ТЫВА РЕСПУБЛИКАНЫН
ТУДУГ ЯАМЫЗЫ

МИНИСТЕРСТВО СТРОИТЕЛЬСТВА
РЕСПУБЛИКИ ТЫВА

ПРИКАЗ

от 01 октября 2021 г. № 89 - од

г. Кызыл

Об организации обработки персональных данных в Министерстве строительства Республики Тыва

В соответствии с Положением о Министерстве строительства Республики Тыва, утвержденным постановлением Правительства Республики Тыва от 5 июля 2021 г. № 319, на основании постановления Правительства Российской Федерации от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» и в целях совершенствования работы по организации обработки персональных данных в Министерстве строительства Республики Тыва ПРИКАЗЫВАЮ:

1. Утвердить:

– Правила обработки персональных данных в Министерстве строительства Республики Тыва согласно Приложению № 1;

– Правила рассмотрения запросов субъектов персональных данных или их представителей согласно Приложению № 2;

– Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных», в Министерстве строительства Республики Тыва согласно Приложению № 3;

– Правила работы с обезличенными персональными данными в Министерстве строительства Республики Тыва согласно Приложению № 4;

– Типовое обязательство государственного служащего (сотрудника) Министерства строительства 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 согласно Приложению № 5;

– Типовую форму разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные согласно Приложению № 6;

– Порядок доступа государственных служащих (сотрудников) в помещения Министерства строительства Республики Тыва в которых ведется обработка конфиденциальной информации, в том числе персональных данных, в

рабочее и нерабочее время, а также в нештатных ситуациях, согласно Приложению № 7;

– Типовую форму обязательства о неразглашении персональных данных в Министерство строительства Республики Тыва согласно Приложению № 8;

– Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации в Министерство строительства Республики Тыва согласно Приложению № 9;

– Типовую форму согласия на обработку персональных данных субъекта персональных данных согласно Приложению № 10,

2. Назначить ответственными за организацию обработки персональных данных следующих лиц:

– Монгуша Буяна Мергеновича - заместителя министра строительства Республики Тыва (статс-секретаря);

– Канзываа Урану Отук-ооловну - заместителя министра строительства Республики Тыва;

– Канкова Владимира Викторовича - заместителя министра строительства Республики Тыва – главного архитектора Республики Тыва;

– Чанзан Веронику Артуровну – начальника отдела правового и кадрового обеспечения;

– Самдан Людмилу Монгушовну – консультанта отдела правового и кадрового обеспечения;

– Дадар-оол Алесю Богдановну – ведущего эксперта отдела правового и кадрового обеспечения;

– Доспан-Самбу Роксану Александровну – начальника отдела экономического анализа, контроля, бухгалтерского учета и отчетности;

– Ооржак Эллу Сергеевну – заместителя начальника отдела экономического анализа, контроля, бухгалтерского учета и отчетности (главного бухгалтера);

– Бегзи-Хуурак Алену Борисовну – начальника отдела по вопросам государственных программ и инвестиций;

– Очур Айлан Владимировну – начальника отдела архитектуры, территориального планирования и контроля за градостроительной деятельностью;

– Монгуш Амелия Анатольевна – консультант отдела архитектуры, территориального планирования и контроля за градостроительной деятельностью;

– Монгуш Риану Александровну – начальника отдела реализации национальных проектов;

– Серен-Чимит Орланмаа Шолбановну – консультанта отдела реализации национальных проектов;

– Дадаштай Валентину Мартай-ооловну – начальника отдела организационного и документационного обеспечения и контроля;

– Бады Херела Васильевича – начальника отдела строительства и развития стройиндустрии;

– Ооржака Буян-Даша Владимировича – консультанта отдела строительства и развития стройиндустрии.

3. Контроль за исполнением настоящего приказа возложить на заместителя министра строительства Республики Тыва (статс-секретаря) Монгуша Б.М.

И.о. министра А.В. Хунай-оол

Приложение № 1
к приказу от 01 октября 2021 г. № 89- од

Правила обработки персональных данных в Министерстве строительства Республики Тыва

1. Общие положения

Настоящие Правила обработки персональных данных в Министерстве строительства Республики Тыва (далее – Министерство) 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.

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. Категории субъектов ПДн

В Министерстве осуществляется обработка ПДн следующих субъектов ПДн:

- государственных служащих (сотрудников) Министерства;
- кандидатов, участвующих в конкурсе на замещение вакантных должностей государственной службы, на включение в кадровый резерв;
- граждан, включенных в кадровый резерв государственной службы;
- граждан, направляющих обращения в Министерство;
- награждаемых юридических и физических лиц.
- граждане и организации, обратившиеся в Министерство в связи с предоставлением государственных услуг.

