

**ГОСУДАРСТВЕННОЕ КАЗЕННОЕ УЧРЕЖДЕНИЕ
ТЮМЕНСКОЙ ОБЛАСТИ
«ЦЕНТР ХРАНЕНИЯ УЧЕТНО - ТЕХНИЧЕСКОЙ
ДОКУМЕНТАЦИИ»**

П Р И К А З

«04» июля 2017 г.

№ 3/3

г. Тюмень

Об организации работ по защите персональных данных

В соответствии с требованиями федерального закона Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных», Положения «Об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденного Постановлением Правительства Российской Федерации от 17.11.2007 № 781 и Положения «Об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утвержденного Постановлением Правительства Российской Федерации от 15.09.2008 N 687 в целях обеспечения безопасности персональных данных, обрабатываемых в ГКУ ТО «Центр хранения учетно-технической документации» (далее - учреждение),

ПРИКАЗЫВАЮ:

1. Возложить ответственность за обеспечение безопасности персональных данных в Учреждении на начальника отдела учетно-технической документации.
2. Утвердить:
 - 2.1. Положение об обработке и защите персональных данных работников Учреждения, согласно Приложению №1 к настоящему Приказу.
 - 2.2. Положение об обработке и защите персональных данных субъектов персональных данных в Учреждении, согласно Приложению №2 к настоящему Приказу.
 - 2.3. Инструкцию о порядке учета, хранения и уничтожения носителей персональных данных в Учреждении, согласно Приложению №3 к настоящему Приказу.
 - 2.4. Инструкцию для работников Учреждения, осуществляющих обработку персональных данных заявителей по правилам обработки, хранения и передачи персональных данных, согласно Приложению №4 к настоящему Приказу.

2.5. Инструкцию для работников Учреждения ответственным за кадровое делопроизводство по правилам обработки, хранения и передачи персональных данных работника, согласно Приложению №5 к настоящему Приказу.

2.6. Утвердить перечень сведений, составляющих персональные данные, обрабатываемых в Учреждении, согласно Приложению №6 к настоящему Приказу.

2.7. Утвердить перечень работников, имеющих доступ к персональным данным, обрабатываемым в Учреждении с разграничением прав доступа, согласно Приложению №7 к настоящему Приказу.

2.8. Утвердить перечень помещений, где обрабатываются персональные данные, согласно Приложению №8 к настоящему Приказу.

3. Утвердить формы журналов по вопросам организации защиты персональных данных:

3.1. Журнал учета машинных носителей информации содержащих персональные данные, согласно Приложению №9 к настоящему Приказу. Ответственный за ведение и хранение журнала – Филимонцев А.А.

3.2. Журнал учета проводимых контрольных мероприятий, согласно Приложению №10 к настоящему Приказу. Ответственный за ведение и хранение журнала начальник отдела - Филимонцев А.А.

3.3. Журнал учета обращений субъектов персональных данных, согласно Приложению №11 к настоящему Приказу. Ответственный за ведение и хранение журнала делопроизводитель.

3.4. Журнал учета передачи сведений содержащих персональные данные, согласно Приложению №12 к настоящему Приказу. Ответственный за ведение и хранение журнала делопроизводитель.

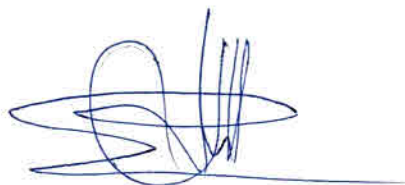
3.5. Журнал учета лиц имевших доступ к сведениям ПДН в период трудовой деятельности, согласно Приложению №13 к настоящему Приказу. Ответственный за ведение и хранение журнала руководитель учреждения.

4. Ввести в Учреждении режим защиты персональных данных.

5. Руководителям структурных подразделений Учреждения, в которых производится обработка персональных данных, организовать ознакомление подчиненных работников с требованиями обработки и защиты персональных данных, установленными в Учреждении, в том числе с Положениями, Инструкциями. При приеме на работу, ознакомление работников с требованиями обработки и защиты персональных данных, установленными в Учреждении, осуществлять в течение одного рабочего дня со дня приема на работу.

6. Контроль за исполнением настоящего приказа оставляю за собой.

Руководитель



А.М. Смирнова

Лист согласования

К приказу ГКУ ТО «Центр хранения учетно-технической документации» № 3/3 от 04.07.2017

№ п/п	Должность	Ф.И.О.	Подпись	Дата согласования	Примечание
1	Начальник отдела	Филимонцев А.А.		.12.17	

УКАЗАТЕЛЬ РАССЫЛКИ

№ п/п	Наименование адресата	Кол-во Экз.	№ экз. (ДСП)
1.	Руководитель	1	
2.	Начальник отдела	1	
3	Специалисты по запросам	8	
4	Инженер	1	
5	Архивариусы	5	
6	Делопроизводитель	1	

Всего экземпляров 17 (семнадцать)

Положение об обработке и защите персональных данных работников Учреждения

1. Термины и определения

Работник - физическое лицо, вступившее в трудовые отношения с работодателем.

Работодатель – ГКУ ТО «Центр хранения учетно-технической документации» (далее - Учреждение), вступивший в трудовые отношения с работником.

Трудовые отношения - отношения, основанные на соглашении между работником и работодателем о личном выполнении работником за плату трудовой функции (работы по определенной должности, специальности, квалификации), конкретного вида поручаемой работнику работы, подчинении работника правилам внутреннего трудового распорядка при обеспечении условий труда, предусмотренных трудовым законодательством, коллективным договором, соглашениями.

Информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Использование персональных данных - действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц, либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

Конфиденциальность персональных данных - обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их раскрытия третьим лицам и распространения без согласия субъекта персональных данных или наличия иного законного основания.

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

Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту

персональных данных).

Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Трансграничная передача персональных данных - передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства.

Уничтожение персональных данных - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

2. Общие положения

Настоящее Положение определяет порядок обработки персональных данных работников. Положение о защите персональных данных работников разработано в соответствии с Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным законом от 27.07.2006 г. №152-ФЗ «О персональных данных», а также другими нормативными правовыми актами, действующими на территории РФ. Требования настоящего Положения доводятся до всех работников Филиала под роспись.

3. Понятие и состав персональных данных работника

Персональные данные работника представляют собой информацию, необходимую работодателю в связи с трудовыми отношениями и касающуюся конкретного работника.

К персональным данным работника относятся следующие сведения:

- анкетно-биографические и характеризующие материалы, содержащиеся:

- в документе, удостоверяющем личность;
 - в трудовой книжке;
 - в страховом свидетельстве государственного пенсионного страхования;
 - в документах воинского учета – при наличии;
 - в документах об образовании, квалификации или наличии специальных знаний или подготовки;
 - в аттестационных документах;
 - в документах, необходимых для определения и исполнения трудовых отношений;
- информация
- медицинского характера, в случаях, предусмотренных законодательством;
 - об имущественном и финансовом положении и др.

4. Обработка персональных данных

1. Общие требования при обработке персональных данных работника.

Обработка персональных данных работника Учреждения может осуществляться с целью обеспечения соблюдения законов и иных нормативных правовых актов, содействия работнику в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работника, контроля количества и качества выполняемой им работы и обеспечения сохранности имущества работника и работодателя.

Все персональные данные работника, следует получать у него самого. Работник дает согласие на обработку своих персональных данных. Форма согласия установлена в Приложении №1 к настоящему Положению. 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.

Работник обязан предоставить письменное согласие/отказ на получение Филиалом своих персональных данных у третьей стороны в течении 1 (одного) дня с момента получения уведомления от работодателя.

Работник предоставляет работодателю достоверные сведения о себе. Работодатель проверяет достоверность сведений, сверяя данные, предоставленные работником, с имеющимися у работника документами.

Работодатель не имеет права получать и обрабатывать персональные данные работника о его политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьей 24 Конституции Российской Федерации работодатель вправе получать, обрабатывать данные частной жизни работника только с его письменного согласия.

Работодатель не имеет права получать и обрабатывать персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных трудовым законодательством и иными федеральными законами.

