



**РЕСПУБЛИКА БУРЯТИЯ
АДМИНИСТРАЦИЯ МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ
«ЗАКАМЕНСКИЙ РАЙОН»**

ПО С Т А Н О В Л Е Н И Е

от 17 мая 2024 г.

№ 346

г. Закаменск

**Об утверждении Положения об обработке и защите персональных данных
работников Администрации муниципального образования
«Закаменский район»**

В соответствии с Конституцией Российской Федерации, Федеральным законом от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Гражданским кодексом Российской Федерации, Трудовым кодексом Российской Федерации, Постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Уставом муниципального образования «Закаменский район», Администрация муниципального образования «Закаменский район» **п о с т а н о в л я е т:**

1. Утвердить Положение об обработке и защите персональных данных работников Администрации муниципального образования «Закаменский район» (приложение).

2. Постановление Главы муниципального образования «Закаменский район» от 31.12.2015 № 994 «Об утверждении Положения об обработке и защите персональных данных работников Администрации муниципального образования «Закаменский район» считать утратившими силу.

3. Контроль за исполнением настоящего постановления возложить на руководителя аппарата Администрации муниципального образования «Закаменский район» Дамбаева Ю.А.

4. Настоящее постановление вступает в силу с момента подписания и официального опубликования на официальном сайте муниципального образования «Закаменский район» <https://mcuzakamna.gosuslugi.ru/>.

И.О. Главы муниципального образования «Закаменский район»
руководителя Администрации муниципального образования
«Закаменский район»



А.В. Тудунов

**ПОЛОЖЕНИЕ
ОБ ОБРАБОТКЕ И ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ
АДМИНИСТРАЦИИ МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ
«ЗАКАМЕНСКИЙ РАЙОН»**

1. ОБЩЕЕ ПОЛОЖЕНИЕ

1.1. Настоящее Положение об обработке и защите персональных данных (далее – Положение) Администрации муниципального образования «Закаменский район» (далее – работодатель) разработано в соответствии с Конституцией Российской Федерации, Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Трудовым кодексом Российской Федерации, Гражданским кодексом Российской Федерации, Постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Уставом муниципального образования «Закаменский район».

1.2. Цель разработки Положения – определение порядка обработки персональных данных работников Администрации; обеспечение защиты прав и свобод работников Администрации при обработке их персональных данных, хранение персональных данных, а также установление ответственности должностных лиц, имеющих доступ к персональным данным работников Администрации, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

1.3. Порядок ввода в действие и изменения Положения:

1.3.1. Настоящее Положение вступает в силу с момента его утверждения Администрацией муниципального образования «Закаменский район» и действует бессрочно, до замены его новым Положением.

1.3.2. Все изменения в Положение вносятся постановлением Администрации муниципального образования «Закаменский район».

1.4. Все работники Администрации муниципального образования «Закаменский район» должны быть ознакомлены с настоящим Положением под роспись.

1.5. Режим конфиденциальности персональных данных снимается в случаях их обезличивания и по истечении 75 лет срока хранения или продлевается на основании заключения экспертной комиссии работодателя, если иное не определено законом.

2. ОСНОВНЫЕ ПОНЯТИЯ И СОСТАВ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ

2.1. Для целей настоящего Положения используются следующие основные понятия:

- персональные данные работника – любая информация, относящаяся к определенному или определяемому на основании такой информации работнику, в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация, необходимая работодателю в связи с трудовыми отношениями;

- обработка персональных данных – сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передача), обезличивание, блокирование, уничтожение персональных данных работников Администрации;

- конфиденциальность персональных данных – обязательное для соблюдения назначенного ответственного лица, получившего доступ к персональным данным работников,

требование не допускать их распространения без согласия работника или иного законного основания;

- использование персональных данных – действия (операции) с персональными данными, совершаемые должностным лицом Администрации в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении работников либо иным образом затрагивающих их права и свободы или права и свободы других лиц;

- блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использование, распространения персональных данных работника, в том числе их передача;

- уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных работников и обучающихся или в результате которых уничтожаются материальные носители персональных данных работников;

- обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному работнику;

- документированная информация – зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель.

