки его ПДн, при нарушении субъектом ПДн своих обязанностей по подаче такого запроса;

– ограничить право субъекта ПДн на доступ к его ПДн в соответствии с федеральными законами, в т.ч. если обработка ПДн осуществляется в соответствии с законодательством о противодействии легализации доходов, полученных преступным путем, и финансированию терроризма;

– ограничить право субъекта ПДн на доступ к его ПДн в соответствии с федеральными законами, в т.ч. если доступ субъекта ПДн к его персональным данным нарушает права и законные интересы третьих лиц;

– самостоятельно определять состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных действующим законодательством в области ПДн, если иное не предусмотрено федеральными законами;

– осуществлять или обеспечивать блокирование или уничтожение ПДн, если обеспечить правомерность обработки ПДн невозможно;

– осуществлять или обеспечивать уничтожение ПДн;

– в случае достижения цели обработки ПДн продолжить обработку ПДн, если обработка ПДн осуществляется без согласия субъекта ПДн на основании пункта 4 статьи 21 Федерального закона от 27.07.2006 № 152-ФЗ;

– в случае отзыва субъектом ПДн согласия на обработку его ПДн продолжить обработку ПДн, если обработка ПДн осуществляется без согласия субъекта ПДн на основании пункта 5 статьи 21 Федерального закона от 27.07.2006 № 152-ФЗ;

– в случае отсутствия возможности уничтожения ПДн осуществить блокирование таких ПДн и обеспечить уничтожение ПДн в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами;

– осуществлять без уведомления уполномоченного органа по защите прав субъектов ПДн обработку ПДн, указанных в пункте 2 статьи 22 Федерального закона от 27.07.2006 № 152-ФЗ.

19.4. Обязанности Министерства при обработке ПДн субъектов ПДн

Министерство при обработке ПДн субъектов ПДн обязан:

– строго соблюдать принципы и правила обработки ПДн;

– в случае, если обработка ПДн осуществляется по поручению оператора, строго соблюдать и выполнять требования оператора;

– не раскрывать третьим лицам и не распространять ПДн без согласия субъекта ПДн, если иное не предусмотрено федеральным законом;

– по требованию субъекта ПДн либо по решению суда или иных уполномоченных государственных органов исключить из общедоступных источников ПДн сведения о субъекте ПДн;

– обеспечить конкретность и информированность согласия на обработку ПДн;

– получать согласие на обработку ПДн, если иное не предусмотрено действующим законодательством;

– в случае получения согласия на обработку ПДн от представителя субъекта ПДн проверять полномочия данного представителя на дачу согласия от имени субъекта ПДн;

– представить доказательство получения согласия субъекта ПДн на обработку его ПДн или доказательство наличия оснований обработки ПДн без получения согласия;

– строго соблюдать требования к содержанию согласия в письменной форме субъекта ПДн на обработку его ПДн;

– предоставить субъекту ПДн сведения по запросу субъекта ПДн в доступной форме, в которых не должны содержаться ПДн, относящиеся к другим субъектам ПДн, за исключением случаев, если имеются законные основания для раскрытия таких ПДн;

– мотивировать и представить доказательства обоснованности отказа в выполнении повторного запроса субъекта ПДн;

– разъяснить субъекту ПДн порядок принятия решения на обработку его ПДн и возможные юридические последствия такого решения, предоставить возможность заявить возражение против такого решения, а также разъяснить порядок защиты субъектом ПДн своих прав и законных интересов;

– предоставить субъекту ПДн по его просьбе информацию, касающуюся обработки его ПДн;

– разъяснить субъекту ПДн юридические последствия отказа предоставить его ПДн, если предоставление ПДн является обязательным в соответствии с федеральным законом;

– принимать меры, необходимые и достаточные для обеспечения выполнения своих обязанностей в области ПДн, если иное не предусмотрено федеральными законами;

– опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки ПДн, к сведениям о реализуемых требованиях к защите ПДн;

– по запросу уполномоченного органа по защите прав субъектов ПДн представить документы, определяющие политику в отношении обработки ПДн, и сведения о реализуемых требованиях к защите ПДн;

– принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн;

– сообщить субъекту ПДн или его представителю информацию о наличии ПДн, относящихся к соответствующему субъекту ПДн, а также предоставить возможность ознакомления с этими ПДн при обращении субъекта ПДн или его представителя, либо при получении запроса субъекта ПДн или его представителя;

– в случае отказа в предоставлении информации о наличии ПДн о соответствующем субъекте ПДн или ПДн субъекту ПДн, или его представителю при их обращении, либо при получении запроса субъекта ПДн или его представителя дать в письменной форме мотивированный ответ;

– предоставить безвозмездно субъекту ПДн или его представителю возможность ознакомления с ПДн, относящимися к этому субъекту ПДн;

– внести в ПДн необходимые изменения или уничтожить такие ПДн в случае предоставления субъектом ПДн или его представителем сведений, подтверждающих, что ПДн являются неполными, неточными или неактуальными;

– строго соблюдать сроки по уведомлениям, блокированию и уничтожению ПДн;

– уведомить субъекта ПДн или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым ПДн этого субъекта были переданы;

– сообщить в уполномоченный орган по защите прав субъектов ПДн по запросу этого органа необходимую информацию;

– в случае выявления неправомерной обработки ПДн при обращении субъекта ПДн или его представителя либо по запросу субъекта ПДн или его представителя, либо уполномоченного органа по защите прав субъектов ПДн оператор обязан осуществить блокирование неправомерно обрабатываемых ПДн, относящихся к этому субъекту ПДн, или обеспечить их блокирование (если обработка ПДн осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки;

– в случае выявления неточных ПДн при обращении субъекта ПДн или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов ПДн оператор обязан осуществить блокирование ПДн, относящихся к этому субъекту ПДн, или обеспечить их блокирование (если обработка ПДн осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки, если блокирование ПДн не нарушает права и законные интересы субъекта ПДн или третьих лиц;

– уточнить ПДн, либо обеспечить их уточнение (если обработка ПДн осуществляется другим лицом, действующим по поручению оператора) и снять блокирование ПДн в случае подтверждения факта неточности ПДн на основании сведений, представленных субъектом ПДн или его представителем либо уполномоченным органом по защите прав субъектов ПДн, или иных необходимых документов;

– прекратить неправомерную обработку ПДн или обеспечить прекращение неправомерной обработки ПДн лицом, действующим по поручению оператора в случае выявления неправомерной обработки ПДн, осуществляемой оператором или лицом, действующим по поручению оператора;

– уничтожить ПДн или обеспечить их уничтожение в случае, если обеспечить правомерность обработки ПДн невозможно;

– уведомить субъекта ПДн или его представителя, а в случае, если обращение субъекта ПДн или его представителя либо запрос уполномоченного органа по защите прав субъектов ПДн были направлены уполномоченным органом по защите прав субъектов ПДн, также указанный орган об устранении допущенных нарушений или об уничтожении ПДн;

– прекратить обработку ПДн или обеспечить ее прекращение (если обработка ПДн осуществляется другим лицом, действующим по поручению оператора) и уничтожить ПДн или обеспечить их уничтожение (если обработка ПДн осуществляется другим лицом, действующим по поручению оператора):

– в случае достижения цели обработки ПДн, если обработка ПДн осуществляется без согласия субъекта ПДн на основаниях, предусмотренных федеральным законом;

– в случае отзыва субъектом ПДн согласия на обработку его ПДн, если обработка ПДн осуществляется без согласия субъекта ПДн на основаниях, предусмотренных федеральным законом;

– уведомить уполномоченный орган по защите прав субъектов ПДн о своем намерении осуществлять обработку ПДн;

– уведомить уполномоченный орган по защите прав субъектов ПДн в случае изменения сведений, указанных в уведомлении о своем намерении осуществлять обработку ПДн;

– назначить лицо, ответственное за организацию обработки ПДн;

– предоставлять лицу, ответственному за организацию обработки ПДн, необходимые сведения;

– неукоснительно соблюдать все требования настоящих Правил;

– ознакомить государственных служащих (сотрудников) Министерства, непосредственно осуществляющих обработку ПДн, с положениями законодательства Российской Федерации о ПДн, в т.ч. требованиями к защите ПДн, документами, определяющими политику в отношении обработки ПДн, и организовать их обучение.

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

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

– реализация мер, направленных на обеспечение выполнения Министерства своих обязанностей;

– обеспечение личной ответственности государственных служащих (сотрудников) Министерства, осуществляющих обработку, либо доступ к ПДн;

– организация рассмотрения запросов субъектов ПДн или их представителей и ответов на такие запросы;

– организация внутреннего контроля соответствия обработки ПДн требованиям к защите ПДн, установленным действующим законодательством в области ПДн и правовыми актами Министерства;

– определение порядка доступа государственных служащих (сотрудников) Министерства в помещения, в которых ведется обработка ПДн;

– проведение необходимых мероприятий по обеспечению безопасности ПДн и носителей их содержащих;

– проведение периодических проверок условий обработки ПДн;

– блокирование, внесение изменений и уничтожение ПДн в предусмотренных действующим законодательством в области ПДн случаях;

– оповещение субъектов ПДн в предусмотренных действующим законодательством в области ПДн случаях;

– разъяснение прав субъекту ПДн в вопросах обработки и обеспечения безопасности их ПДн;

– оказание содействия правоохранительным органам в случаях нарушений законодательства в отношении обработки ПДн;

– публикация на официальном сайте Министерства документов и правовых актов, определяющих политику в отношении обработки ПДн.