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.

В случае, если при исполнении должностных обязанностей в функции работника входит обработка персональных данных субъектов персональных данных, то такой работник должен быть уведомлен об этом под расписку.

Работники должны быть ознакомлены под роспись с документами работодателя, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области.

2. Передача персональных данных работников.

При передаче персональных данных работника работодатель должен соблюдать следующие требования:

- не сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в других случаях, предусмотренных федеральными законами;
- не сообщать персональные данные работника в коммерческих целях без его письменного согласия;
- предупредить лиц, получающих персональные данные работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные работника, обязаны соблюдать режим конфиденциальности;
- осуществлять передачу персональных данных работника в пределах одной организации, у одного индивидуального предпринимателя в соответствии с локальным нормативным актом, с которым работник должен быть ознакомлен под роспись;
- разрешать доступ к персональным данным работников только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций;
- не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции;
- передавать персональные данные работника представителям работников в порядке, установленном настоящим Положением, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.

3. Хранение персональных данных работников

Персональные данные работника хранятся в отделе кадров центрального аппарата Филиала в сейфах и/или металлических шкафах, обеспечивающих защиту от несанкционированного доступа, аналогично документам, содержащим сведения конфиденциального характера, на бумажных носителях: трудовая книжка, личная карточка Т-2, копии документов, представляемых при приеме на работу (личное дело).

Учет, хранение и уничтожение бумажных носителей персональных данных должен осуществляться в соответствии с Инструкцией о порядке учета, хранения и уничтожения носителей персональных данных.

Дополнительно персональные данные работников хранятся в электронном

виде в информационных системах персональных данных.

Доступ к электронным базам данных, содержащим персональные данные работников, обеспечивается с помощью подсистемы идентификации/аутентификации пользователей (логин/пароль) на уровне приложений.

4. Доступ к персональным данным.

Право доступа к персональным данным работника в соответствии со своими должностными обязанностями имеют:

- руководитель Учреждения;
- лицо, ответственное за ведение кадрового делопроизводства Учреждения;
- прочие работники структурных подразделений Учреждения в рамках своих должностных обязанностей.

Лицо, ответственное за ведение кадрового делопроизводства Учреждения, а также иные работники по поручению руководителя, вправе передавать персональные данные работников в бухгалтерию Учреждения и другие подразделения Учреждения в случаях, установленных законодательством, необходимых для исполнения работниками соответствующих подразделений их должностных обязанностей, определенных в соответствии с должностной инструкцией и/или трудовым договором.

Иные права, обязанности, действия работников, в трудовые обязанности которых входит обработка персональных данных работника, определяются должностными инструкциями и локальными нормативными актами Учреждения.

Доступ к персональным данным работника осуществляется в соответствии со Списком лиц, допущенных к работе с персональными данными работников, утвержденным Приказом директора Учреждения.

5. Права работника.

В целях обеспечения защиты персональных данных, хранящихся у работодателя, работники имеют право на:

- полную информацию об их персональных данных и обработке этих данных;
- свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные работника, за исключением случаев, предусмотренных федеральными законами;
- определение своих представителей для защиты своих персональных данных;
- доступ к относящимся к ним медицинским данным с помощью медицинского специалиста по их выбору;
- требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований Трудового Кодекса Российской Федерации, Федерального закона от

27.07.2006 г. №152-ФЗ « О персональных данных» и иных федеральных законов. При отказе работодателя исключить или исправить персональные данные работника он имеет право заявить в письменной форме работодателю о своем несогласии, с соответствующим обоснованием такого несогласия;

- требование об извещении работодателем всех лиц, которым ранее были сообщены неверные или неполные персональные данные работника, обо всех произведенных в них исключениях, исправлениях или дополнениях;
- обжалование в суд любых неправомерных действий или бездействия работодателя при обработке и защите его персональных данных.
- каждый работник Учреждения обязан при заключении трудового договора и при изменении персональных данных своевременно, в течение 10 календарных дней представлять в Учреждение достоверные документы и сведения.

6. Гарантии конфиденциальности персональных данных работника

Персональные данные работника имеют статус конфиденциальной информации в соответствии с Указом Президента РФ от 06.03.1997 № 188 «Об утверждении Перечня сведений конфиденциального характера».

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

7. Контроль выполнения требований настоящего Положения

Повседневный контроль порядка обращения с персональными данными осуществляют руководители тех структурных подразделений Учреждения, в которых обрабатываются персональные данные субъектов.

Периодический контроль выполнения настоящего Положения возлагается на должностное лицо, назначенное руководителем Учреждения, ответственным за обеспечение безопасности персональных данных.

СОГЛАСИЕ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ

Я,

паспорт _____ серии _____ № _____
 выдан _____

дата выдачи _____, место регистрации _____

в соответствии со статьей 9 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», даю согласие ГКУ ТО «Центр хранения учетно-технической документации» (далее – Оператор), расположенному по адресу: город Тюмень, улица 50 лет Октября, дом 57Б/6,

с целью проведения проверочных мероприятий в отношении достоверности и полноты представленных мною сведений, осуществления иных прав и обязанностей, возложенных на Оператора как работодателя действующим законодательством,

на смешанную обработку (автоматизированную, а также без использования средств автоматизации), включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение, следующих моих персональных данных:

- фамилия, имя, отчество (в том числе прежние фамилия, имя, отчество, дата, место и причина изменения (в случае изменения));
- год, месяц, дата и место рождения;
- адрес места жительства (место регистрации и фактический адрес) и дата регистрации по месту жительства или по месту пребывания;
- номера телефонов (мобильного и домашнего);
- пол;
- семейное, социальное, имущественное положение;
- сведения об образовании, квалификации и о наличии специальных знаний или специальной подготовки (серия, номер, дата выдачи диплома, свидетельства, аттестата или другого документа об окончании образовательного учреждения);
- страховой номер индивидуального лицевого счета в Пенсионном фонде РФ;
- гражданство;
- идентификационный номер налогоплательщика;
- номер страхового свидетельства государственного пенсионного страхования;
- информация о наличии (отсутствии) судимости;
- сведения о доходах, полученных мной в данном учреждении и от иной оплачиваемой деятельности, составе декларируемых сведений о наличии материальных ценностей;
- сведения о доходах моего(ей) супруга(и) и несовершеннолетних членов моей семьи;
- сведения об имуществе и обязательствах имущественного характера моих, моего(ей)

супруга(и) и несовершеннолетних членов моей семьи;

- стаж работы;
- паспортные данные или данные иного документа, удостоверяющего личность;
- данные трудовой книжки;
- информация, содержащаяся в фотографии;
- сведения о воинском учете;
- государственные и ведомственные награды;
- почетные звания;
- социальные льготы;
- состав семьи;
- данные свидетельств о регистрации брака и рождении детей;
- информация о повышении квалификации и профессиональной переподготовке;
- информация, содержащаяся в документах по служебным и иным проверкам, осуществляемым Оператором в рамках действующего законодательства;
- другая информация, необходимая Оператору в связи с исполнением обязанностей, возложенных на Оператора как работодателя действующим законодательством.

Обработка персональных данных разрешается на срок действия трудового договора. В случае моего увольнения персональные данные подлежат хранению в порядке и в сроки, установленные действующим законодательством.

Я оставляю за собой право отозвать настоящее согласие посредством составления соответствующего письменного документа, который может быть направлен мной в адрес Оператора по почте заказным письмом с уведомлением о вручении либо вручен лично под расписку представителю Оператора.

В случае отзыва мною настоящего согласия Оператор обязан прекратить обработку персональных данных и уничтожить персональные данные в срок, предусмотренный действующим законодательством. Вместе с тем Оператор вправе продолжить обработку персональных данных без согласия при наличии оснований, указанных в Федеральном законе от 27.07.2006 № 152-ФЗ «О персональных данных». Уничтожению не подлежат те персональные данные, которые Оператор обязан хранить в соответствии с действующим законодательством.