2.2. Получение персональных данных осуществляется в соответствии с нормативно-правовыми актами Российской Федерации в области трудовых отношений, нормативными и распорядительными документами, Положением об обработке и защите персональных данных на основе согласия субъектов на обработку их персональных данных. Работодатель не вправе требовать от субъекта персональных данных, предоставляющих информации о его национальности и расовой принадлежности, политических и религиозных убеждениях и о его частной жизни. Без согласия субъектов осуществляется обработка общедоступных персональных данных или содержащих только фамилии, имена и отчества, обращений и запросов организаций и физических лиц, регистрация и отправка корреспонденции почтовой связью, оформление разовых пропусков, обработка персональных данных для исполнения трудовых договоров или без использования средств автоматизации, и в иных случаях, предусмотренных законодательством Российской Федерации.

2.3. Обработка и использование персональных данных осуществляется в целях, указанных в соглашениях с субъектами персональных данных, а также в случаях, предусмотренных нормативно-правовыми актами Российской Федерации. Не допускается принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы. В случае увольнения субъекта персональных данных и иного достижения целей обработки персональных данных, зафиксированных в письменном соглашении, Работодатель обязан незамедлительно прекратить обработку персональных данных и уничтожить соответствующие персональные данные в срок, не превышающий трех рабочих дней, если иное не предусмотрено федеральными законами.

Правила обработки и использования персональных данных устанавливаются инструкциями Работодателя (приложения № 1, 2).

2.4. Персональные данные могут храниться в бумажном и (или) электронном виде централизованно или в соответствующих структурных подразделениях с соблюдением предусмотренных правил. Право на обработку персональных данных предоставляется работникам структурных подразделений и (или) должностным лицам, определенным настоящим Положением об обработке и защите персональных данных, распорядительными документами и иными письменными указаниями Работодателя.

2.5. Персональные данные защищаются от несанкционированного доступа в соответствии с нормативно-правовыми актами Российской Федерации, нормативно-распорядительными актами и рекомендациями регулирующих органов в области защиты информации, а также утвержденными нормативно-правовыми актами и инструкциями Работодателя.

3. ПРАВА, ОБЯЗАННОСТИ И ОТВЕТСТВЕННОСТЬ СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ И РАБОТОДАТЕЛЯ ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Права субъекта персональных данных в целях обеспечения защиты своих персональных данных:

- получать сведения о Работодателе в целях обеспечения защиты своих персональных данных, за исключением случаев, предусмотренных данным Федеральным законом;

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

- получать при обращении или при получении запроса информацию, касающуюся обработки его персональных данных;

- обжаловать действия или бездействия Работодателя в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

3.2. Работодатель обязан безвозмездно предоставить субъекту персональных данных или его законному представителю возможность ознакомления с персональными данными, относящимися к соответствующему субъекту персональных данных, а также внести в них необходимые изменения, уничтожить или заблокировать соответствующие персональные данные по представлению субъектом персональных данных или его законным представителем сведений, подтверждающих, что персональные данные, которые относятся к соответствующему субъекту и обработку которых осуществляет Работодатель, являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки. О внесенных изменениях и предпринятых мерах Работодатель обязан уведомить субъекта персональных данных или его законного представителя и третьих лиц, которым персональные данные этого субъекта были переданы.

3.3. В случае выявления неправомерных действий с персональными данными Работодатель обязан сообщить непосредственному руководителю по безопасности о выявленных нарушениях, в срок, не превышающий трех рабочих дней с даты такого выявления, устранить допущенные нарушения. В случае невозможности устранения допущенных нарушений Работодатель в срок, не превышающий трех рабочих дней с даты выявления неправомерности действий с персональными данными, обязан уничтожить персональные данные. Об устранении допущенных нарушений или об уничтожении персональных данных Работодатель обязан уведомить субъекта персональных данных или его законного представителя.

3.4. В случае отзыва субъекта персональных данных согласия на обработку своих персональных данных Работодатель обязан прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва, если иное не предусмотрено Федеральными законами и (или) соглашением между Работодателем и субъектом персональных данных. Об уничтожении персональных данных Работодатель обязан уведомить субъекта персональных данных.