21. Требования к государственным служащим (сотрудникам) Министерства земельных и имущественных отношений Республики Тыва, осуществляющим доступ к ПДн или их обработку

Министерство осуществляет ознакомление государственных служащих (сотрудников), непосредственно осуществляющих обработку ПДн или доступ к ним, с положениями законодательства Российской Федерации о ПДн (в т.ч. с требованиями к защите ПДн), правовых актов Министерства по вопросам обработки ПДн, включая настоящие Правила:

– при оформлении служебного контракта (трудового договора);

– при первоначальном допуске к обработке ПДн;

– при назначении на должность, связанную с обработкой ПДн или доступом к ним;

– после внесения изменений в действующее законодательство Российской Федерации о ПДн, правовые акты Министерства по вопросам обработки ПДн.

Государственные служащие (сотрудники) Министерства, непосредственно осуществляющие обработку ПДн или доступ к ним, обязаны:

– неукоснительно следовать принципам обработки ПДн;

– знать и строго соблюдать положения действующего законодательства Российской Федерации в области ПДн;

– знать и строго соблюдать положения правовых актов Министерства в области обработки и обеспечения безопасности ПДн;

– знать и строго соблюдать инструкции, руководства и иные эксплуатационные документы на применяемые средства автоматизации, в том числе программное обеспечение, и средства защиты информации;

– соблюдать конфиденциальность ПДн, не предоставлять третьим лицам и не распространять ПДн без согласия субъекта ПДн, если иное не предусмотрено федеральным законом;

– не допускать нарушений требований и правил обработки и обеспечения безопасности ПДн.

Государственные служащие (сотрудники) Министерства несут личную ответственность за соблюдение требований действующего законодательства Российской Федерации, настоящих Правил.

22. Обеспечение безопасности ПДн при их обработке

22.1. В соответствии с требованиями действующего законодательства в области ПДн при обработке ПДн Министерство обязано принимать необходимые правовые, организационные и технические меры для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения ПДн, а также от иных неправомерных действий.

Безопасность ПДн достигается путем исключения несанкционированного, в т.ч. случайного, доступа к ПДн, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение ПДн, а также иных несанкционированных действий.

22.2. Принципы обеспечения безопасности ПДн при их обработке

Обеспечение безопасности ПДн в Министерстве осуществляется на основе следующих принципов:

– соблюдение конфиденциальности ПДн;

– реализация права на доступ к ПДн лиц, доступ которых к таким данным разрешается в рамках действующего законодательства Российской Федерации и нормативными актами Министерства;

– обеспечение защиты информации, содержащей ПДн, от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

– проведение мероприятий, направленных на предотвращение несанкционированной передачи их лицам, не имеющим права доступа к такой информации;

– своевременное обнаружение фактов несанкционированного доступа к ПДн;

– недопущение воздействия на технические средства автоматизированной обработки ПДн, в результате которого может быть нарушено их функционирование;

– возможность незамедлительного восстановления ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

– постоянный контроль за обеспечением уровня защищенности ПДн;

– применение средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия требованиям безопасности ПДн.

22.3. Требования к уровню обеспечения безопасности

С целью установления методов и способов защиты информации, необходимых для обеспечения безопасности ПДн, определяется уровень защищенности ПДн в зависимости от объема обрабатываемых ими ПДн и угроз безопасности жизненно важным интересам личности, общества и государства.

Определение уровня защищенности ПДн проводится на этапе ее создания или в ходе эксплуатации (для ранее введенных в эксплуатацию и (или) модернизируемых информационных систем ПДн).

22.4. Состав мероприятий по обеспечению безопасности ПДн

Мероприятия по обеспечению безопасности ПДн в Министерстве носят комплексный характер и включают в себя организационные и технические меры, предусмотренные приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

22.5. Состав мероприятий по обеспечению безопасности ПДн при их обработке, осуществляемой без использования средств автоматизации

Обработка ПДн, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории ПДн можно было определить места хранения ПДн (материальных носителей) и установить перечень лиц, осуществляющих обработку ПДн, либо имеющих к ним доступ.

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

При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность ПДн и исключающие несанкционированный к ним доступ.

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

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

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

22.6. Состав мероприятий по обеспечению безопасности ПДн при их обработке, осуществляемой с использованием средств автоматизации

Мероприятия по обеспечению безопасности ПДн при их обработке в информационных системах персональных данных (далее – ИСПДн) включают в себя:

– определение угроз безопасности ПДн при их обработке, формирование на их основе модели угроз;

– разработку на основе модели угроз системы защиты ПДн, обеспечивающей нейтрализацию предполагаемых угроз;

– проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;

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

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

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

– учет лиц, допущенных к работе с ПДн;

– контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией.

Методами и способами защиты информации от несанкционированного доступа являются:

– реализация разрешительной системы допуска пользователей к информационным ресурсам, ИСПДн и связанным с ее использованием работам, документам;

– ограничение доступа пользователей в помещения, где размещены технические средства, позволяющие осуществлять обработку ПДн, а также хранятся носители информации;

– разграничение доступа пользователей к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;

– регистрация действий пользователей, контроль несанкционированного доступа и действий пользователей;

– учет и хранение съемных носителей информации, и их использование, исключающее хищение, подмену и уничтожение;

– резервирование технических средств, дублирование массивов и носителей информации;

– использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия;

– использование защищенных каналов связи;

– размещение технических средств, позволяющих осуществлять обработку ПДн, в пределах охраняемой территории;

– организация физической защиты помещений и собственно технических средств, позволяющих осуществлять обработку ПДн;

– предотвращение внедрения в ИСПДн вредоносных программ (программ-вирусов) и программных закладок.

В ИСПДн, имеющих подключение к информационно-телекоммуникационным сетям международного информационного обмена (сетям связи общего пользования) или при функционировании которых предусмотрено использование съемных носителей информации, используются средства антивирусной защиты.

При взаимодействии ИСПДн с информационно-телекоммуникационными сетями международного информационного обмена (сетями связи общего

пользования) основными методами и способами защиты информации от несанкционированного доступа являются:

– межсетевое экранирование с целью управления доступом, фильтрации сетевых пакетов и трансляции сетевых адресов для скрытия структуры информационной системы;

– обнаружение вторжений в информационную систему, нарушающих или создающих предпосылки к нарушению установленных требований по обеспечению безопасности ПДн;

– анализ защищенности информационных систем, предполагающий применение специализированных программных средств (сканеров безопасности);

– защита информации при ее передаче по каналам связи;

– использование смарт-карт, электронных замков и других носителей информации для надежной идентификации и аутентификации пользователей;

– использование средств антивирусной защиты.

Обмен ПДн при их обработке в ИСПДн осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и (или) путем применения технических средств, в том числе средств криптографической защиты информации.

23. Требования к помещениям, в которых производится обработка ПДн

Размещение оборудования ИСПДн, специального оборудования и охрана помещений, в которых ведется работа с ПДн, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей ПДн и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

Помещения, в которых располагаются технические средства ИСПДн или хранятся носители ПДн, должны соответствовать требованиям пожарной безопасности, установленным действующим законодательством Российской Федерации.

24. Мероприятия при возникновении обстоятельств непреодолимой силы (форс-мажор)

В случае обстоятельств непреодолимой силы, возникших в результате событий чрезвычайного характера, повлекших нарушения прав субъектов ПДн, Министерство освобождается от ответственности при наличии доказательств указанных выше обстоятельств.

В случае возникновения обстоятельств непреодолимой силы и нарушения прав субъектов ПДн, связанных с такими обстоятельствами, Министерство принимает все меры для извещения субъекта ПДн.

Приложение № 2

Утверждено
приказом Министерства
земельных и имущественных
отношений Республики Тыва
от 26.04.2021 г. № 16-од

Правила рассмотрения запросов субъектов персональных данных или их представителей

1. Общие положения

Настоящие Правила рассмотрения запросов субъектов персональных данных или их представителей (далее – Правила) регулируют отношения, возникающие при выполнении Министерства земельных и имущественных отношений Республики Тыва (далее – Оператор) обязательств согласно требованиям статей 14, 20 и 21 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ).

Положения настоящих Правил распространяются на действия оператора при получении запроса от юридических или физических лиц и их законных представителей (далее – субъект ПДн) и уполномоченного органа по защите прав субъектов персональных данных.

Эти действия направлены на определение порядка учета (регистрации), рассмотрение запросов, а также на подтверждение наличия, ознакомления, уточнения, уничтожения персональных данных (далее – ПДн) или отзыв согласия на обработку ПДн, а также на устранение нарушений законодательства, допущенных при обработке ПДн.

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

2. Организация и проведение работ Министерства земельных и имущественных отношений Республики Тыва по запросу ПДн

Субъект персональных данных имеет право на получение информации, касающейся обработки его ПДн в соответствии с частью 7 статьи 14 Федерального закона № 152-ФЗ.