“ _____ ” _____ 20 ____ г. _____
(подпись) _____
_____ (расшифровка подписи)

Подтверждаю, что ознакомлен(а) с положениями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», права и обязанности в области защиты персональных данных мне разъяснены.

Подтверждаю, что, давая такое Согласие, я действую своей волей и в своих интересах.

“ _____ ” _____ 20 ____ г. _____
(подпись) _____
_____ (расшифровка подписи)

СОГЛАСИЕ НА ПЕРЕДАЧУ ПЕРСОНАЛЬНЫХ ДАННЫХ

Я,

паспорт _____
 выдан _____ серии _____ № _____

дата выдачи _____, место регистрации _____

в соответствии со статьей 9 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных»,

даю согласие Департаменту имущественных отношений Тюменской области (далее – Оператор), расположенному по адресу: город Тюмень, улица Сакко, дом 30, корпус 1 на передачу моих персональных данных третьим лицам:

- **Департаменту финансов Тюменской области (г. Тюмень, ул. Сакко, д. 17)** в целях размещения информации о возглавляемом мною государственном казенном учреждении «Центр хранения учетно-технической документации» на официальном сайте bus.gov.ru: данные паспорта, идентификационный номер налогоплательщика, номер страхового свидетельства государственного пенсионного страхования;

- **ГКУ ТО «Фонд имущества Тюменской области» (г. Тюмень, ул. Водопроводная, д. 12)** в целях ведения кадровой работы, начисления и выплаты заработной платы: фамилия, имя, отчество (в том числе прежние фамилия, имя, отчество); год, месяц, дата и место рождения; адрес места жительства (место регистрации и фактический адрес) и дата регистрации по месту жительства или по месту пребывания; номера телефонов (мобильного и домашнего); пол; семейное, социальное, имущественное положение; страховой номер индивидуального лицевого счета в Пенсионном фонде РФ; гражданство; идентификационный номер налогоплательщика; номер страхового свидетельства государственного пенсионного страхования; стаж работы; паспортные данные или данные иного документа, удостоверяющего личность; данные трудовой книжки; данные трудового договора; социальные льготы; состав семьи; данные свидетельств о рождении детей.

Я оставляю за собой право отозвать настоящее согласие посредством составления соответствующего письменного документа, который может быть направлен мной в адрес Оператора по почте заказным письмом с уведомлением о вручении либо вручен лично под расписку представителю Оператора.

В случае отзыва мною настоящего согласия Оператор обязан прекратить обработку персональных данных и уничтожить персональные данные в срок, предусмотренный действующим законодательством. Вместе с тем Оператор вправе продолжить обработку персональных данных без согласия при наличии оснований, указанных в Федеральном законе от 27.07.2006 № 152-ФЗ «О персональных данных». Уничтожению не подлежат те персональные данные, которые Оператор обязан хранить в соответствии с действующим законодательством.

_____ 20 17 г. _____
 (подпись) (расшифровка подписи)

Подтверждаю, что ознакомлен(а) с положениями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», права и обязанности в области защиты персональных данных мне разъяснены.

Подтверждаю, что, давая такое Согласие, я действую своей волей и в своих интересах.

_____ 20 17 г. _____
 (подпись) (расшифровка подписи)

ПОЛОЖЕНИЕ

об обработке и защите персональных данных субъектов персональных данных в ГКУ ТО «Центр хранения учетно-технической документации».

1. Общие положения

1. Цель данного Положения – обеспечение требований защиты прав физических лиц (далее – Контрагент), обратившихся в ГКУ ТО «Центр хранения учетно-технической документации» (далее по тексту Положения – Учреждение), при обработке их персональных данных в Учреждении.
2. Персональные данные могут обрабатываться только для целей, непосредственно связанных с деятельностью Учреждения, в частности для оказания услуг, предусмотренных Уставом Учреждения, а также во исполнение Учреждением действующего законодательства Российской Федерации. Учреждение собирает данные только в объеме, необходимом для достижения названных целей.
3. Сбор, хранение, использование и распространение, в том числе передача третьим лицам, персональных данных без письменного его согласия не допускаются, за исключением случаев, установленных действующим законодательством РФ.
4. Режим конфиденциальности персональных данных снимается в случаях обезличивания или включения их в общедоступные источники персональных данных, если иное не определено действующим законодательством РФ.
5. Сотрудники Учреждения, в обязанность которых входит обработка персональных данных субъектов персональных данных, обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.
6. Персональные данные не могут быть использованы в целях причинения имущественного и морального вреда гражданам, затруднения реализации прав и свобод граждан Российской Федерации. Ограничение прав граждан Российской Федерации на основе использования информации об их социальном происхождении, о расовой, национальной, языковой, религиозной и партийной принадлежности запрещено и карается в соответствии с законодательством.
7. Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.

8. Настоящее положение утверждается руководителем Учреждения и является обязательным для исполнения всеми сотрудниками, имеющими доступ к персональным данным Контрагента.

9. Настоящее Положение не распространяется на отношения по организации хранения, учета и использования содержащих персональные данные документов: технических паспортов, оценочной и иной учетно-технической документации по объектам капитального строительства, включая регистрационные книги, реестры, копии зарегистрированных документов, сформированные в инвентарные дела, образующие архивные фонды, которые относятся к государственной части Архивного фонда Российской Федерации, в соответствии с законодательством об архивном деле в Российской Федерации.

10. Для целей настоящего Положения используются следующие понятия:
Оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Контрагент – физическое лицо, обратившееся в Учреждение, с целью заключения договора с Учреждением, подачи заявления на выполнение работ (оказание услуг) Учреждением, подачи запроса, претензии, жалобы, и т.п.

Персональные данные — любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу, в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, другая информация, необходимая Учреждению для осуществления полномочий;

Обработка персональных данных — сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передача), обезличивание, блокирование, уничтожение персональных данных Контрагентов Учреждения;

Конфиденциальность персональных данных — обязательное для соблюдения назначенного ответственного лица, получившего доступ к персональным данным работников, требование не допускать их распространения без согласия Контрагента или иного законного основания;

Распространение персональных данных — действия, направленные на передачу персональных данных Контрагента определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных работников в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным работников каким-либо иным способом;

Использование персональных данных — действия (операции) с персональными данными, совершаемые должностным лицом Учреждения в целях принятия решений или совершения иных действий, порождающих

юридические последствия в отношении Контрагентов, либо иным образом затрагивающих их права и свободы или права и свободы других лиц;

Блокирование персональных данных — временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных Контрагента, в том числе их передачи;

Уничтожение персональных данных — действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных Контрагентов или в результате которых уничтожаются материальные носители, содержащие персональные данные Контрагентов;

Обезличивание персональных данных — действия, в результате которых невозможно определить принадлежность персональных данных конкретному Контрагенту;

Общедоступные персональные данные — персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия Контрагента или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

Информация — сведения (сообщения, данные) независимо от формы их представления.

Документированная информация — зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель.

Информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Информация ограниченного доступа - информация, доступ к которой ограничен федеральными законами.

Конфиденциальность персональных данных - обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

2. Цели обработки персональных данных. Состав персональных данных

2.1. К целям обработки персональных данных относятся:

- заключение и исполнение запросов в рамках оказания государственной услуги Учреждением;
- заключение и исполнение договоров, заключаемых для нужд Учреждения (расходные договоры);
- иные случаи, предусмотренные действующим законодательством Российской Федерации.

2.2. К персональным данным Контрагентов, которые обрабатывает Учреждение относятся:

- Фамилия, Имя, Отчество
- паспортные данные;
- адрес места жительства;
- номер телефона;
- Идентификационный номер налогоплательщика (ИНН);
- иные сведения и документы, содержащие персональные данные, позволяющие идентифицировать субъекта персональных данных.

3. Принципы обработки персональных данных Контрагента

3.1. Обработка персональных данных должна осуществляться на основе принципов:

- законности целей и способов обработки персональных данных и добросовестности;
- соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям Учреждения;
- соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;
- достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;
- недопустимости объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных;
- уничтожения персональных данных после достижения целей обработки или в случае утраты необходимости в их достижении;
- личной ответственности сотрудников Учреждения за сохранность и конфиденциальность персональных данных, а также носителей этой информации;
- наличие четкой разрешительной системы доступа сотрудников Учреждения к документам и базам данных, содержащим персональные данные.