4. ОБЩИЕ ПРАВИЛА ХРАНЕНИЯ И ПЕРЕДАЧИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Лица, осуществляющие хранение и передачу персональных данных, обязаны соблюдать следующие правила:

- запрещается оставлять материальные носители с персональными данными без присмотра в незапертом помещении;

- все сотрудники ответственные за обработку персональных данных, постоянно работающие в помещениях, в которых ведется обработка персональных данных, должны быть допущены к работе с соответствующими видами персональных данных;

- сотрудникам, работающим с персональными данными, запрещается сообщать их устно или письменно кому бы то ни было, если это не вызвано служебной необходимостью, письменным запросам установленного образца;

- после подготовки и передачи документа в соответствии с резолюцией, файлы черновиков и вариантов документа переносятся подготовившим их сотрудником на маркированные носители, предназначенные для хранения персональных данных;

- без согласования с руководителем формирование и хранение баз данных (картотек, файловых архивов и др.), содержащих конфиденциальные данные, запрещается.

- передача персональных данных допускается только в случаях, установленных Федеральными законами Российской Федерации «О персональных данных», «О порядке рассмотрения обращений граждан Российской Федерации», настоящей инструкцией, а также по письменному поручению (резолюции) вышестоящих должностных лиц;

- запрещается передача персональных данных по телефону, факсу, электронной почте за исключением случаев, установленных законодательством и настоящей инструкцией;

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

5. ПРАВА РАБОТОДАТЕЛЯ НА ПЕРЕДАЧУ ПЕРСОНАЛЬНЫХ ДАННЫХ ТРЕТЬИМ ЛИЦАМ

Работодатель не вправе без письменного согласия субъекта персональных данных передавать обрабатываемые персональные данные третьим лицам, за исключением случаев, предусмотренных законодательством Российской Федерации.

6. ОТВЕТСТВЕННОСТЬ РАБОТОДАТЕЛЯ ЗА РАЗГЛАШЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Работодатель, а также должностные лица, виновные в нарушении требований настоящего Федерального закона, несут гражданскую, уголовную, административную, дисциплинарную и иную ответственность, предусмотренную законодательством Российской Федерации.

Ответственность за соблюдение требований законодательства Российской Федерации при обработке и использовании персональных данных возлагается в приказе об утверждении Положения и иных приказах на руководителей структурных подразделений и конкретных должностных лиц Работодателя, обрабатывающих персональные данные.

ИНСТРУКЦИЯ ПОЛЬЗОВАТЕЛЯ ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ НА ОБЪЕКТАХ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Предметом настоящей Инструкции являются основные права, обязанности и ответственность пользователя, допущенного к автоматизированной обработке персональных данных и иной конфиденциальной информации на объектах вычислительной техники персональной электронно-вычислительной машины (далее – ПЭВМ) Администрации муниципального образования «Закаменский район».

1.2. Пользователь должен быть допущен к обработке соответствующих категорий персональных данных и иметь навыки работы на ПЭВМ.

1.3. Пользователь при выполнении работ в пределах своих функциональных обязанностей обеспечивает безопасность персональных данных, обрабатываемых и хранимых в ПЭВМ, и несет персональную ответственность за соблюдение требований руководящих документов по защите информации.

2. ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЯ

2.1. Пользователь обязан выполнять общие требования по обеспечению режима конфиденциальности проводимых работ, установленные в настоящей Инструкции;

- при работе с персональными данными не допускать присутствие в помещении, где расположены средства вычислительной техники, лиц, не допущенных к обрабатываемой информации, или располагать во время работы экран видеомонитора так, чтобы исключалась возможность просмотра отображаемой на нем информации посторонними лицами;

- соблюдать правила работы со средствами защиты информации и установленный режим разграничения доступа к техническим средствам, программам, данным, файлам с персональными данными при ее обработке;

- после окончания обработки персональных данных в рамках выполнения одного задания, а также по окончании рабочего дня, произвести удаление остаточной информации с жесткого диска ПЭВМ;