3. Принципы обработки ПДн

Обработка ПДн в Министерстве 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 неполных, 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 ПДн подлежат уничтожению, либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

4. Цели обработки ПДн

Цели обработки ПДн должны быть четко определены и соответствовать:

- заявленным в положении о Министерстве основным полномочиям и правам;
- задачам и функциям Министерства.

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 осуществляется для исполнения наделенных полномочий, организации кадровой работы, финансовой деятельности в соответствии с действующим положением.

5. Способы и правила обработки ПДн

5.1. В Министерстве 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 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 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 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.

7. Обработка ПДн без согласия субъекта ПДн

Обработка ПДн без получения согласия на такую обработку от субъекта ПДн в Министерстве 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 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, обязано соблюдать принципы и правила обработки ПДн.

В случае, если Министерство поручит обработку ПДн другому лицу, ответственность перед субъектом ПДн за действия указанного лица несет Министерство. Лицо, осуществляющее обработку ПДн по поручению Министерства несет ответственность перед Министерством.

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 государственными служащими (сотрудниками) Министерства получающими доступ к ПДн, должна обеспечиваться конфиденциальность таких данных.

Конфиденциальность персональных данных – это обязательное для соблюдения Министерство 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 Министерство 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 обязан 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 обязан 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 Министерство 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 Министерство 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 Министерство 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 Министерстве.

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 строительства 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 Министерства,
- 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 Министерстве, 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 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) Министерстве, 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 строительства 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 Министерство 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 Министерства обязан 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 и принимает все меры для извещения субъекта ПДн.

Приложение № 2
к приказу от 01 октября 2021 г. № 89- 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 в Министерстве (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 строительства 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 Министерства 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 Министерства 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 обязан руководствоваться частью 2 статьи 20 Федерального закона № 152-ФЗ.

Министерство обязан:

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 строительства 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 Министерстве;

– правовые основания и цели обработки ПДн;

– цели и применяемые Министерство способы обработки ПДн;

– наименование и место нахождения Министерстве, сведения о лицах (за исключением работников Министерства), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с Министерством строительства Республики Тыва 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 Министерстве, 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 Министерстве, 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 Министерстве, 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 обязан 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 ПДн 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 строительства Республики Тыва

Персональные данные не подлежат разглашению (распространению).

Прекращение доступа к такой информации не освобождает государственных служащих (сотрудников) Министерство 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
к приказу от 01 октября 2021 г. № 89- од

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

1. Общие положения

Настоящие Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в Министерстве (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 Министерство 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) Министерство положений действующего законодательства Российской Федерации в области ПДн, правовых актов Министерстве

– соблюдения государственными служащими (работниками) Министерство 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 Министерство (заместителю руководителя Министерства).

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 министром строительства Республики Тыва (либо его заместителем) и утверждается руководителем.

Приложение
к Правилам осуществления внутреннего контроля
соответствия обработки персональных данных
требованиям к защите персональных данных в
Министерстве строительства Республики Тыва

Протокол № ___
контроля выполнения требований по обеспечению безопасности информации, содержащей сведения ограниченного доступа, при ее автоматизированной обработке в ИС Министерства строительства 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
к приказу от 01 октября 2021 г. № 89- од

Правила работы
с обезличенными персональными данными в Министерстве строительства Республики Тыва

1. Общие положения

Настоящие Правила работы с обезличенными персональными данными в Министерстве стороительства Республики Тыва (далее – Министерство) 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 Министерстве, 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
к приказу от 01 октября 2021 г. № 89- од

Типовое обязательство
государственного служащего (сотрудника) Министерства строительства 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
к приказу от 01 октября 2021 г. № 89- 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 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 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
к приказу от 01 октября 2021 г. № 89- од

Порядок доступа
государственных служащих (сотрудников) в помещения Министерства строительства Республики Тыва, в которых ведется обработка конфиденциальной информации, в том числе персональных данных, в рабочее и нерабочее время, а также в нештатных ситуациях

1. Общие положения

Настоящий Порядок доступа государственных служащих (сотрудников) в помещения Министерства, в которых ведется обработка конфиденциальной информации, в том числе персональных данных (далее – Порядок) разработан 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», постановлением Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказом ФСБ России от 10.07.2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» и другими нормативными правовыми актами.

Настоящий Порядок регламентирует условия и порядок осуществления доступа государственных служащих (сотрудников) Министерство и других лиц в помещения Министерстве, в которых ведется обработка конфиденциальной информации, в том числе персональных данных (далее – помещения) в целях обеспечения безопасности персональных данных (далее – ПДн).