4. Обязанности Учреждения

4.1. В целях обеспечения прав и свобод человека и гражданина Учреждение при обработке персональных данных Контрагента обязан соблюдать следующие общие требования:

4.1.1. Обработка персональных данных Контрагента может осуществляться исключительно в целях оказания законных услуг Контрагентам.

4.1.2. Персональные данные Контрагента следует получать у него самого. Если персональные данные Контрагента возможно получить только у третьей стороны, то Контрагент должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие, за исключением случаев когда:

1) Контрагент был уведомлен об осуществлении обработки его персональных данных Учреждением;

2) персональные данные получены Учреждением на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является Контрагент;

3) персональные данные сделаны общедоступными субъектом персональных данных или получены из общедоступного источника;

4) Учреждение осуществляет обработку персональных данных для статистических или иных исследовательских целей;

4.1.3. Сотрудники Учреждения должны сообщить Контрагенту о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа Контрагента дать письменное согласие на их получение.

4.1.4. При наличии надлежащим образом оформленного запроса предоставлять Контрагенту доступ к его персональным данным.

4.1.5. Хранение и защита персональных данных Контрагента от неправомерного их использования или утраты должна быть обеспечена Учреждением в порядке, установленном законодательством, и локальными актами Учреждения.

4.1.6. В случае выявления недостоверных персональных данных или неправомерных действий с ними оператора при обращении или по запросу Контрагента либо уполномоченного органа по защите прав субъектов персональных данных Учреждение обязано осуществить блокирование персональных данных на период проверки.

4.1.7. В случае подтверждения факта недостоверности персональных данных оператор на основании документов, представленных Контрагентом либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязан уточнить персональные данные и снять их блокирование.

4.1.8. В случае достижения цели обработки персональных данных Учреждение обязано незамедлительно прекратить обработку персональных данных и уничтожить соответствующие персональные данные в срок, не превышающий трех рабочих дней, и уведомить об этом Контрагента, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

4.1.8. В случае отзыва Контрагента согласия на обработку своих персональных данных Учреждение обязано прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий тридцати рабочих дней, если иное не предусмотрено соглашением, договором между Учреждением и Контрагентом.

5. Права Контрагента

1. Право на доступ к информации о самом себе.
2. Право на определение форм и способов обработки персональных данных.

3. Право на отзыв согласия на обработку персональных данных.
4. Право ограничивать способы и формы обработки персональных данных, запрет на распространение персональных данных без его согласия.
5. Право требовать изменение, уточнение, уничтожение информации о самом себе.
6. Право обжаловать неправомерные действия или бездействия по обработке персональных данных и требовать соответствующей компенсации в суде.
7. Право на дополнение персональных данных оценочного характера заявлением, выражающим его собственную точку зрения.
8. Право определять представителей для защиты своих персональных данных.
9. Право требовать от Учреждения уведомления всех лиц, которым ранее были сообщены неверные или неполные персональные данные Контрагента, обо всех произведенных в них изменениях или исключениях из них.

6. Сбор, обработка, передача, хранение персональных данных

- 6.1. Обработка персональных данных – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.
- 6.2. Порядок получения персональных данных.
 - 6.2.1. Все персональные данные Контрагента следует получать у него самого после предоставления им письменного согласия (Приложение №1 к настоящему Положению), за исключением случаев, когда обработка персональных данных возможна без получения письменного согласия.
 - 6.2.2. Письменное согласие включает в себя:
 - фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
 - наименование (фамилию, имя, отчество) и адрес Учреждения, получающего согласие Контрагента;
 - цель обработки персональных данных;
 - перечень персональных данных, на обработку которых дается согласие Контрагента;
 - перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых Учреждением способов обработки персональных данных;
 - срок, в течение которого действует согласие, а также порядок его отзыва.
 - 6.2.3. Допускается обработка персональных данных без согласия субъекта персональных данных, в случаях:
 - обработка персональных данных необходима для достижения целей, предусмотренных законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;
 - обработка персональных данных осуществляется в целях исполнения договора, одной из сторон которого является Контрагент;

- обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;
- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов Контрагента, если получение его согласия невозможно;
- в иных случаях, предусмотренных действующим законодательством Российской Федерации.

6.2.4. В случае недееспособности субъекта персональных данных согласие на обработку его персональных данных дает законный представитель субъекта персональных данных.

6.2.5. В случае смерти субъекта персональных данных согласие на обработку его персональных данных дают наследники субъекта персональных данных, если такое согласие не было дано субъектом персональных данных при его жизни.

6.2.6. Персональные данные могут быть получены Учреждением от лица, не являющегося субъектом персональных данных, при условии предоставления Учреждению подтверждения наличия оснований, указанных в пунктах 2-11 части 1 статьи 6 ФЗ «О персональных данных».

2. При сборе персональных данных оператор обязан предоставить субъекту персональных данных по его просьбе следующую информацию:

- подтверждение факта обработки персональных данных Учреждением, а также цель такой обработки;
- способы обработки персональных данных, применяемые Учреждением;
- сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;
- перечень обрабатываемых персональных данных и источник их получения;
- сроки обработки персональных данных, в том числе сроки их хранения;
- сведения о том, какие юридические последствия для субъекта персональных данных может повлечь за собой обработка его персональных данных.

6.4. Если персональные данные о Контрагенте возможно получить только у третьей стороны, то Контрагенту должна быть предоставлена следующая информация:

- наименование (фамилия, имя, отчество) и адрес Учреждения;
- цель обработки персональных данных и ее правовое основание;
- предполагаемые пользователи персональных данных;
- установленные Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» права субъекта персональных данных.

6.5. Учреждение не имеет права получать и обрабатывать персональные данные Контрагента о его расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, за исключением случаев, предусмотренных законом. В частности, Учреждение вправе обрабатывать указанные персональные данные Контрагента только с его письменного согласия.

6.6. Учреждение не вправе производить обработку данных о судимости

Контрагента.

6.7. К обработке, передаче и хранению персональных данных Контрагента могут иметь доступ работники, перечень которых установлен Приказом Учреждения.

6.8. Обработка персональных данных ведется работниками Учреждения на рабочих местах, выделенных для исполнения ими должностных обязанностей.

6.8. При передаче персональных данных Контрагента Учреждение должно соблюдать следующие требования:

6.8.1. Запрещается передавать персональные данные третьей стороне без письменного согласия субъекта персональных данных, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в случаях установленных законодательством РФ.

6.8.2. Учреждение обязано предупредить лиц, получающих персональные данные Контрагента о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные субъекта персональных данных, обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется в случае обезличивание персональных данных и в отношении общедоступных данных.

6.8.3. Учреждение должен разрешать доступ к персональным данным Контрагентов только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций.

6.8.4. При трансграничной передаче персональных данных Учреждение обязано убедиться в том, что иностранным государством, на территорию которого осуществляется передача персональных данных, обеспечивается адекватная защита прав субъектов персональных данных.

6.9. Все меры конфиденциальности при сборе, обработке и хранении персональных данных сотрудника распространяются как на бумажные, так и на электронные (автоматизированные) носители информации.

6.10. Не допускается отвечать на вопросы, связанные с передачей персональной информации, по телефону или факсу.

6.11. Все факты передачи персональных данных третьим лицам должны учитываться в Журнале учета передачи сведений, содержащих ПДн. В Журнале указывают сведения о поступившем запросе (кто является отправителем запроса, дата его поступления), дату ответа на запрос, данные, какая именно информация была передана, или отметку об отказе в ее предоставлении (в случае трудовых отношений разрешается ограничиваться помещением в личное дело работника выписок, копий документов и т.п., отражающих сведения о поступившем запросе и результатах его рассмотрения). Учет передачи персональных данных разрешается не производить при передаче их в случае, установленном законом, а также при внутренней передаче.