- оповещать обслуживающий ПЭВМ персонал, а также непосредственного начальника о всех фактах или попытках несанкционированного доступа к информации, обрабатываемой в ПЭВМ;

- не допускать «загрязнение» ПЭВМ посторонними программными средствами;

- знать способы выявления нештатного поведения используемых операционных систем и пользовательских приложений, последовательность дальнейших действий;

- знать и соблюдать правила поведения в экстренных ситуациях, последовательность действий при ликвидации последствий аварий;

- помнить личные пароли, персональные идентификаторы не оставлять без присмотра и хранить в запирающемся ящике стола или сейфе;

- знать штатные режимы работы программного обеспечения, знать пути проникновения и распространения компьютерных вирусов;

- при применении внешних носителей информации перед началом работы провести их проверку на предмет наличия компьютерных вирусов.

2.2. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь должен провести внеочередной антивирусный контроль своей рабочей станции.

2.3. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователь обязан:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов своего непосредственного начальника, администратора системы, а также смежные подразделения, использующие эти файлы в работе;
- оценить необходимость дальнейшего использования файлов, зараженных вирусом;
- провести лечение или уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта следует привлечь администратора системы).

3. ЗАПРЕЩАЕМЫЕ ДЕЙСТВИЯ

Пользователю запрещается выполнять следующие действия:

- записывать и хранить персональные данные на неучтенным установленным порядком машинных носителях информации;
- удалять с обрабатываемых или распечатываемых документов грифы конфиденциальности;
- самостоятельно подключать к ПЭВМ какие-либо устройства и вносить изменения в состав, конфигурацию, размещение ПЭВМ;
- самостоятельно устанавливать и/или запускать (выполнять) на ПЭВМ любые системные или прикладные программы, загружаемые по сети Интернет или с внешних носителей;
- осуществлять обработку персональных данных в условиях, позволяющих осуществлять их просмотр лицами, не имеющими к ним допуска, а также при несоблюдении требований по эксплуатации ПЭВМ;
- сообщать кому-либо устно или письменно личные атрибуты доступа к ресурсам ПЭВМ;
- отключать (блокировать) средства защиты информации;
- производить какие-либо изменения в подключении и размещении технических средств;
- производить иные действия, ограничения на исполнение которых предусмотрены утвержденными регламентами и инструкциями.
- оставлять бесконтрольно ПЭВМ с загруженными персональными данными, с установленными маркированными носителями, электронными ключами, а также распечатываемыми бумажными документами с персональными данными.

4. ПРАВА ПОЛЬЗОВАТЕЛЯ ПЭВМ

Пользователь вправе обрабатывать (создавать, редактировать, уничтожать, копировать, выводить на печать) информацию в пределах установленных ему полномочий, обращаться к обслуживающему ПЭВМ персоналу с просьбой об оказании технической и методической помощи при работе с общесистемным и прикладным программным обеспечением, установленным в ПЭВМ, а также со средствами защиты информации.

5. ОТВЕТСТВЕННОСТЬ ПОЛЬЗОВАТЕЛЕЙ ПЭВМ

5.1. Пользователь несет ответственность за:

- надлежащее выполнение требований настоящей инструкции;

- соблюдение требований нормативных документов и инструкций, определяющих порядок организации работ по защите информации и использования информационных ресурсов;

- сохранность и работоспособное состояние средств вычислительной техники ПЭВМ;

- сохранность персональных данных.

5.2. Особенности обработки персональных данных пользователями отдельных автоматизированных систем могут регулироваться дополнительными инструкциями.