Для обеспечения доступа государственных служащих (сотрудников) Министерство в вышеуказанные помещения предусматривается комплекс специальных мер, препятствующих возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих прав доступа в такие помещения, а также направленных на поддержание и обеспечение установленного порядка деятельности Министерстве.

Указанные меры осуществляются руководителями подразделений Министерства, осуществляющих обработку ПДн.

2. Правила доступа в помещения в рабочее, нерабочее время, а внештатных ситуациях

Доступ в Помещения в рабочее (служебное) время имеют сотрудники, включенные в Перечень должностей лиц, допущенных (имеющих доступ) в помещения

Министерства, в которых ведется обработка конфиденциальной информации, утвержденный Министерством строительства Республики Тыва.

В нерабочее (неслужебное) время пребывание вышеуказанных сотрудников разрешается на основании <служебных записок (или иных видов разрешающих документов)>, подписанных руководителем Министерстве

Допуск лиц, не указанных в «Перечне должностей лиц, допущенных (имеющих доступ) в помещения, в которых ведется обработка конфиденциальной информации», осуществляется сотрудниками Министерстве, имеющими постоянный доступ в помещения Министерства

Руководитель и лица, его замещающие, могут находиться в Помещениях в любое время, в том числе в нерабочие и праздничные дни.

Перед началом рабочего дня вскрытие помещения сотрудником осуществляется следующим образом:

– на посту охраны в журнале приема-сдачи помещений под охрану делается запись о снятии помещения с сигнализации и о его вскрытии, при этом указываются: время, № кабинета, фамилия, имя, отчество сотрудника и подпись;

– при вскрытии помещения проверяется целостность печати и исправность замков;

– при обнаружении нарушения целостности оттисков печатей, повреждения замков, а также других признаков, указывающих на возможное проникновение в защищаемое помещение посторонних лиц, вскрытие не производят, о случившемся составляют акт и немедленно ставят в известность руководителя предприятия и орган безопасности. Одновременно принимаются меры по охране места происшествия, до прибытия сотрудников органа безопасности.

По окончанию рабочего времени сотрудник, ответственный за сдачу помещения под охрану, выполняет следующие действия:

– закрывает в металлических шкафах служебную документацию, литературу, предназначенную для служебного пользования;

– закрывает окна;

– выключает освещение, бытовые приборы, оргтехнику и проверяют противопожарное состояние помещения;

– закрывает дверь на замок, проверяет прочность закрытия двери, опечатывает кабинет;

– лично информирует охрану о постановке помещения на сигнализацию и о его закрытии, при этом в журнале приема-сдачи помещений под охрану делается запись о постановке на охрану помещения, при этом указываются: время, № кабинета, свою фамилию, имя и отчество.

На посту охраны должны находиться списки сотрудников, подписанные руководителем предприятия, которым разрешено вскрытие и сдача под охрану защищаемого помещения, с фотографиями сотрудников и образцами подписей этих сотрудников.

Все ключи учитываются в журнале учета ключей от защищаемого помещения (далее - журнал). Листы журнала должны быть пронумерованы, прошнурованы и скреплены мастичной печатью на последней странице.

При срабатывании охранной сигнализации в служебных помещениях в нерабочее время охранник сообщает о случившемся ответственному за помещение или руководителю структурного подразделения. Помещения вскрывать запрещается. Помещения вскрываются ответственным за помещение или руководителем структурного подразделения в присутствии сотрудника охраны с составлением акта.

Уборка помещений, в которых ведется обработка конфиденциальной информации и хранятся документы и носители защищаемой информации, должна производиться в присутствии сотрудников Министерства.

Установка оборудования, его замена или ремонт в защищаемых помещениях должны проводиться по согласованию с лицом, ответственным за проведение соответствующих работ (установку оборудования) в Министерстве.

В случае возникновения нештатной ситуации необходимо незамедлительно сообщать руководителю Министерства

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

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 ФИО	Подразделение
АИС «Дети России»		
1.	Министр Сандан Э.Ф.	
2.	Заместитель министра Ондар О.К.	
3.	Региональный оператор ГБД детей-сирот Борбак-оол Е.С.	**Отдел по вопросам опеки и попечительства**
4.		
5.		
Документ оборот для служебного пользования		
6.	Министр Сандан Э.Ф.	
7.	И.о. первого заместителя министра Увангур А.К-Х.	
8.	Главный специалист Дамбаа Н.Б.	**Отдел содействия занятости населения**

Приложение № 8
к приказу от 01 октября 2021 г. № 89- од

Типовая форма обязательства о неразглашении персональных данных в Министерстве строительства 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
к приказу от 01 октября 2021 г. № 89- од

Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации в Министерстве строительства 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* (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 Министерство 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
к приказу от 01 октября 2021 г. № 89- 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.