Право субъекта персональных данных на доступ к его ПДн может быть ограничено в соответствии с частью 8 статьи 14 Федерального закона № 152-ФЗ.

Субъект ПДн вправе требовать от Министерства уточнения его ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными,

устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

Сведения, указанные в части 7 статьи 14 Федерального закона № 152-ФЗ, предоставляются субъекту ПДн Министерство при получении запроса от субъекта персональных данных.

Сведения, указанные в части 7 статьи 14 Федерального закона № 152-ФЗ, должны быть предоставлены субъекту ПДн в доступной форме и в них не должны содержаться ПДн, относящиеся к другим субъектам ПДн, за исключением случаев, если имеются законные основания для раскрытия таких ПДн.

Запрос субъекта ПДн должен содержать номер основного документа, удостоверяющего личность субъекта ПДн, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта ПДн в отношениях с Оператором, либо сведения, иным образом подтверждающие факт обработки ПДн Оператором, подпись субъекта ПДн. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

Рассмотрение запросов является служебной обязанностью должностных лиц Оператора, в чьи обязанности входит обработка ПДн.

Должностные лица Оператора обеспечивают:

– объективное, всестороннее и своевременное рассмотрения запроса;

– принятие мер, направленных на восстановление или защиту нарушенных прав, свобод и законных интересов субъектов ПДн;

– направление письменных ответов по существу запроса.

Все поступившие запросы регистрируются в день их поступления в журнале учета запросов граждан (субъектов персональных данных) по вопросам обработки ПДн.

В случае подачи субъектом ПДн повторного запроса, в целях получения сведений, указанных в части 7 статьи 14 Федерального закона № 152-ФЗ, необходимо руководствоваться частями 4 и 5 статьи 14 Федерального закона № 152-ФЗ. Повторный запрос наряду со сведениями, указанными выше, должен содержать обоснование направления повторного запроса.

Министерство вправе отказать субъекту ПДн в выполнении повторного запроса, не соответствующего условиям, предусмотренным частями 4 и 5 статьи 14 Федерального закона № 152-ФЗ.

Такой отказ должен быть мотивированным.

При рассмотрении запроса Министерство принимаются необходимые законные, обоснованные и мотивированные решения для обеспечения своевременного принятия решения по данному запросу.

Субъекту ПДн в письменной форме в установленный срок сообщается о решениях по запросу, со ссылками на законодательство Российской Федерации, а в случае отклонения запроса – разъясняется также порядок обжалования принятого решения.

Министерство обязан сообщить субъекту ПДн информацию о наличии ПДн, относящихся к соответствующему субъекту ПДн, а также предоставить

возможность ознакомления с этими ПДн при запросе субъекта ПДн либо в течение тридцати дней с даты получения запроса субъекта ПДн.

В случае отказа в предоставлении информации о наличии ПДн о соответствующем субъекте ПДн или ПДн субъекту ПДн при получении запроса субъекта ПДн Министерство обязано руководствоваться частью 2 статьи 20 Федерального закона № 152-ФЗ.

Министерство обязано:

предоставить безвозмездно субъекту ПДн возможность ознакомления с ПДн, относящимися к этому субъекту ПДн;

уведомить субъекта ПДн о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым ПДн этого субъекта были переданы.

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

Должностное лицо, назначенное руководителем Министерства, осуществляет непосредственный контроль за соблюдением установленного законодательством и настоящими Правилами порядка рассмотрения запросов.

3. Действия Министерства земельных и имущественных отношений Республики Тыва в ответ на запросы по ПДн

3.1. В случае поступления запроса субъекта ПДн по ПДн необходимо выполнить следующие действия:

а) при получении запроса субъекта ПДн на наличие ПДн необходимо в течение 30 дней с даты получения запроса (согласно части 1 статьи 20 Федерального закона № 152-ФЗ) подтвердить обработку ПДн в случае ее осуществления. Если обработка ПДн субъекта не ведется, то в течение 30 дней с даты получения запроса (согласно части 2 статьи 20 Федерального закона № 152-ФЗ) необходимо отправить уведомление об отказе в предоставлении информации о наличии ПДн.

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

– подтверждение факта обработки ПДн Министерства;

– правовые основания и цели обработки ПДн;

– цели и применяемые Министерством способы обработки ПДн;

– наименование и место нахождения Министерства, сведения о лицах (за исключением работников Министерства), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с Министерства или на основании Федерального закона № 152-ФЗ;

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

– сроки обработки ПДн, в том числе сроки их хранения;

– порядок осуществления субъектом ПДн прав, предусмотренных Федеральным законом № 152-ФЗ;

– информацию об осуществленной или предполагаемой трансграничной передаче данных;

– наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению Министерства, если обработка поручена или будет поручена такому лицу;

– иные сведения, предусмотренные Федеральным законом № 152-ФЗ или другими федеральными законами;

б) при получении запроса субъекта ПДн или его представителя на уточнение ПДн необходимо внести в них необходимые изменения в срок, не превышающий 7 рабочих дней со дня предоставления субъектом ПДн или его представителем сведений, подтверждающих, что ПДн являются неполными, неточными или неактуальными, по предоставлению субъектом ПДн или его представителем сведений, подтверждающих, что ПДн, которые относятся к соответствующему субъекту и обработку которых осуществляет Министерство, являются неполными, неточными или неактуальными (согласно части 3 статьи 20 Федерального закона № 152-ФЗ) и отправить уведомление о внесенных изменениях. Если обработка ПДн субъекта не ведется или не были предоставлены сведения, подтверждающие, что ПДн, которые относятся к соответствующему субъекту и обработку которых осуществляет Оператор, являются неполными, неточными или неактуальными, то необходимо в течение 30 дней с даты получения запроса отправить уведомление об отказе в осуществлении изменения ПДн;

в) при получении запроса субъекта ПДн на уничтожение ПДн необходимо их уничтожить в срок, не превышающий 7 рабочих дней со дня представления субъектом ПДн или его представителем сведений, подтверждающих, что такие ПДн являются незаконно полученными или не являются необходимыми для заявленной цели обработки (согласно части 3 статьи 20 Федерального закона № 152-ФЗ), и отправить уведомление об уничтожении. Если обработка ПДн субъекта не ведется или не были предоставлены сведения, подтверждающие, что ПДн, которые относятся к соответствующему субъекту и обработку которых осуществляет Министерство, являются незаконно полученными или не являются необходимыми для заявленной цели обработки, а также в силу необходимости обработки ПДн по требованиям иных законодательных актов, то необходимо в течение 30 дней с даты получения запроса отправить уведомление об отказе в уничтожении ПДн;

г) при получении запроса на отзыв согласия субъекта ПДн на обработку ПДн необходимо прекратить их обработку и, в случае, если сохранение ПДн более не требуется для целей обработки ПДн, уничтожить ПДн в срок, не превышающий 30 дней с даты поступления указанного отзыва (согласно части 5 статьи 21 Федерального закона № 152-ФЗ);

д) при выявлении недостоверности ПДн при обращении или по запросу субъекта персональных данных необходимо их блокировать с момента такого обращения или получения такого запроса на период проверки (согласно части 1 статьи 21 Федерального закона № 152-ФЗ). Если факт недостоверности ПДн подтвержден на основании сведений, представленных субъектом ПДн или его

представителем, либо уполномоченным органом по защите прав субъектов ПДн, или иных необходимых документов, необходимо уточнить ПДн в течение 7 рабочих дней со дня представления таких сведений и снять блокирование ПДн (согласно части 2 статьи 21 Федерального закона № 152-ФЗ). Если факт недостоверности ПДн не подтвержден, то необходимо отправить уведомление об отказе в изменении ПДн;

е) при выявлении неправомерных действий с ПДн Министерство по запросу субъекта персональных данных необходимо в срок, не превышающий 3 рабочих дней с даты этого выявления, прекратить неправомерную обработку ПДн (согласно части 3 статьи 21 Федерального закона № 152-ФЗ). В случае, если обеспечить правомерность обработки ПДн невозможно, Министерство в срок, не превышающий 10 рабочих дней с даты выявления неправомерной обработки ПДн (согласно части 3 статьи 21 Федерального закона № 152-ФЗ), обязан уничтожить такие ПДн.

При достижении целей обработки ПДн Министерство обязано незамедлительно прекратить обработку ПДн и уничтожить соответствующие ПДн в течение 30 дней с даты достижения цели обработки ПДн (согласно части 4 статьи 21 Федерального закона № 152-ФЗ), если иное не предусмотрено договором, стороной которого или поручителем по которому является субъект ПДн, иным соглашением между оператором и субъектом ПДн, либо если Оператор не вправе осуществлять обработку ПДн без согласия субъекта ПДн, если иное не предусмотрено действующим законодательством.