ИНСТРУКЦИЯ О ПОРЯДКЕ ОБЕСПЕЧЕНИЯ КОНФИДЕНЦИАЛЬНОСТИ ПРИ ОБРАЩЕНИИ С ИНФОРМАЦИЕЙ, СОДЕРЖАЩЕЙ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Обязательные для Администрации муниципального образования «Закаменский район» требования по обеспечению конфиденциальности документов, содержащих персональные данные работников:

1) обработка персональных данных работника может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, получении образования и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества;

2) при определении объема и содержания обрабатываемых персональных данных работника работодатель должен руководствоваться Конституцией Российской Федерации, настоящим Кодексом и иными федеральными законами;

3) все персональные данные работника следует получать у него самого. Если персональные данные работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Работодатель должен сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение;

4) работодатель не имеет права получать и обрабатывать сведения о работнике, относящиеся в соответствии с законодательством Российской Федерации в области персональных данных к специальным категориям персональных данных, за исключением случаев, предусмотренных настоящим Кодексом и другими федеральными законами;

5) работодатель не имеет права получать и обрабатывать персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных настоящим Кодексом или иными федеральными законами;

6) при принятии решений, затрагивающих интересы работника, работодатель не имеет права основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронного получения;

7) защита персональных данных работника от неправомерного их использования или утраты должна быть обеспечена работодателем за счет его средств в порядке, установленном настоящим Кодексом и иными федеральными законами;

8) работники и их представители должны быть ознакомлены под роспись с документами работодателя, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области;

- 9) работники не должны отказываться от своих прав на сохранение и защиту тайны;
- 10) работодатели, работники и их представители должны совместно вырабатывать меры защиты персональных данных работников.

1.2. Когда обеспечение конфиденциальности персональных данных не требуется.

В случае обезличивания персональных данных или в отношении общедоступных персональных данных. В общедоступные источники персональных данных (в том числе справочники, адресные книги) в целях информационного обеспечения с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, предоставленные субъектом персональных данных.

1.3. Конфиденциальность персональных данных предусматривает обязательное согласие субъекта персональных данных или наличие иного законного основания на их обработку.

1.4. Согласие субъекта персональных данных не требуется на обработку данных:

- в целях исполнения обращения, запроса субъекта персональных данных, трудового или иного договора с ним;
- адресных данных, необходимых для доставки почтовых отправлений организациями почтовой связи;
- данных, включающих в себя только фамилии, имена и отчества;
- персональных данных, обрабатываемых без использования средств автоматизации.

2. НОРМАТИВНЫЕ ДОКУМЕНТЫ, ОПРЕДЕЛЯЮЩИЕ ОСНОВНЫЕ ТРЕБОВАНИЯ И МЕРОПРИЯТИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПРИ ОБРАБОТКЕ И ХРАНЕНИИ ПЕРСОНАЛЬНЫХ ДАННЫХ И ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ

Основные требования и мероприятия по обеспечению безопасности при обработке и хранении персональных данных установлены постановлением Правительства Российской Федерации от 17 ноября 2007г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных данных» и от 15 сентября 2008г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

3. ОТВЕТСТВЕННОСТЬ ЗА ЗАЩИТУ ОБРАБАТЫВАЕМЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ

Сотрудники Администрации муниципального образования «Закаменский район», а также иные лица, осуществляющие обработку или хранение конфиденциальных данных, несут ответственность в соответствии с пунктом 5 настоящего положения за обеспечение их информационной безопасности.

Лица, виновные в нарушении норм, регулирующих обработку и хранение конфиденциальных данных, несут дисциплинарную, административную или уголовную ответственность в соответствии с законодательством и нормативно – правовыми актами.

4. ПОРЯДОК ОЗНАКОМЛЕНИЯ С ИНСТРУКЦИЕЙ

Сотрудники Администрации муниципального образования «Закаменский район» и лица, выполняющие работы по договорам и контрактам, имеющие отношение к работе с

персональными данными, должны быть в обязательном порядке ознакомлены под роспись с настоящей Инструкцией.

5. ПОРЯДОК

ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПРИ ОБРАБОТКЕ И ХРАНЕНИИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОСУЩЕСТВЛЯЕМОЙ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ, В ТОМ ЧИСЛЕ УСЛОВИЯ ХРАНЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

Безопасность при обработке и хранении персональных данных обеспечивается путем соблюдения следующих требований:

- обработка персональных работников, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных;

- при хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключаяющие несанкционированный к ним доступ. Лица, осуществляющие обработку персональных данных без использования средств автоматизации, должны быть проинформированы о факте обработки ими персональных данных, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки;

- необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях;

- при фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы;

- для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель;

- при несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, исключаящие одновременное копирование иных персональных данных, не подлежащих распространению и использованию.