Ответ на запрос подписывается (визуруется) руководителем того структурного подразделения, который отвечает за достоверность содержащихся в них сведений, если иное не предусмотрено законодательством.

6.11. Хранение персональных данных.

6.11.1. Персональные данные Контрагента хранятся на бумажном носителе, а также могут храниться в электронном виде в локальной компьютерной сети.

6.11.2. По возможности персональные данные обезличиваются.

6.11.3. При выполнении работ, связанных с использованием персональных данных Контрагента, персональные данные, зафиксированные на бумажном носителе подлежат хранению в структурном подразделении Учреждения, осуществляющем текущую работу, после выполнения работ документы, содержащие персональные данные хранятся в Архиве Учреждения, в соответствии с установленным порядком хранения документов и утвержденной номенклатурой дел в Учреждении.

6.13. Доступ к электронным базам данных, содержащим персональные данные Контрагента, обеспечивается паролями.

6.14. Пароли сообщаются индивидуально работникам Учреждения, имеющим доступ к персональным данным Контрагентов. Изменение паролей происходит в соответствии с Инструкцией об организации парольной защиты в информационной системе персональных данных.

6.15. Для обеспечения хранения персональных данных необходимо выполнить следующие шаги:

- при работе с Контрагентом, работник Учреждения, осуществляющий обработку персональных данных не должен выполнять функции, не связанные с приемом, вести служебные и личные переговоры по телефону. На его столе не должно быть никаких документов, кроме тех, которые касаются данного Контрагента.

- не допускается отвечать на вопросы, связанные с передачей персональных данных по телефону.

- сотрудникам Учреждения не разрешается при выходе из помещения оставлять какие-либо документы, содержащие персональные данные, на рабочем столе или оставлять шкафы незапертыми.

- на рабочем столе сотрудника должен всегда находиться только тот массив документов и учетных карточек, с которым в настоящий момент он работает. Другие документы, дела, карточки, журналы должны находиться в запертом шкафу. Исполняемые документы не разрешается хранить в россыпи. Их следует помещать в папки, на которых указывается вид производимых с ними действий (подшивка в дела, для отправки и пр.).

- в конце рабочего дня все документы, дела, листы бумаги и блокноты с рабочими записями, инструктивные и справочные материалы должны быть убраны в шкафы, сейфы. На рабочем столе не должно оставаться ни одного документа, содержащего персональные данные. Черновики и редакции документов, испорченные бланки, листы со служебными записями в конце рабочего дня уничтожаются.

- документы, содержащие персональные данные Контрагента, журналы и книги учета, с которыми не выполняются работы, хранятся в рабочее и нерабочее время в Архиве Учреждения.

- Архив Учреждения, ежедневно открывается и закрывается архивариусами,

или уполномоченным начальником сотрудником отдела.

- Проведение уборки помещения, в которых хранятся персональные данные должно производиться в присутствии работников соответствующих отделов.

7. Доступ к персональным данным Контрагента

7.1. Внутренний доступ (доступ внутри Учреждения).

7.1.1. Право доступа к персональным данным Контрагента имеют:

- руководитель Учреждения;
- начальники отделов и подразделений;
- сотрудники отделов Учреждения, непосредственно связанные с обработкой персональных данных, в соответствии с должностными обязанностями.

7.1.2. К хранению персональных данных имеют доступ сотрудники Архива Учреждения.

7.1.3. Другие сотрудники Учреждения имеют доступ к персональным данным Контрагента только при наличии специального указания в письменном согласии руководителя Учреждения, если эти персональные данные необходимы для выполнения функций, возложенных на сотрудника Учреждения.

7.1.4. При получении доступа к персональным данным, хранящимся в электронном виде, сотрудник Учреждения должен ввести соответствующий пароль, обеспечивающий вход в систему.

7.1.5. Получение доступа к персональным данным, хранящихся на бумажном носителе, в соответствии с локальным актом Учреждения, устанавливающим порядок выдачи дел из Архива.

7.2. Внешний доступ.

7.2.1. Доступ Контрагента к своим персональным данным предоставляется при обращении либо при получении запроса Контрагента. Учреждение обязано сообщить Контрагенту информацию о наличии персональных данных о нем, а также предоставить возможность ознакомления с ними в течение десяти рабочих дней с момента обращения.

7.2.2. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись субъекта персональных данных или его законного представителя.

7.2.3. Контрагент имеет право на получение при обращении или при получении запроса информации, касающейся обработки его персональных данных, в том числе содержащей:

- подтверждение факта обработки персональных данных Учреждением, а также цель такой обработки;
- способы обработки персональных данных, применяемые Учреждением;
- сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;
- перечень обрабатываемых персональных данных и источник их получения;

- сроки обработки персональных данных, в том числе сроки их хранения;
- сведения о том, какие юридические последствия для Контрагента может повлечь за собой обработка его персональных данных.

2.4. Сведения о наличии персональных данных должны быть предоставлены Контрагента в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных.

2.5. Право Контрагента на доступ к своим персональным данным ограничивается в случае, если предоставление персональных данных нарушает конституционные права и свободы других лиц.

2.6. Персональные данные Контрагента могут быть предоставлены третьим лицам только с письменного согласия Контрагента либо в соответствии с действующим законодательством РФ.

2.7. Учреждение обеспечивает ведение журнала учета выданных персональных данных Контрагента, в котором фиксируются сведения о лице, которому передавались персональные данные Контрагента, дата передачи персональных данных или дата уведомления об отказе в предоставлении персональных данных, а также отмечается, какая именно информация была передана.

2.8. Сведения о персональных данных, либо документы, содержащие персональные данные Контрагента, могут предоставляться по письменным запросам органов, в полномочия которых в соответствии с действующим законодательством РФ входит получение, в том числе, информации о персональных данных (правоохранительные органы, суды и т.п.)

8. Защита персональных данных

8.1. Защита персональных данных субъектов от неправомерного их использования или утраты обеспечивается Учреждением, в установленном действующем законодательством и локальными актами Учреждения порядке, выполнением комплекса организационно-технических мер, обеспечивающих их безопасность.

8.2. Под угрозой или опасностью утраты персональных данных понимается единичное или комплексное, реальное или потенциальное, активное или пассивное проявление злоумышленных возможностей внешних или внутренних источников угрозы создавать неблагоприятные события, оказывать дестабилизирующее воздействие на защищаемую информацию.

8.2. Риск угрозы любым информационным ресурсам создают стихийные бедствия, экстремальные ситуации, террористические действия, аварии технических средств и линий связи, другие объективные обстоятельства, а также заинтересованные и незаинтересованные в возникновении угрозы лица.

8.3. Защита персональных данных представляет собой жестко регламентированный и динамически развивающийся технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и, в конечном счете, обеспечивающий достаточно надежную безопасность информации в процессе

управленческой и производственной деятельности Учреждения.

8.4. Для защиты персональных данных Контрагентов необходимо соблюдение ряда мер:

- рационально размещать рабочие места работников, при которых исключалось бы бесконтрольное использование защищаемой информации;
- не допускать выдачи документов, содержащих персональные данные лицам, в служебные обязанности которых не входит работа с Контрагентами.
- документы, содержащие персональные данные должны храниться в надежно запираемых хранилищах, а также в незапираемых шкафах, при условии, что бесконтрольный доступ посторонних лиц в хранилища (кабинеты) исключен.
- хранение персональных данных в структурных подразделениях Учреждения, сотрудники которых имеют доступ к персональным данным, осуществляется в порядке, исключающим к ним доступ третьих лиц.
- организация защиты персональных данных в Информационных системах Учреждения осуществляется в рамках действующей системы защиты информации. Доступ к Информационным системам Учреждения, содержащим персональные данные, обеспечиваются системой паролей, а так же программно-техническими средствами защиты информации.
- помещения, в которых ведется обработка персональных данных, должны обеспечивать их сохранность, исключать возможность бесконтрольного проникновения в них посторонних лиц.
- в течение рабочего дня ключи от шкафов (ящиков, хранилищ), в которых содержатся персональные данные, а также помещений, где находятся средства вычислительной техники, предназначенные для обработки персональных данных, находятся на хранении у ответственных работников.
- по окончании рабочего времени помещения, предназначенные для обработки персональных данных должны быть закрыты на ключ, бесконтрольный доступ в такие помещения должен быть исключен (например применением опечатывания, видеонаблюдения или систем контроля доступа).