3.2. В случае поступления запроса уполномоченного органа по защите прав субъекта ПДн по ПДн необходимо выполнить следующие действия:

при получении запроса необходимо в течение 30 дней (согласно части 4 статьи 20 Федерального закона № 152-ФЗ) предоставить информацию, необходимую для осуществления деятельности указанного органа;

при выявлении недостоверных ПДн по запросу уполномоченного органа по защите прав субъекта ПДн необходимо их блокировать с момента такого обращения или получения такого запроса на период проверки (согласно части 1 статьи 21 Федерального закона № 152-ФЗ). Если факт недостоверности ПДн подтвержден на основании документов, предоставленных субъектом ПДн, необходимо в течение 7 рабочих дней уточнить ПДн и снять их блокирование (согласно части 2 статьи 21 Федерального закона № 152-ФЗ). Если факт недостоверности ПДн не подтвержден, то необходимо отправить уведомление об отказе изменения и снять блокирование ПДн;

при выявлении неправомерных действий Оператора с ПДн по запросу уполномоченного органа по защите прав субъекта ПДн необходимо прекратить неправомерную обработку ПДн в срок, не превышающий 3 рабочих дней с момента такого обращения или получения такого запроса на период проверки (согласно части 1 статьи 21 Федерального закона № 152-ФЗ). В случае невозможности обеспечения правомерности обработки Министерство в срок, не превышающий 10 рабочих дней с даты выявления неправомерности действий с ПДн, необходимо уничтожить ПДн и отправить уведомление об уничтожении ПДн.

4. Ответственность Министерства земельных и имущественных отношений Республики Тыва

Персональные данные не подлежат разглашению (распространению).

Прекращение доступа к такой информации не освобождает государственных служащих (сотрудников) Министерства от взятых им обязательств по неразглашению информации ограниченного доступа.

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

Приложение № 3

Утверждено
приказом Министерства
земельных и имущественных
отношений Республики Тыва
от 26.04.2021 г. № 16-од

Правила
осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных» в Министерстве земельных и имущественных отношений Республики Тыва

1. Общие положения

Настоящие Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в Министерстве земельных и имущественных отношений Республики Тыва (далее – Правила) разработаны в соответствии с требованиями 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».

В Правилах определен порядок организации и осуществления внутреннего контроля обработки персональных данных с целью своевременного выявления и предотвращения:

– хищения технических средств и носителей информации;

– утраты информации;

– преднамеренных программно-технических воздействий на информацию и (или) средства вычислительной техники, вызывающих нарушение целостности информации и нарушение работоспособности автоматизированной системы;

– несанкционированного доступа к ПДн с целью уничтожения, искажения, модификации (подделки), копирования и блокирования;

– утечки информации по техническим каналам.

Внутренний контроль состояния защиты информации включает в себя:

– контроль организации защиты информации;

– контроль эффективности защиты информации.

2. Порядок внутреннего контроля за соблюдением требований по обработке и обеспечению безопасности ПДн

В целях осуществления внутреннего контроля соответствия обработки ПДн установленным требованиям организуется проведение периодических проверок

условий обработки ПДн. Проверки осуществляются не реже одного раза в год в соответствии с утвержденным графиком.

При осуществлении внутреннего контроля соответствия обработки ПДн установленным требованиям производится проверка:

– соблюдения принципов обработки ПДн;

– соответствия правовых актов Министерства в области ПДн действующему законодательству Российской Федерации;

– выполнения государственными служащими (работниками) Министерства требований и правил обработки ПДн в информационных системах персональных данных (далее – ИСПДн);

– актуальности информации о законности целей обработки ПДн и оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности ПДн;

– правильности осуществления сбора, систематизации, записи, накопления, хранения, уточнения (обновления, изменения), извлечения, использования, передачи (распространения, предоставления, доступа), обезличивания, блокирования, удаления, уничтожения ПДн в каждой ИСПДн;

– актуальности перечня должностей должностных лиц, уполномоченных на обработку ПДн, имеющих доступ к ПДн;

– соблюдения прав субъектов персональных данных, чьи ПДн обрабатываются в ИСПДн;

– соблюдения обязанностей оператора ПДн, предусмотренных действующим законодательством в области ПДн;

– порядка взаимодействия с субъектами персональных данных, ПДн которых обрабатываются в ИСПДн, в том числе соблюдения сроков, предусмотренных действующим законодательством в области ПДн, соблюдения требований по уведомлениям, порядка разъяснения субъектам персональных данных необходимой информации, порядка реагирования на обращения (запросы) субъектов персональных данных, порядка действий при достижении целей обработки ПДн и отзыве согласий субъектами персональных данных;

– наличия необходимых согласий субъектов персональных данных, чьи ПДн обрабатываются в ИСПДн;

– актуальности сведений, содержащихся в уведомлении об обработке (о намерении осуществлять обработку) персональных данных;

– актуальности перечня ИСПДн;

– знания и соблюдения государственными служащими (работниками) Министерства положений действующего законодательства Российской Федерации в области ПДн, правовых актов Министерства;

– соблюдения государственными служащими (работниками) Министерства конфиденциальности ПДн;

– соблюдения государственными служащими (работниками) требований по обеспечению безопасности ПДн;

– наличия и актуальности локальных актов, технической и эксплуатационной документации технических и программных средств ИСПДн.

О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, лицо, ответственное за проведение проверки, докладывает руководителю Министерства (заместитель министра).

При проведении внутреннего контроля на ИСПДн составляется протокол контроля выполнения требований по обеспечению безопасности информации, содержащей сведения ограниченного доступа, при ее автоматизированной обработке на автоматизированном рабочем месте по форме, приведенной в приложении к настоящим Правилам.

3. Оценка соотношения вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности ПДн

Во время осуществления внутреннего контроля соответствия обработки ПДн установленным требованиям производится соответствие оценки соотношения вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности ПДн и принимаемых мер по обработке и обеспечению безопасности ПДн в Министерстве.

При оценке соотношения вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности ПДн, для каждой ИСПДн производится экспертное сравнение заявленной оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности ПДн и применяемых мер, направленных на обеспечение выполнения обязанностей, предусмотренных действующим законодательством в области ПДн и изложенных в настоящих Правилах осуществления внутреннего контроля соответствия обработки ПДн.

Оценка соотношения вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности ПДн и принимаемых мер по обработке и обеспечению безопасности ПДн, оформляется в виде отдельного документа, подписывается руководителем структурного подразделения Министерства (либо его заместителем) и утверждается руководителем Министром.

Приложение
к Правилам осуществления внутреннего контроля
соответствия обработки персональных данных
требованиям к защите персональных данных

Протокол № ___
контроля выполнения требований по обеспечению безопасности информации, содержащей сведения ограниченного доступа, при ее автоматизированной обработке в ИС Министерстве земельных и имущественных отношений Республики Тыва

1. Объект контроля:

наименование автоматизированного рабочего места (далее – АРМ);

заводской (инвентарный) номер системного блока персональной электронно-вычислительной машины АРМ;

адрес размещения АРМ.

2. Назначение объекта:

тип информации, обрабатываемой (хранимой) на АРМ;

уровень защищенности персональных данных при их обработке в информационной системе.

3. Контролируемые вопросы:

– состояние организации технической защиты информации при обработке (хранении) информации ограниченного доступа;

– контроль наличия руководящих документов, инструкций, документации, регламентирующей обработку (хранение) информации ограниченного доступа;

– перечень защищаемых ресурсов и уровня их конфиденциальности;

– перечень лиц, обслуживающих АРМ;

– перечень лиц, имеющих право самостоятельного доступа в помещение с АРМ;

– перечень лиц, имеющих право самостоятельного доступа к штатным средствам АРМ и уровень их полномочий;

– распоряжение о назначении администратора информационной безопасности;

– данные по уровню подготовки персонала;

– инструкции по обеспечению защиты информации, обрабатываемой на АРМ;

– перечень программного обеспечения;

– описание технологического процесса обработки информации;

– схемы информационных потоков;

– технический паспорт;

– матрицы доступа субъектов к защищаемым информационным ресурсам;

– акт установки системы активного зашумления (при наличии);

– акт установки системы защиты информации от несанкционированного доступа (далее – СЗИ НСД) (при наличии);

– описание системы разграничения доступа и настроек СЗИ НСД;

– инструкции администратора безопасности;

– инструкции пользователя;

– инструкции по антивирусному контролю;

– распоряжения о допуске государственных служащих (сотрудников) Министерства;

– распоряжение о вводе в эксплуатацию.

Контроль соответствия настройки СЗИ НСД требованиям присвоенного уровня защищенности ПДн.

При контроле следует руководствоваться требованиями следующих документов:

– постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

– приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

4. Метод проведения контроля: экспертно-документальный.

5. Средства контроля: программные возможности операционной системы, установленной на контролируемом АРМ.

6. Перечень документов, регламентирующих выполнение требований по обеспечению безопасности информации.

Контроль проводится в соответствии с требованиями:

– указа Президента Российской Федерации от 17.03.2008 № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»;

– постановления Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– приказа ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

– приказа ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

Контроль выполнил:

_____	_____	_____
должность	подпись	фамилия, инициалы

При проведении контроля присутствовали:

_____	_____	_____
должность	подпись	фамилия, инициалы
_____	_____	_____
должность	подпись	фамилия, инициалы

Дата проведения контроля: _____.

(число, месяц, год)

Приложение № 4

Утверждено
приказом Министерства
земельных и имущественных
отношений Республики Тыва
от 26.04.2021 г. № 16-од

Правила работы с обезличенными персональными данными в Министерстве земельных и имущественных отношений Республики Тыва

1. Общие положения

Настоящие Правила работы с обезличенными персональными данными в Министерстве земельных и имущественных отношений Республики Тыва (далее – Правила) разработаны с учетом требований 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».