6. ИСПОЛЬЗОВАНИЕ ТИПОВЫХ ФОРМ ДОКУМЕНТОВ И ЖУРНАЛОВ УЧЕТА

При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (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 персональных данных, осуществляемой без использования средств автоматизации, имя (наименование) и адрес работника, фамилия, 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 Работодателем способов обработки персональных данных;

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

- типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими

персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;

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

7. ПОРЯДОК УНИЧТОЖЕНИЯ ИЛИ ОБЕЗЛИЧИВАНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание). Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, то путем фиксации на том же материальном носителе сведений о вносимых в них изменениях, либо путем изготовления нового материального носителя с уточненными персональными данными.

8. ПОРЯДОК ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПРИ ОБРАБОТКЕ И ХРАНЕНИИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОСУЩЕСТВЛЯЕМОЙ С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ АВТОМАТИЗАЦИИ, В ТОМ ЧИСЛЕ ПРАВИЛА ДОСТУПА, ХРАНЕНИЯ И ПЕРЕСЫЛКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации, а также используемые в информационной системе информационные технологии.

Допуск лиц к обработке персональных данных в информационной системе осуществляется на основании соответствующих разрешительных документов и ключей (паролей) доступа.

Размещение информационных систем, специальное оборудование и организация работы с персональными данными должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого пребывания в этих помещениях посторонних лиц.

Компьютеры и (или) электронные папки, в которых содержатся файлы с персональными данными, для каждого пользователя должны быть защищены индивидуальными паролями доступа, состоящими из 6 и более символов. Работа на компьютерах с персональными данными без паролей доступа или под чужим, или общими (одинаковыми) паролями, запрещается.

Пересылка персональных данных без использования специальных средств защиты по общедоступным сетям связи, в том числе Интернета, запрещается.

9. ОБЩИЕ ТРЕБОВАНИЯ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ

Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации. Средства защиты информации, применяемые в информационных системах, в установленном порядке проходят процедуру оценки соответствия.

При обработке персональных данных в информационной системе пользователями должно быть обеспечено:

- использование предназначенных для этого разделов (каталогов) носителей информации, встроенных в технические средства, или съемных маркированных носителей;

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

- постоянное использование антивирусного обеспечения для обнаружения зараженных файлов и незамедлительное восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

- недопущение несанкционированного выноса из помещений, установки, подключения оборудования, а также удаления, инсталляции или настройки программного обеспечения.

При обработке персональных данных в информационной системе разработчиками и администраторами систем должны обеспечиваться:

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

- учет лиц, допущенных к работе с персональными данными в информационной системе, прав и паролей доступа;

- учет применяемых средств защиты информации, эксплуатационной и технической документации к ним;

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

- описание систем защиты персональных данных.

Специфические требования по защите персональных данных в отдельных автоматизированных системах устанавливаются инструкциями по их использованию и эксплуатации.

10. ПОРЯДОК УЧЕТА, ХРАНЕНИЯ И ОБРАЩЕНИЯ СО СЪЕМНЫМИ НОСИТЕЛЯМИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ТВЕРДЫМИ КОПИЯМИ И ИХ УТИЛИЗАЦИИ, В ТОМ ЧИСЛЕ ОРГАНИЗАЦИЯ УЧЕТА НОСИТЕЛЕЙ ПЕРСОНАЛЬНЫХ ДАННЫХ

Все находящиеся на хранении и обращении съемные носители с персональными данными подлежат учету.

Каждый съемный носитель с записанными на нем персональными данными должен иметь этикетку, на которой указывается его уникальный учетный номер.

Учет и выдачу съемных носителей персональных данных осуществляют сотрудники, на которых возложены функции хранения носителей персональных данных.

Сотрудники получают учетный съемный носитель от уполномоченного сотрудника для выполнения работ на конкретный срок, по окончании работ пользователь сдает съемный носитель для хранения уполномоченному сотруднику о чем делаются соответствующие записи в журнале учета (приложение 1).