8.5. Хранение персональных данных должно происходить в порядке, исключающем их утрату или их неправомерное использование.

8.6. При принятии решений, затрагивающих интересы субъекта, Предприятие не имеет права основываться на персональных данных субъекта, полученных исключительно в результате их автоматизированной обработки или электронного получения.

8.7. Все меры конфиденциальности при сборе, обработке и хранении персональных данных работника распространяются как на бумажные, так и на электронные носители информации.

8.8. Внутренняя защита.

8.9.1. Защита данных на бумажных носителях:

- установка несгораемых сейфов, хранение документов в Архиве.

8.9.2. Защита информации на электронных носителях.

- Установка паролей;

9.10. Внешняя защита.

- Система контроля доступа;

- Пультовая охрана;
- Пожарная сигнализация, система порошкового пожаротушения.

9. Уточнение, блокирование и уничтожение персональных данных

9.1. Блокирование информации, содержащей персональные данные Контрагента, производится в случае:

- если персональные данные являются неполными, устаревшими, недостоверными;
- если сведения являются незаконно полученными или не являются необходимыми для заявленной цели обработки.

9.2. В случае подтверждения факта недостоверности персональных данных Учреждение на основании документов, представленных Контрагентом, уполномоченным органом по защите прав субъектов персональных данных или полученных в ходе самостоятельной проверки, обязан уточнить персональные данные и снять их блокирование.

9.3. В случае выявления неправомерных действий с персональными данными Учреждение обязано устранить допущенные нарушения. В случае невозможности устранения допущенных нарушений оператор в срок, не превышающий трех рабочих дней с даты выявления неправомерности действий с персональными данными, обязан уничтожить персональные данные.

9.4. Об устранении допущенных нарушений или об уничтожении персональных данных Учреждение обязан уведомить Контрагента, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

9.5. Учреждение обязан уничтожить персональные данные Контрагента в случае:

- достижения цели обработки персональных данных, с соблюдением условий, установленных в пункте 9.6 настоящего Положения.
- отзыва Контрагентом согласия на обработку своих персональных данных.

9.6. Персональные данные уничтожаются по истечении следующих сроков:

- при заключении договора, по истечении 5 (пяти) лет с момента окончания срока действия договора,
- при подаче заявлений на оказание услуги, по истечении 5 лет, с даты получения Учреждением, соответствующего заявления.
- при получении запросов, жалоб, претензий, по истечении 5 лет, с даты получения Учреждением, соответствующего запроса, жалобы, претензии.

9.7. Уничтожение персональных данных должно быть осуществлено в течение 30 дней с указанных моментов. Соглашением Учреждения с Контрагентом могут быть установлены иные сроки уничтожения персональных данных при достижении цели обработки персональных данных.

9.8. Сведения и документы, содержащие персональные данные (технические паспорта, оценочная и иная учетно-техническая документация по объектам капитального строительства, включая регистрационные книги, реестры, копии зарегистрированных документов, сформированные в инвентарные дела, образующие архивные фонды, которые относятся к государственной части

Архивного фонда Российской Федерации), хранятся и уничтожаются в соответствии с законодательством об архивном деле.

10. Ответственность за разглашение персональных данных и нарушение

10.1. Учреждение ответственен за персональную информацию, которая находится в его распоряжении и закрепляет персональную ответственность сотрудников за соблюдение установленных в организации принципов уважения приватности.

10.2. Работники Учреждения, которым персональные данные становятся известными в связи с исполнением должностных обязанностей, принимают на себя обязательства и несут ответственность за обеспечение конфиденциальности действий с этими персональными данными.

10.4. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, в соответствии с федеральными законами несут дисциплинарную, административную, гражданско-правовую, уголовную ответственность.

11. Заключительные Положения

11.1. С работниками, которые в силу своих должностных обязанностей, осуществляют обработку персональных данных Контрагентов, или имеют доступ к персональным данным, заключается Соглашение об обязательствах неразглашения сведений конфиденциального характера и информации ограниченного распространения. Экземпляр соглашения хранится в личном деле работника Учреждения.

11.2. Работники должны быть ознакомлены под роспись с документами Учреждения, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области. Об ознакомлении с настоящим положением вновь принятого работника, делается отдельная запись в тексте трудового договора с работником.

11.3. Каждый работник Учреждения, получающий для работы конфиденциальный документ, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

11.4. Работники Учреждения, которым сведения о персональных данных стали известны в силу их служебного положения, несут ответственность за их разглашение.

11.5. Обязательства по соблюдению конфиденциальности персональных данных остаются в силе и после окончания работы с ними вышеуказанных лиц.

11.6. За неисполнение или ненадлежащее исполнение работником по его вине возложенных на него обязанностей по соблюдению установленного порядка работы со сведениями конфиденциального характера работодатель вправе применять предусмотренные Трудовым Кодексом дисциплинарные взыскания.

11.7. Ответственность за соблюдение вышеуказанного порядка обработки персональных данных несет работник, а также руководитель структурного

подразделения, осуществляющего обработку персональных данных.

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

11.9. Настоящее положение вступает в силу с момента его утверждения руководителем и вводится в действие приказом руководителя Учреждения.

Приложение №1

Я, _____,

паспорт серии _____ № _____ выдан _____

дата _____ выдачи _____, место _____ регистрации _____

В соответствии со статьей 9 Федерального закона от 27 июля 2006 года №152-ФЗ «О персональных данных», даю согласие: ГКУ ТО «Центр хранения учетно-технической документации», расположенному по адресу: город Тюмень, улица 50 лет Октября, дом 576, на смешанную обработку (автоматизированную, а также без использования средств автоматизации), включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение, следующих моих персональных данных: фамилия, имя, отчество (в том числе прежние), год, месяц, дата и место рождения; паспортные данные или данные иного документа, удостоверяющего личность и гражданство; адрес места жительства (место регистрации и фактический адрес) и дата регистрации по месту жительства или по месту пребывания; номера телефонов (мобильного и домашнего) и иных сведений, предоставленных мною в ГКУ ТО «Центр хранения учетно-технической документации» в целях исполнения ГКУ ТО «Центр хранения учетно-технической документации» государственной услуги.

Также даю согласие на передачу ГКУ ТО «Центр хранения учетно-технической документации» моих персональных данных ГКУ ТО «Фонд имущества Тюменской области», расположенному по адресу: г. Тюмень, улица Водопроводная 12, в целях учета взимания (поступления) платы в рамках предоставления государственной услуги.

Настоящее согласие даю на срок, необходимый для предоставления ГКУ ТО «Центр хранения учетно-технической документации» мне государственной услуги.

Я оставляю за собой право отозвать настоящее согласие посредством составления соответствующего письменного документа, который может быть направлен мной в адрес ГКУ ТО «Центр хранения учетно-технической документации» по почте заказным письмом с уведомлением о вручении либо вручен лично под расписку представителю ГКУ ТО «Центр хранения учетно-технической документации».

В случае отзыва мною настоящего согласия ГКУ ТО «Центр хранения учетно-технической документации» обязан прекратить обработку персональных данных и уничтожить персональные данные в срок, предусмотренный действующим законодательством. Вместе с тем ГКУ ТО «Центр хранения учетно-технической документации» вправе продолжить обработку персональных данных без согласия при наличии оснований, указанных в Федеральном законе от 27.07.2006 № 152-ФЗ «О персональных данных». Уничтожению не подлежат те персональные данные, которые ГКУ ТО «Центр хранения учетно-технической документации» обязан хранить в соответствии с действующим законодательством.