2. Условия обезличивания

Обезличивание персональных данных (далее – ПДн) проводится с целью снижения ущерба от разглашения защищаемых ПДн и снижения требований к защите информационной системы персональных данных (далее – ИСПДн).

Обезличивание персональных данных также осуществляется по достижению целей обработки ПДн или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено Федеральным законом.

Способы обезличивания при условии дальнейшей обработки ПДн:

уменьшение перечня обрабатываемых сведений;

замена части сведений идентификаторами;

замена численных значений минимальным, средним или максимальным значением;

деление сведений на части и обработка их в разных информационных системах и другие способы.

Для обезличивания ПДн применяются любые способы явно не запрещенные законодательно.

Руководители подразделений Министерства, непосредственно осуществляющих обработку ПДн, готовят предложения по обезличиванию ПДн, обоснование такой необходимости и определяют способ обезличивания.

3. Порядок работы с обезличенными персональными данными

Обезличенные персональные данные не подлежат разглашению и нарушению конфиденциальности.

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

При обработке обезличенных ПДн с использованием средств автоматизации необходимо соблюдение:

парольной политики;

антивирусной политики;

правил работы со съемными носителями;

правил резервного копирования;

правил доступа в помещения, где расположены элементы информационных систем.

При обработке обезличенных ПДн без использования средств автоматизации необходимо соблюдение:

правил хранения бумажных носителей;

правил доступа к ним и в помещения, где они хранятся.

Приложение № 5

Утверждено
приказом Министерства
земельных и имущественных
отношений Республики Тыва
от 26.04.2021 г. № 16-од

Типовое обязательство
государственного служащего (сотрудника) Министерства земельных и имущественных отношений Республики Тыва, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним трудового договора прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей

Обязательство о соблюдении конфиденциальности персональных данных

Я, _____,
(фамилия, имя, отчество, должность)

непосредственно осуществляя обработку персональных данных при выполнении своих должностных обязанностей, ознакомлен (а) с требованиями по соблюдению конфиденциальности обрабатываемых мною персональных данных субъектов персональных данных и обязуюсь в случае расторжения со мной трудового договора прекратить обработку персональных данных, ставших мне известными в связи с исполнением должностных обязанностей.

Я ознакомлен (а) с предусмотренной действующим законодательством Российской Федерации ответственностью за нарушения неприкосновенности частной жизни и установленного порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных).

_____
(фамилия, имя, отчество)

_____
(паспортные данные)

_____
(подпись)

_____
(дата)

Приложение № 6

Утверждено
приказом Министерства
земельных и имущественных
отношений Республики Тыва
от 26.04.2021 г. № 16-од

Типовая форма разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные

Уважаемый _____!
(Ф.И.О)

В соответствии с требованиями Федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных» уведомляем Вас, что обязанность предоставления Вами персональных данных установлена

_____
(пункт, статья, часть)

Федерального закона _____,
(реквизиты и наименование)

а также следующими нормативными актами _____

_____
(указываются реквизиты и наименования таких нормативных актов)

В случае отказа Вами предоставить свои персональные данные Министерство земельных и имущественных отношений Республики Тыва не сможет на законных основаниях осуществлять обработку Ваших персональных данных, что приведет к следующим для Вас юридическим последствиям

_____
(перечислить юридические последствия для субъекта персональных данных)

В соответствии с действующим законодательством Российской Федерации в области персональных данных Вы имеете право:

– на получение сведений о Министерстве земельных и имущественных отношений Республики Тыва как операторе, осуществляющем обработку Ваших персональных данных (в объеме, необходимом для защиты своих прав и законных интересов по вопросам обработки своих персональных данных), о месте нахождения Министерства, о наличии у оператора своих персональных данных, а также на ознакомление с такими персональными данными;

– подавать запрос на доступ к своим персональным данным;

– требовать безвозмездного предоставления возможности ознакомления со своими персональными данными, а также внесения в них необходимых

изменений, их уничтожения или блокирования при предоставлении сведений, подтверждающих, что такие персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки;

– получать уведомления по вопросам обработки персональных данных в установленных действующим законодательством Российской Федерации случаях и сроки;

– требовать от оператора разъяснения порядка защиты субъектом персональных данных своих прав и законных интересов;

– обжаловать действия или бездействие оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке;

– на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

_____

(фамилия, имя, отчество)

_____

(паспортные данные)

_____

(подпись)

_____

(дата)

Приложение № 7

Утверждено
приказом Министерства
земельных и имущественных
отношений Республики Тыва
от 26.04.2021 г. № 16-од

ПОРЯДОК ДОСТУПА СЛУЖАЩИХ МИНИСТЕРСТВА ЗЕМЕЛЬНЫХ И ИМУЩЕСТВЕННЫХ ОТНОШЕНИЙ РЕСПУБЛИКИ ТЫВА В ПОМЕЩЕНИЯ, В КОТОРЫХ ВЕДЕТСЯ ОБРАБОТКА ПЕРСОНАЛЬНЫХДАННЫХ

1. Общие положения

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

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

Объектами охраны Министерства земельных и имущественных отношений республики Тыва (далее по тексту - Министерство) являются:

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

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

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

Бесконтрольный доступ посторонних лиц в указанные помещения исключен.

Посторонними лицами считаются работники Министерства, не допущенные к обработке персональных данных и лица, не являющиеся работниками Министерства.

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

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

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

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

Например: металлические решетки на окнах, металлическая дверь, система контроляи управления доступа и так далее.

2. Правила доступа в помещения, в которых ведется обработка персональныхданных

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

При этом должны быть приняты меры, исключающие ознакомление посторонних лиц

с персональными данными. Пример: мониторы повернуты в сторону от посетителей, документы убраны в стол, либо находятся в непрозрачной папке (накрыты чистыми листами бумаги).

При возникновении чрезвычайных ситуаций природного и техногенного характера,

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

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

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

Правила доступа в серверные помещения

Доступ в серверные помещения, в которых ведется обработка персональных данных, осуществляется в соответствии со списком, утвержденным в Министерстве.

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

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

Нахождение в серверных помещениях посторонних лиц без сопровождающего запрещено.

При возникновении чрезвычайных ситуаций природного и техногенного характера,

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

Доступ работников в серверные помещения в нерабочее время допускается по распоряжению руководства Министерства.

Правила доступа в спецпомещения

Спецпомещения выделяют с учетом размеров контролируемых зон, регламентированных эксплуатационной и технической документацией к средствам криптографической защиты информации (далее - СКЗИ). Помещения должны иметь прочные входные двери с замками, гарантирующими надежное закрытие помещений в нерабочее время. Окна помещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц й других мест, откуда возможно проникновение в спецпомещения посторонних лиц, необходимо оборудовать металлическими решетками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в спецпомещения.

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

Для предотвращения просмотра извне спецпомещений их окна должны быть защищены.

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

Доступ в спецпомещения осуществляется в соответствии с перечнем лиц, имеющих право доступа в помещения, где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ, утвержденным приказом министра.

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

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

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

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

Доступ работников в спецпомещения в нерабочее время допускается на основании служебных записок (или иных видов разрешающих документов), подписанных руководителем Министерства.

Нахождение в спецпомещениях посторонних лиц в нерабочее время запрещается.

Приложение
к Порядку доступа
государственных служащих (сотрудников) в
помещения Министерства, в которых ведется
обработка конфиденциальной информации, в
том числе персональных данных, в рабочее и
нерабочее время, а также в нештатных
ситуациях

Перечень должностей лиц, допущенных (имеющих доступ) в помещения, в которых ведется обработка конфиденциальной информации, в том числе персональных данных

№ п/п	Должность	Подразделение
ИС «Кадры»		
1.	Начальник отдела	Отдел бюджетного учета, делопроизводства, правового и кадрового обеспечения
ИС «Бухгалтерия»		
2.	Консультант (бухгалтер)	Отдел бюджетного учета, делопроизводства, правового и кадрового обеспечения
ИС «Обращения граждан»		
3.	Министр	
4.	Заместитель министра - 2	
5.	Начальник отдела – 1 Консультант – 1 Главный специалист – 1 Специалист ГПХ - 3	Отдел управления не разграниченными землями г.Кызыла Отдел
6.	Начальник отдела – 1 Консультант – 1 Главный специалист – 1	Отдел управления республиканскими землями
7.	Начальник отдела – 1 Консультант – 1 Главный специалист – 1	Отдел управления республиканским имуществом
8.	Заведующий сектором – 1 Консультант – 1	Сектор анализа и контроля государственными унитарными предприятиями, корпоративного управления акционерными обществами
9.	Консультант – 1	Отдел бюджетного учета, делопроизводства, правового и кадрового обеспечения
ИС «Документы»		
10.	Министр	
11.	Заместитель министра - 2	