11. ПРАВИЛА ИСПОЛЬЗОВАНИЯ СЪЕМНЫХ НОСИТЕЛЕЙ ПЕРСОНАЛЬНЫХ ДАННЫХ

Съемные носители с персональными данными нельзя хранить вместе с носителями открытой информации, на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам, нельзя выносить съемные носители с персональными данными из служебных помещений для работы с ними на дому, в гостиницах и т.д.

При отправке или передаче персональных данных адресатам на съемные носители записываются только предназначенные адресатам данные. Отправка персональных данных адресатам на съемных носителях осуществляется в порядке, установленном для документов с ограниченным правом пользования. Вынос съемных носителей персональных данных для непосредственной передачи адресату осуществляется только с письменного разрешения руководителя.

12. ПОРЯДОК ДЕЙСТВИЙ ПРИ УТРАТЕ ИЛИ УНИЧТОЖЕНИИ СЪЕМНЫХ НОСИТЕЛЕЙ ПЕРСОНАЛЬНЫХ ДАННЫХ

12.1. О фактах утраты съемных носителей, содержащих персональные данные, либо разглашения содержащихся в них сведений немедленно ставится в известность руководитель Администрации муниципального образования «Закаменский район».

12.2. По факту утраты и (или) разглашения персональных данных распоряжением Администрации муниципального образования «Закаменский район» создается комиссия, которая проводит служебное разбирательство, по результатам которого может быть принято решение о привлечении виновных лиц к ответственности.

12.3. В журналы персонального учета съемных носителей персональных данных вносятся соответствующие записи, составляется акт об утрате носителя.

12.4. Съёмные носители персональных данных, пришедшие в негодность или отслужившие установленный срок, подлежат уничтожению. Уничтожение съемных носителей с конфиденциальной информацией осуществляется уполномоченной комиссией с составлением акта об уничтожении персональных данных (приложение 2).

Журнал
учета съемных носителей персональных данных

наименование структурного подразделения

Начат «__» _____ 20__ г.

Окончен «__» _____ 20__ г.

На _____ лист

№ п/п	Наименование (тип и емкость носителя)	№ носителя	Местонахождение носителя	Ф.И.О. должность получателя	(получил вернул передал/ дата)	Ответственное за учет лицо (Ф.И.О.)	Примечание*
1	2	3	4	5	6	7	8
1.							
2.							
3.							
4.							
5.							
6.							

* Причина и основание окончания использования (№ и дата отправки адресату или распоряжения о передаче, № и дата акта утраты, неисправность, заполнение подлежащими хранению данными, уничтожение носителя)

Приложение 2
к Инструкции о порядке обеспечения
конфиденциальности при обращении с
информацией, содержащей
персональные данные

Разрешаю уничтожить

(руководитель организации)

« ____ » _____ 20__ г.

**Акт
об уничтожении персональных данных**

Комиссия в составе:

	ФИО	Должность
Председатель		
Члены комиссии		

провела отбор носителей персональных данных и установила, что в соответствии с требованиями руководящих документов по защите информации _____ информация, записанная на них в процессе эксплуатации, подлежит уничтожению:

№ п/п	Дата	Тип носителя	Регистрационный номер носителя ПДн	Примечание

Всего уничтожению подлежит _____ носителей
(цифрами и прописью)

После утверждения акта перечисленные носители сверены с записями в акте и на указанных носителях персональные данные уничтожены путем

_____.
(стирания на устройстве гарантированного уничтожения информации и т.п.)

После утверждения акта перечисленные носители сверены с записями в акте и уничтожены путем

(разрезания, сжигания, механического уничтожения, сдачи предприятию по утилизации вторичного сырья и т.п.)

Уничтоженные носители с книг и журналов учета списаны.

Председатель комиссии:

_____ / _____ /

Члены комиссии:

_____ / _____ /

_____ / _____ /

_____ / _____ /

_____ / _____ /

Примечание:

1. Акт составляется отдельно на каждый способ уничтожения носителей.
2. Все листы акта, а так же все произведенные исправления и дополнения в акте заверяются подписями всех членов комиссии.