« _____ » _____ 20 ____ г. _____ (подпись) _____ (расшифровка подписи)

Инструкция о порядке учета, хранения и уничтожения носителей персональных данных в ГКУ ТО «Центр хранения учетно-технической документации»

1. Общие положения

1.1. Настоящая Инструкция разработана в целях обеспечения выполнения требований «Положения о порядке обработке персональных данных при их обработке в информационных системах персональных данных», утвержденного Постановлением Правительства РФ от 17 ноября 2007 г. №781, «Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утвержденного Постановлением Правительства РФ от 15 сентября 2008 г. №687 и «Требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных» утвержденных Постановлением Правительства от 06.07.08 №512.

1.2. Настоящая Инструкция устанавливает порядок учета, хранения и уничтожения носителей информации, а также носителей информации на бумажной основе, относящейся к персональным данным в соответствии с законодательством Российской Федерации.

1.3. Настоящая Инструкция является локальным нормативным актом ГКУ ТО «Центр хранения учетно-технической документации» (далее – Учреждение) и вступает в силу с момента подписания руководителем Учреждения приказа об ее утверждении.

1.4. Для целей настоящей инструкции используются термины и определения:

Информационная система персональных данных - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Контролируемая зона – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

Конфиденциальность персональных данных - обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, осуществляемые с нарушением

установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своим функциональному назначению и техническим характеристикам.

Обработка персональных данных - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Персональные данные - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Уничтожение персональных данных - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

2. Мероприятия по контролю за выполнением инструкции.

2.1. В целях контроля выполнения требований, установленных настоящей Инструкцией, проводится периодический контроль.

2.2. Периодичность контроля, а также лица, ответственные за его проведение назначаются приказом руководителя Учреждения.

3. Материальные носители информации

3.1. В настоящей инструкции рассматриваются следующие виды материальных носителей информации:

- носители информации;
- носители информации на бумажной основе.

3.2. Носители информации. Носители информации (далее – НИ) – изделия и устройства, предназначенные для записи и обработки информации в составе средств вычислительной техники, а также для хранения и перемещения записанной информации за пределы состава средств вычислительной техники.

Виды носителей информации:

- жесткие магнитные диски;
- гибкие магнитные диски;
- оптические и магнитооптические диски;
- устройства долговременной электронной памяти (Flash Memory);
- магнитные ленты.

Типы носителей информации:

- съемные, носители информации, устанавливаются и/или подключаются к средствам вычислительной техники на время сеанса работы пользователя, а по

окончанию его снимаются и хранятся в оборудованном хранилище;

- несъемные, носитель информации в процессе работы пользователя не снимается и не изымается из состава средств вычислительной техники автоматизированной системы и находится там постоянно.

3.3. Носители информации на бумажной основе.

Носители информации на бумажной основе – материальные носители графической и буквенно-цифровой информации отраженной (зафиксированной) на бумаге.

К носителям информации на бумажной основе относятся:

- личные дела работников (пакет анкетно-биографических и характеризующих работника материалов);

- другие документы, содержащие персональные данные (далее - ПДн) субъектов персональных данных.

4. Порядок учета носителей информации

4.1. Учет носителей информации

Все НИ, предназначенные для обработки ПДн подлежат учету. Учет всех видов и типов НИ производится в журнале учета машинных носителей информации. Допускается ведение электронного журнала учета. Для ведения электронного журнала учета может применяться специализированное программное обеспечение. Ответственность за ведение журнала возлагается на начальника отдела учетно-технической документации.

4.2. В журнал заносятся следующие данные регистрации:

- Регистрационный номер;
- Дата учета;
- Тип/емкость носителя;
- Серийный номер;
- Отметка о постановке на учет (ФИО, подпись, дата);
- Отметка о снятии с учета (ФИО, подпись, дата);
- Местоположение носителя;
- Сведения об уничтожении носителя/стирания информации.

4.3. Каждому НИ присваивается уникальный идентификационный номер. Допускается в качестве идентификационного номера использовать серийный номер НИ. В случае отсутствия возможности использования серийного номера изделия, идентификационный номер наносится на несъемную часть корпуса НИ.

НИ могут сниматься с учета в случае уничтожения (стирания) с них информации (ПДн).

Гарантированное уничтожение информации, может быть произведено с использованием специализированных программных или программно-аппаратных средств, производящих несколько циклов перезаписи случайных последовательностей на все пространство носителя.

В случае передачи НИ содержащих ПДн на постоянной основе (в компании-партнеры, государственные учреждения и организации), об этом делается соответствующая запись в журнале учета носителей информации.

5. Учет носителей информации на бумажной основе

5.1. Учет личных дел работников Учреждения осуществляется работниками, ответственными за документационное обеспечение кадровой деятельности Учреждения.

5.2. Учет документов, содержащих персональные данные граждан – клиентов Учреждения, осуществляется структурными подразделениями в соответствии с утвержденной в Учреждении номенклатурой дел, и установленным порядком работы в Учреждении.

6. Правила хранения носителей информации

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

6.2. Хранение НИ должно осуществляться в условиях, соответствующих техническим условиям заводов-изготовителей НИ.

6.3. Недопустимо воздействие на НИ теплового, светового (ультрафиолетового) и ионизирующего излучений. Также недопустимо размещение мест хранения НИ вблизи источников электромагнитных колебаний (телефоны, электродвигатели, кабели и т.п.).

6.4. Необходимо обеспечивать отдельное хранение ПДн (материальных носителей ПДн на бумажной основе), обработка которых осуществляется в различных целях.

6.5. Места хранения материальных носителей ПДн утверждаются приказом.

6.6. Для хранения материальных носителей ПДн используются специально оборудованные хранилища (сейфы, шкафы, и т.п.), исключающие возможность несанкционированного копирования информации и хищения носителей.

6.7. Резервные копии не выдаются для работы обычным пользователям и служат только для восстановления НИ в случае аварии или поломки рабочего носителя.

6.8. НИ с резервными копиями рекомендуется хранить в отдельном хранилище.

6.9. Хранение носителей информации на бумажной основе осуществляется в соответствии с порядком, установленным локальными актами Учреждения, и утвержденной номенклатурой дел в Учреждении.

7. Порядок уничтожения носителей информации

7.1. Носители ПДн подлежат уничтожению в следующих случаях:

- при достижении целей обработки или в случае утраты необходимости в их достижении, для носителей, уничтожение ПДн на которых невозможно без уничтожения самого носителя;

- выхода из строя, повреждение носителя ПДн, в результате которого невозможно осуществлять корректную обработку ПДн с использованием данного носителя ПДн;

- возникновения иных обстоятельств, в результате которых необходимо уничтожить носители ПДн.

7.2. Уничтожение материальных носителей ПДн должно осуществляться только

по решению комиссии, назначенной приказом руководителя Учреждения, в соответствие с требованиями Федерального закона от 27.08.2006 № 152-ФЗ "О персональных данных".

Уничтожение материальных носителей ПДн должно обеспечивать полное физическое и не восстановимое уничтожение ПДн, содержащихся на таких носителях.

7.3. Работник, ответственный за учет носителей ПДн делает в журнале учета соответствующую отметку.

7.4. Персональные данные, находящиеся в информационных системах, после достижения целей обработки должны быть удалены из ИСПДн. Удаление должно обеспечить полное физическое и не восстановимое уничтожение ПДн.

7.5. Уничтожение носителей информации. НИ, пришедшие в негодность, отслужившие установленный срок или утратившие практической значение, подлежат уничтожению. Уничтожение носителей информации оформляется соответствующим актом.

7.6. Уничтожение носителей информации на бумажной основе. Носители ПДн на бумажной основе подлежат уничтожению в случае достижения целей обработки ПДн, и в соответствии с утвержденной номенклатурой дел в Учреждении. Уничтожение носителей информации на бумажной основе оформляется актом об уничтожении, либо актом о выделении к уничтожению документов, не подлежащих хранению, в соответствии с порядком, определенным локальными актами Учреждения.

8. Права и обязанности работников при обращении с носителями информации

8.1. Запрещается выносить носители ПДн из служебных помещений (за пределы контролируемой зоны) для работы с ними на дому, в гостиницах, общественном транспорте и т.д.

8.2. Запрещается записывать на НИ, предназначенные для хранения ПДн, любые иные данные, не имеющие отношения к ПДн.