12.	Начальник отдела – 1 Консультант – 1 Главный специалист – 1 Специалист ГПХ - 3	Отдел управления не разграниченными землями г.Кызыла
13.	Начальник отдела – 1 Консультант – 1 Главный специалист – 1	Отдел управления республиканскими землями
14.	Начальник отдела – 1 Консультант – 1 Главный специалист – 1	Отдел управления республиканским имуществом
15.	Заведующий сектором – 1 Консультант – 1	Сектор анализа и контроля государственными унитарными предприятиями, корпоративного управления акционерными обществами
16.	Начальник отдела – 1 Консультант – 1 Главный специалист – 1	Отдел бюджетного учета, делопроизводства, правового и кадрового обеспечения
АСГОР		
17.	Начальник отдела – 1 Консультант – 1 Главный специалист – 1 Специалист ГПХ - 3	Отдел управления не разграниченными землями г.Кызыла
18.	Начальник отдела – 1 Консультант – 1 Главный специалист – 1	Отдел управления республиканскими землями
19.	Начальник отдела – 1 Консультант – 1 Главный специалист – 1	Отдел управления республиканским имуществом
20.	Заведующий сектором – 1 Консультант – 1	Сектор анализа и контроля государственными унитарными предприятиями, корпоративного управления акционерными обществами
Технокад		
21.	Заместитель министра - 1	
22.	Начальник отдела – 1 Консультант – 1 Главный специалист – 1 Специалист ГПХ - 3	Отдел управления не разграниченными землями г.Кызыла
23.	Консультант – 1	Отдел управления республиканским имуществом

Приложение № 8

Утверждено
приказом Министерства
земельных и имущественных
отношений Республики Тыва
от 26.04.2021 г. № 16-од

Типовая форма обязательства о неразглашении персональных данных в Министерстве земельных и имущественных отношений Республики Тыва

ОБЯЗАТЕЛЬСТВО
о неразглашении конфиденциальной информации (персональных данных), не содержащих сведений, составляющих государственную тайну

Я,_____
(ФИО государственного гражданского служащего)
_____,

исполняющий(ая) должностные обязанности по занимаемой должности: _____

_____
(должность, наименование структурного подразделения организации)
_____

предупрежден(а), что на период исполнения должностных обязанностей в соответствии с должностным регламентом, мне будет предоставлен допуск к конфиденциальной информации (персональным данным), не содержащим сведений, составляющих государственную тайну. Настоящим добровольно принимаю на себя обязательства:

1. Не разглашать третьим лицам конфиденциальные сведения, которые мне доверены (будут доверены) или станут известными в связи с выполнением должностных обязанностей.
2. Не передавать и не раскрывать третьим лицам конфиденциальные сведения, которые мне доверены (будут доверены) или станут известными в связи с выполнением должностных обязанностей.
3. В случае попытки третьих лиц получить от меня конфиденциальные сведения, сообщать непосредственному руководителю.
4. Не использовать конфиденциальные сведения с целью получения выгоды.
5. Выполнять требования нормативных правовых актов, регламентирующих вопросы защиты конфиденциальных сведений.
6. В течение года после прекращения права на допуск к конфиденциальным сведениям не разглашать и не передавать третьим лицам известные мне конфиденциальные сведения.

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

_____ /_____/

«_ __ _» _____ 20___ г.

Приложение № 9

Утверждено
приказом Министерства
земельных и имущественных
отношений Республики Тыва
от 26.04.2021 г. № 16-од

Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации в Министерстве земельных и имущественных отношений Республики Тыва

1. Общие положения

1.1. Положение об особенностях обработки персональных данных без использования средств автоматизации (далее — Положение) определяет особенности и порядок обработки персональных данных при их обработке без использования средств автоматизации в *Министерстве земельных и имущественных отношений Республики Тыва* (далее — Оператор).

1.2. Положение разработано во исполнение Политики в отношении обработки персональных данных и в соответствии с Федеральным законом от 27.06.2006 г. № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации».

1.3. Настоящее Положение направлено на обеспечение безопасности персональных данных от несанкционированного доступа, их неправомерного использования или их утраты при обработке персональных данных в Министерстве без использования средств автоматизации

1.4. Все сотрудники Оператора, непосредственно осуществляющие обработку персональных данных без использования средств автоматизации, должны быть ознакомлены с настоящим Положением под роспись.

2. Особенности и порядок обработки

2.1. Обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

2.2. Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на разных материальных носителях

персональных данных, в специальных разделах или на полях форм (бланков).

2.3. Оператор обеспечивает раздельное хранение персональных данных на разных материальных носителях, обработка которых осуществляется в различных целях.

2.4. Для обработки каждой категории персональных данных используется отдельный материальный носитель.

2.5. При необходимости уничтожение или обезличивание части персональных данных, производится способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на том же материальном носителе (удаление, вымарывание).

2.6. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее – типовая форма), соблюдаются условия:

– типовая форма или связанные с ней документы содержат сведения о цели обработки персональных данных, наименование и адрес Оператора, 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;

– типовая форма предусматривает поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, при необходимости получения такого согласия;

– типовая форма составлена таким образом, что каждый из субъектов персональных данных, содержащихся в документе, имеет возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;

– типовая форма исключает объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

Перечень типовых форм, использующихся Оператором, приведён в Приложении 1.

2.7. Сотрудники Оператора, осуществляющие обработку персональных данных без использования средств автоматизации, информируются о факте такой обработки, об особенностях и правилах.

2.8. Оператор принимает организационные и физические меры, обеспечивающие сохранность материальных носителей персональных данных и исключающие возможность несанкционированного доступа к ним.

2.9. Во избежание несанкционированного доступа к персональным данным Оператор оборудует отдельное помещение, либо помещение, где хранятся документы и внешние электронные носители информации, содержащие персональные данные, в сейфах, металлических шкафах или в запираемых шкафах.

2.10. Перечень лиц, имеющих доступ к персональным данным,

обрабатываемым без использования средств автоматизации, в помещения и к местам хранения носителей, ограничен сотрудниками, работающими в указанных помещениях на постоянной основе. Исключена возможность доступа в помещения, где обрабатываются персональные данные без использования средств автоматизации, посторонних лиц без сопровождения допущенного сотрудника.

2.11. Работа с материальными носителями, содержащими персональные данные, организовывается следующим образом. Материальные носители могут находиться на рабочем месте сотрудника в течение времени, необходимого для обработки персональных данных, но не более одного рабочего дня. При этом должна быть исключена возможность просмотра персональных данных посторонними лицами. В конце рабочего дня все материальные носители, содержащие персональные данные, должны быть убраны в запираемые шкафы (в сейфы, если таковые имеются в подразделении). Черновики и редакции документов, испорченные бланки, листы со служебными записями в конце рабочего дня уничтожаются.

2.12. Передача материальных носителей, содержащий персональные данные, любым лицам без письменного согласия субъекта персональных данных, за исключением случаев, когда это необходимо в целях, предусмотренных федеральными законами и иными нормативными правовыми актами Российской Федерации, запрещена.

2.13. В случае достижения цели обработки персональных данных или отзыва субъектом персональных данных согласия на обработку его персональных данных обработка персональных данных должна прекратиться и такие данные должны быть уничтожены в срок, не превышающий 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 настоящим Федеральным законом или другими федеральными законами.

2.14. В случае отсутствия возможности уничтожения персональных данных в указанный срок, должно быть осуществлено блокирование таких персональных данных и уничтожение персональных данные в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

3. Ответственность

3.1. Все сотрудники Оператора, допущенные к обработке персональных данных без использования средств автоматизации, несут административную, материальную, уголовную ответственность в соответствии с действующим законодательством за обеспечение сохранности и соблюдение правил работы с персональными данными.

3.2. Ответственность за доведение требований настоящего Положения до сотрудников Оператора несёт ответственный за организацию обработки персональных данных.

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

Приложение № 10

Утверждено
приказом Министерства
земельных и имущественных
отношений Республики Тыва
от 26.04.2021 г. № 16-од

Типовая форма
согласия на обработку персональных данных
субъекта персональных данных

_____
(фамилия, имя, отчество субъекта персональных данных
_____
(или представителя субъекта персональных данных))
_____
(адрес субъекта персональных данных (его представителя)
_____
(номер основного документа, удостоверяющего личность,
_____
сведения о дате выдачи указанного документа
_____
и выдавшем его органе),
_____
(реквизиты доверенности или иного документа,
_____
подтверждающего полномочия представителя субъекта
_____
персональных данных)

Я даю письменное согласие на обработку своих персональных данных свободно, своей волей и в своем интересе

_____
(наименование оператора, получающего согласие субъекта персональных данных)

_____
(адрес оператора, получающего согласие субъекта персональных данных)

с целью _____
(цель обработки персональных данных)

на обработку персональных данных _____

(перечень персональных данных, на обработку которых

_____

дается согласие субъекта персональных данных)

обработка персональных данных поручается _____
(наименование или фамилию, имя, отчество,

_____

адрес лица, осуществляющего обработку персональных данных по поручению

_____

оператора (указать наименование оператора), если обработка будет поручена такому лицу)

с персональными данными будут совершаться следующие действия _____
(перечень действий

_____

с персональными данными, на совершение которых дается согласие)

персональные данные будут обрабатываться с использованием способов _____
(общее описание

_____

используемых оператором (указать наименование оператора) способов обработки

_____

персональных данных)

настоящее согласие на обработку персональных данных действует в течение срока _____
(срок,

_____

в течение которого действует согласие субъекта персональных данных)

настоящее согласие на обработку персональных данных может быть отозвано мною _____
(способ

_____

отзыва согласия на обработку персональных данных, если иное не установлено федеральным законом)

_____

(подпись субъекта персональных данных или его представителя) (расшифровка подписи)

«____»_____20___г.

Приложение № 11

Утверждено
приказом Министерства
земельных и имущественных
отношений Республики Тыва
от 26.04.2021 г. № 16-од

ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ МИНИСТЕРСТВА ЗЕМЕЛЬНЫХ И ИМУЩЕСТВЕННЫХ ОТНОШЕНИЙ РЕСПУБЛИКИ ТЫВА

№	Наименование (сегмент) ИСПДн/ГИС	Категория ИСПДн/ степень возможного ущерба	Уровень защищенности персональных данных/класс защищенности	Использование СКЗИ для обеспечения безопасности персональных данных
1	2	3	4	5
1	УРМ АС «Бюджет»	ИСПДн-И	четвертый	Используются
2	Сегмент ГИС «КП ССТУ»	ИСПДн-И/низкая	четвертый/К3	Используются
3	Сегмент ГИС СЭД «Обращения граждан»	ИСПДн-И/низкая	четвертый/К3	Используются
4	Смарт Роут	ИСПДн-И/низкая	четвертый/К3	Используются
5	«1С Предприятие: Бухгалтерия государственного учреждения»	ИСПДн-И	четвертый	Не используются
6	СУФД	ИСПДн-И	четвертый	Используются
7	Сегмент ГИС «Единая межведомственная система электронного документооборота»	ИСПДн-И/низкая	четвертый/К3	Используются
8	ФСС «Больничные листы»	ИСПДн-И	четвертый	Используются
9	АСГОР	ИСПДн-И	четвертый/К3	Не используются
10	ТехноКад	ИСПДн-И	четвертый/К3	Используются
11	СБИС	ИСПДн-И	четвертый/К3	Не используются

Приложение № 12

Утверждено
приказом Министерства
земельных и имущественных
отношений Республики Тыва
от 26.04.2021 г. № 16-од

ПЕРЕЧЕНЬ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОБРАБАТЫВАЕМЫХ В МИНИСТЕРСТВЕ ЗЕМЕЛЬНЫХ И ИМУЩЕСТВЕННЫХ ОТНОШЕНИЙ РЕСПУБЛИКИ ТЫВА В СВЯЗИ С РЕАЛИЗАЦИЕЙ ТРУДОВЫХ (СЛУЖЕБНЫХ) ОТНОШЕНИЙ

Номер страхового свидетельства обязательного пенсионного страхования.

Идентификационный номер налогоплательщика.

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

1. Прежние фамилия, имя, отчество, дата, место и причина изменения (в случае изменения).
2. Владение иностранными языками и языками народов Российской Федерации.
3. Образование (когда и какие образовательные учреждения закончил, номера дипломов, направление подготовки или специальность по диплому, квалификация по диплому).
4. Послевузовское профессиональное образование (наименование образовательного или научного учреждения, год окончания), ученая степень, ученое звание (когда присвоены, номера дипломов, аттестатов).
5. Выполняемая работа с начала трудовой деятельности (включая военную службу, работу по совместительству, предпринимательскую деятельность).
6. Классный чин федеральной государственной гражданской службы, гражданской службы субъекта Российской Федерации, муниципальной службы, дипломатический ранг, воинское, специальное звание, классный чин правоохранительной службы (кем и когда присвоены).
7. Государственные награды, иные награды и знаки отличия (кем награжден и когда).
8. Степень родства, фамилии, имена, отчества, даты рождения близких родственников (отца, матери, братьев, сестер и детей), а также мужа (жены).
9. Места рождения, места работы и домашние адреса близких родственников (отца, матери, братьев, сестер и детей), а также мужа (жены).
10. Пребывание за границей (когда, где, с какой целью).
11. Фамилии, имена, отчества, даты рождения, места рождения, места работы и домашние адреса бывших мужей (жен).
12. Близкие родственники (отец, мать, братья, сестры и дети), а также муж

(жена), в том числе бывшие, постоянно проживающие за границей и (или) оформляющие документы для выезда на постоянное место жительства в другое государство (фамилия, имя, отчество, с какого времени проживают за границей).

13. Адрес регистрации и фактического проживания.

14. Дата регистрации по месту жительства.

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

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

17. Номер телефона.

18. Отношение к воинской обязанности, сведения по воинскому учету(лиц пребывающих в запасе, и лиц, подлежащих призыву на военную службу).

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

20. Наличие (отсутствие) заболевания, препятствующего поступлению на государственную гражданскую службу Российской Федерации или ее прохождению, подтвержденного заключением медицинского учреждения.

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

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

23. Сведения о последнем месте государственной или муниципальной службы.

24. Фотография.

25. Реквизиты банковских счетов.

26. Сведения о наличии (отсутствии) судимости.

Приложение № 13

Утверждено
приказом Министерства
земельных и имущественных
отношений Республики Тыва
от 26.04.2021 г. № 16-од

**Перечень персональных данных,
обрабатываемых в Министерстве земельных и имущественных отношений Республики Тыва в связи с оказанием государственных услуг
и осуществлением государственных функций**

1. Фамилия, имя, отчество (последнее - при наличии) (в том числе прежние фамилии, имена и отчества (последнее - при наличии) в случае их изменения, сведения о том, когда, где и по какой причине они изменялись).
2. Дата рождения (число, месяц и год рождения).
3. Место рождения.
4. Вид, серия, номер основного документа, удостоверяющего личность гражданина Российской Федерации, наименование органа и код подразделения органа (при наличии), выдавшего его, дата выдачи.
9. Адрес и дата регистрации по месту жительства (пребывания).
10. Адрес фактического проживания (нахождения).
11. Номера телефонов (домашнего, служебного, мобильного).
12. Почтовый адрес и адрес электронной почты.
13. Сведения о семейном положении, о составе семьи.
14. Сведения, содержащиеся в свидетельствах о государственной регистрации актов гражданского состояния.

Приложение № 14

Утверждено
приказом Министерства
земельных и имущественных
отношений Республики Тыва
от 26.04.2021 г. № 16-од

Перечень
должностей государственных гражданских служащих (служащих) Министерства земельных и имущественных отношений Республики Тыва, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных

Министр

Заместитель министра – 2

Начальник отдела бюджетного учета, делопроизводства, правового и кадрового обеспечения

Консультант отдела бюджетного учета, делопроизводства, правового и кадрового обеспечения (бухгалтер)

Начальник отдела управления республиканскими землями

Начальник отдела управления республиканским имущество

Начальник отдела управления не разграниченными землями г.Кызыла

Заведующий сектором анализа и контроля государственных унитарных предприятий, корпоративного управления акционерных обществ

Приложение № 15

Утверждено
приказом Министерства
земельных и имущественных
отношений Республики Тыва
от 26.04.2021 г. № 16-од

Перечень должностей государственных гражданских (служащих) Министерства земельных и имущественных отношений Республики Тыва, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным

Министр
Заместитель министра – 2

Отдел бюджетного учета, делопроизводства, правового и кадрового обеспечения
Начальник отдела
Консультант - 2

Отдел управления республиканскими землями
Начальник отдела
Консультант – 1
Главный специалист - 1

Отдел управления республиканским имуществом
Начальник отдела
Консультант - 1
Главный специалист

Отдел управления не разграниченными землями г.Кызыла
Начальник отдела
Консультант - 1
Главный специалист – 1
Специалист по обработке документов - 3

Сектор анализа и контроля государственных унитарных предприятий, корпоративного управления акционерных обществ
Заведующий сектором
Консультант – 1

Приложение № 16

Утверждено
приказом Министерства
земельных и имущественных
отношений Республики Тыва
от 26.04.2021 г. № 16-од

Инструкция
лица, ответственного за организацию обработки и защиты персональных данных, обрабатываемых в информационных системах Министерства земельных и имущественных отношениях Республики Тыва

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Должностная инструкция ответственного за организацию обработки и защиты персональных данных (далее - Инструкция) разработана в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» и другими нормативными правовыми актами.

1.2. Инструкция определяет ответственность, обязанности и права лица, назначенного ответственным за организацию обработки и защиты персональных данных, обрабатываемых в государственных информационных системах Министерства.

1.3. Ответственный за организацию обработки персональных данных отвечает за осуществление внутреннего контроля за соблюдением законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных, доведение до сведений работников соответствующих структурных подразделений положений законодательства Российской Федерации о персональных данных, правовых актов по вопросам обработки персональных данных, требований к защите персональных данных.

2. ЗАДАЧИ И ФУНКЦИИ ОТВЕТСТВЕННОГО ЗА ОРГАНИЗАЦИЮ ОБРАБОТКИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Основными задачами Ответственного являются:

– разработка нормативной правовой документации, регламентирующей порядок обработки и защиты ПДн;

– организация доведения до сведения сотрудников, допущенных к ПДн, положений законодательства РФ о ПДн, локальных актов по вопросам обработки ПДн, требований к защите ПДн;

– осуществление внутреннего контроля соблюдения требований законодательства РФ и инструкций при обработке ПДн, в том числе требований к защите ПДн;

– организация контроля эффективности защиты ПДн.

2.2. Для выполнения поставленных задач на Ответственного возлагаются следующие функции:

– организация допуска пользователей (разработчиков, эксплуатационного персонала) к техническим, программным средствам и информационным ресурсам ГИС в соответствии с матрицей доступа пользователей к защищаемым ПДн, обрабатываемым в ГИС на всех стадиях жизненного цикла ГИС;

– участие на стадии проектирования (внедрения) ГИС, в разработке технологии обработки ПДн по вопросам:

– организации порядка учета, хранения и обращения с документами и носителями информации;

– подготовка новых инструкций и внесение изменений и дополнений в настоящую Инструкцию, определяющих задачи, функции, ответственность, права и обязанности администраторов и пользователей ГИС по вопросам защиты ПДн;

– организация контроля выполнения требований действующих нормативных документов по вопросам защиты информации при обработке ПДн в ГИС;

– оперативный контроль хода технологического процесса обработки ПДн;

– методическое руководство работой пользователей ГИС в вопросах обеспечения информационной безопасности.

3. ОБЯЗАННОСТИ ОТВЕТСТВЕННОГО ЗА ОРГАНИЗАЦИЮ ОБРАБОТКИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Ответственный за организацию обработки персональных данных обязан:

– определить порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;

– определять порядок и условия применения средств защиты информации;

– анализировать эффективность применения мер по обеспечению безопасности персональных данных;

– контролировать состояние учета машинных носителей персональных данных;

– проверять соблюдение правил доступа к персональным данным;

– контролировать проведение мероприятий по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

– поддерживать в актуальном состоянии организационно-распорядительные документы в области обеспечения защиты персональных данных;

– осуществлять учет и периодический контроль состава и полномочий пользователей АРМ, на которых ведется обработка ПДн;

– обеспечивать конфиденциальность персональных данных, ставших известными в ходе проведения мероприятий внутреннего контроля.

4. ПРАВА ОТВЕТСТВЕННОГО ЗА ОРГАНИЗАЦИЮ ОБРАБОТКИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Ответственный за организацию обработки персональных данных имеет право:

– осуществлять проверки по контролю соответствия обработки персональных данных требованиям к защите персональных данных;

– запрашивать у сотрудников Министерства информацию, необходимую для реализации полномочий;

– требовать от ответственных должностных лиц за обработку персональных данных уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;

– применять меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства Российской Федерации;

– вносить руководителю МИинистерства предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке;

– вносить руководителю Министерства предложения о привлечении к дисциплинарной ответственности работников Министерства, виновных в нарушении законодательства Российской Федерации в отношении обработки персональных данных;

– участвовать в служебных расследованиях по фактам нарушения установленных требований обеспечения информационной безопасности, НСД, утраты, порчи защищаемой информации и технических компонентов ГИС.

5. ПРОВЕДЕНИЕ ВНУТРЕННИХ РАССЛЕДОВАНИЙ ПО ФАКТАМ РАЗГЛАШЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1 Основными целями проведения внутреннего расследования являются:

– выявление предпосылок утраты ПДн в результате нарушения порядка их обработки;

– выявление лиц из числа сотрудников Министерства виновных в утрате ПДн;

– определение ущерба в результате утраты ПДн;

– проверка полноты и качества исполнения нормативных документов по работе со средствами защиты информации;

– документальное подтверждение соответствия обработки, хранения и передачи ПДн нормам и правилам, установленным федеральными правовыми и нормативными актами;

– определение фактического состояния системы защиты ПДн.

5.2. Работник, по вине которого произошло нарушение, обязан по требованию Ответственного представить объяснения в письменной форме не позднее одного рабочего дня с момента получения соответствующего требования. Ответственный вправе увеличить указанный срок, а также поставить перед работником перечень вопросов, на которые работник обязан ответить.

5.3. В целях внутреннего расследования все работники Министерства, по первому требованию Ответственного, должны предъявить для проверки все числящиеся за ними материалы, содержащие ПДн, представить устные или письменные объяснения, в том числе об известных им фактах разглашения ПДн, утраты документов и изделий, содержащих ПДн.

5.4. Для проведения внутреннего расследования министр формирует комиссию из опытных и квалифицированных сотрудников Министерства в составе не менее трех человек. Председателем комиссии является Ответственный за организацию обработки и защиты ПДн.

5.5. До вынесения решения членам комиссии запрещается разглашать сведения остальным сотрудникам Министерства о ходе проведения внутреннего расследования и ставших известными им в связи с этим обстоятельствах.

5.6. В процессе проведения внутреннего расследования выясняются:

- перечень разглашенных сведений, составляющих ПДн;
- причины разглашения ПДн;
- круг лиц, виновных в разглашении ПДн;
- размер причиненного ущерба;
- недостатки и нарушения, допущенные работниками Министерства при работе с ПДн;
- иные обстоятельства.

5.7. По результатам расследования комиссией составляется акт с отражением в нем лиц, виновных в разглашении ПДн, размера причиненного ущерба Министерства, наличии ущерба субъектам персональных данных, а также иных выясненных обстоятельствах.

5.8. На основании акта комиссия выносит решение о:

- применении мер дисциплинарного воздействия к работнику, виновному в разглашении ПДн;
- информировании регулятора о факте нарушения;
- информировании правоохранительных органов;
- информировании субъектов персональных данных.
-

6. ОТВЕТСТВЕННОСТЬ

6.1 Ответственный несет ответственность за:

- реализацию утвержденных в Министерства документов, регламентирующих порядок обработки и обеспечения безопасности ПДн;
- разглашение ПДн и сведений ограниченного распространения, ставших известными Ответственному в ходе осуществления своей деятельности;
- качество и последствия проводимых им работ по контролю действий пользователей при работе с персональными данными.

Приложение № 17

Утверждено
приказом Министерства
земельных и имущественных
отношений Республики Тыва
от 26.04.2021 г. № 16-од

ПОЛОЖЕНИЕ
о порядке уничтожения персональных данных, обрабатываемых в государственной информационной системе Министерства земельных и имущественных отношений Республики Тыва

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий документ устанавливает порядок уничтожения персональных данных, обрабатываемых в государственных информационных системах Министерства земельных и имущественных отношений Республики Тыва, при достижении целей обработки или при наступлении иных законных оснований в целях реализации Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», Постановления Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, 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» и принятыми в соответствии с ним нормативными правовыми актами.

1.2. Основные понятия, используемые в Положении:

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

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

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

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

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

2. ПОРЯДОК УНИЧТОЖЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ДОСТИЖЕНИИ ЦЕЛЕЙ ОБРАБОТКИ ИЛИ ПРИ НАСТУПЛЕНИИ ИНЫХ ЗАКОННЫХ ОСНОВАНИЙ

2.1. Уничтожение документов, содержащих ПДн, производится:

– по достижении целей их обработки согласно номенклатуре дел и документов;

– по достижении окончания срока хранения ПДн, оговоренного в соответствующем соглашении заинтересованных сторон, в том числе, если они не подлежат архивному хранению.

2.2. Уничтожение документов, содержащих персональные данные, производится в случае выявления неправомерной обработки персональных данных в срок, не превышающий десяти рабочих дней с момента выявления неправомерной обработки персональных данных.

2.3. Уничтожение информации с ПДн, хранящейся в электронном виде на материальных носителях, производится путем выполнения процедуры специальной подготовки материальных носителей (многократное форматирование разделов, выделенных под хранение данных).

2.4. Уничтожение материальных носителей с ПДн осуществляется механическим либо электромагнитным воздействием с помощью специализированных средств (шредер, уничтожитель оптических дисков и т.п.). Отобранные к уничтожению материалы измельчаются механическим способом до степени, исключающей возможность прочтения текста или сжигаются.

2.5. Уничтожение производится по мере необходимости, в зависимости от объемов накопленных для уничтожения документов.

2.6. Для уничтожения материальных носителей и информации на материальных носителях документально создается экспертная комиссия в составе не менее 2 человек. Уничтожение осуществляется по акту. Уничтожение документов производится в присутствии всех членов комиссии, которые несут персональную ответственность за правильность и полноту уничтожения перечисленных в акте документов (состав комиссии утверждается приказом). После уничтожения материальных носителей членами комиссии подписывается акт в 2 экземплярах делается запись в журнале учета машинных носителей персональных данных, обрабатываемых в государственной информационной системе, а также в номенклатурах и описях дел проставляется отметка «Уничтожено. Акт №__(дата)».

2.8. Накапливаемые для уничтожения документы, копии документов, черновики, содержащие персональные данные, должны храниться отдельно.

2.9. Пересмотр настоящего положения с целью поддержания в актуальном состоянии проводится при возникновении следующих условий:

– изменение целей и/или состава обрабатываемых персональных данных;

– возникновение условий, существенно влияющих на процессы обработки персональных данных и нерегламентированных настоящим документом;

– по результатам контрольных мероприятий и проверок контролирующих органов, выявивших несоответствие требованиям по обеспечению безопасности персональных данных;

– при появлении новых требований к обеспечению безопасности персональных данных со стороны законодательства Российской Федерации и контролирующих органов.