8.3. Запрещается принимать и передавать НИ без соответствующего разрешения и оформления в установленном порядке.

8.4. Работники, осуществляющие работу с НИ, обязаны работать только с вверенными ему НИ. Самовольная передача НИ другим работникам запрещается.

8.5. Запрещается хранить НИ и носители информации на бумажной основе на рабочих столах, либо оставлять их без присмотра.

8.6. Лица (подразделения), назначенные ответственными за организацию учета и использования НИ, должны пресекать действия работников и других лиц, которые могут привести к хищению или разрушению носителей информации, и сообщать о фактах таких действий вышестоящему руководству.

8.7. О фактах утраты носителей информации немедленно должны быть поставлены в известность лица (подразделения), назначенные ответственными за организацию учета и использования НИ.

9. Проведение отладочных и ремонтных работ

9.1. При проведении технического обслуживания и ремонта запрещается передавать ремонтным организациям узлы и блоки с элементами накопления и хранения ПДн. Отладочные и экспериментальные работы (опробование программ, формирование массивов информации и др.) проводятся с использованием информации, не содержащей ПДн, либо при условии их обезличивания.

9.2. В случае, когда для проведения технического обслуживания, ремонта, отладочных и экспериментальных работ необходимо привлекать сторонние организации, допускается проведение таких работ в присутствии работников ответственных за обеспечение безопасности ПДн.

9.3. В отдельных случаях, когда восстановление информации на неисправном носителе жизненно важно для деятельности Учреждения, допускается осуществлять ремонт таких носителей силами сторонних организаций без предварительного уничтожения персональных данных. Ремонт должен происходить в присутствии работников, ответственных за обеспечение безопасности ПДн.

10. Ответственность

10.1. Персональную ответственность за обеспечение режима безопасности при выполнении непосредственных работ с материальными носителями несет исполнитель, выполняющий эту работу.

10.2. По фактам и попыткам несанкционированного доступа к информации на материальных носителях, а также в случаях утечки или уничтожения обрабатываемых персональных данных, проводятся служебные расследования.

Приложение №1 к Инструкции о порядке учета, хранения и уничтожения носителей персональных данных

Разрешаю уничтожить
Ответственный за обеспечение безопасности персональных данных

« ___ » _____ 20__ г.

Акт об уничтожении персональных данных, зафиксированных в информационных системах персональных данных

Комиссия в составе:

	Ф.И.О.	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 подлежит уничтожению _____ (цифрами и прописью) носителей.

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.)

Уничтоженные носители с книг и журналов учета списаны.

Председатель комиссии:

Члены комиссии:

_____/ /
_____/ /
_____/ /

ИНСТРУКЦИЯ
для работников ГКУ ТО «Центр хранения учетно-технической
документации», осуществляющих обработку персональных данных
субъектов персональных данных по правилам обработки, хранения и
передачи персональных данных

I. Общие положения.

Нормативной базой, регламентирующей положения настоящей Инструкции, является статья 24 Конституции Российской Федерации, глава 14 Трудового кодекса Российской Федерации, статья 137 Уголовного кодекса Российской Федерации.

II. К персональным данным контрагента, необходимым ГКУ ТО «Центр хранения учетно-технической документации» (далее - Учреждение) в связи с оказанием государственной услуги относятся:

- фамилия, имя, отчество;
- год, месяц, дата рождения;
- пол;
- место жительства, в том числе сведения о регистрации по месту жительства;
- реквизиты документа, удостоверяющего личность;
- номера телефона (любого иного вида связи);
- идентификационный номер налогоплательщика (ИНН);
- иные сведения и документы, идентифицирующие субъект персональных данных, которые могут быть получены для исполнения Филиалом, возложенных на него обязательств.

III. Порядок обработки персональных данных

3.1. При обработке персональных данных субъекта, то есть их получении, хранении, комбинировании, передаче или любом другом использовании персональных данных контрагента, сотрудники Учреждения, осуществляющие обработку персональных данных обязаны соблюдать следующие общие требования:

3.2. Обрабатывать персональные данные контрагента можно исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, исполнения договорных обязательств, и в случаях установленных действующим законодательством РФ;

3.3. Все персональные данные контрагента следует получать у него самого. Если персональные данные контрагента, возможно, получить только у третьей стороны, то контрагент должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие;

Допускается обработка персональных данных без согласия субъекта персональных данных, в случаях:

- обработка персональных данных необходима для достижения целей, предусмотренных законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;
- обработка персональных данных осуществляется в целях исполнения договора, одной из сторон которого является контрагент;
- обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;
- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов контрагента, если получение его согласия невозможно;
- в иных случаях, предусмотренных действующим законодательством Российской Федерации.

3.4. Сотрудник Учреждения не имеет права получать и обрабатывать персональные данные контрагента о его политических, религиозных и иных убеждениях и частной жизни, членстве в общественных объединениях или его профсоюзной деятельности, а также случаев предусмотренных федеральным законом;

3.5. Персональную ответственность за соблюдение всеми сотрудниками Филиала, участвующими в обработке персональных данных контрагентов, настоящей Инструкции, а также контроль за ее соблюдением возложен на начальников отделений, начальников структурных подразделений, в которых производится обработка персональных данных.

IV. Хранение персональных данных контрагентов

Хранение документов содержащих персональные данные контрагентов осуществляется в шкафах, (сейфах), в запираемых кабинетах. Другие сотрудники могут использовать данные документы только с разрешения вышеназванных лиц. По окончании работы с бумажными носителями, содержащими персональные данные, документы сдаются в архив на хранение.

V. Передача персональных данных контрагентов

5.1. При передаче персональных данных контрагента сотрудник Учреждения должен соблюдать следующие требования:

5.2. Не сообщать персональные данные контрагента третьей стороне без письменного согласия контрагента, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта персональных данных, а также в случаях, установленных действующим законодательством.

5.3. Сотруднику Филиала разрешается доступ только к тем персональным данным, которые необходимы для выполнения им его должностных обязанностей;

VI. Ответственность.

Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

ИНСТРУКЦИЯ

для работников осуществляющих кадровое делопроизводство по правилам обработки, хранения и передачи персональных данных работника

I. Общие положения.

Нормативной базой, регламентирующей положения настоящей Инструкции, является статья 24 Конституции Российской Федерации, глава 14 Трудового кодекса Российской Федерации, статья 137 Уголовного кодекса Российской Федерации.

II. К персональным данным работника, необходимым работодателю в связи с трудовыми отношениями относятся:

- фамилия, имя, отчество;
- год, месяц, дата и место рождения;
- пол;
- гражданство;
- реквизиты документов об образовании и приложения к ним;
- стаж работы;
- место жительства, в том числе сведения о регистрации по месту жительства;
- место пребывания;
- место работы;
- занимаемая должность;
- реквизиты документа, удостоверяющего личность;
- номера телефона (любого иного вида связи);
- сведения о воинском учете;
- реквизиты полиса обязательного медицинского страхования;
- номер страхового свидетельства государственного пенсионного страхования;
- идентификационный номер налогоплательщика;
- документы, подтверждающие рождение ребенка;
- сведения об учебе;
- сведения о награждении;
- данные о трудовой деятельности (наименование организации, должности, периоды: даты поступления, ухода; местонахождение организации);
- сведения о семейном положении и их основания (свидетельство о заключении брака, о расторжении брака и иное, подтверждающее статус семейного положения), состав семьи;
- специальные категории персональных данных, касающихся состояния здоровья, которые относятся к вопросу о возможности выполнения трудовой функции.

III. Порядок обработки персональных данных работника.

3.1. При обработке персональных данных работника то есть их получении, хранении, комбинировании, передаче или любом другом использовании персональных данных работника, сотрудники отдела кадров обязаны соблюдать следующие общие требования:

3.2. Обрабатывать персональные данные работника можно исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества;

3.3. 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;

3.4. Сотрудник отдела кадров не имеет права получать и обрабатывать персональные данные работника о его политических, религиозных и иных убеждениях и частной жизни, членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев непосредственно связанных с вопросами трудовых отношений с письменного согласия работника, а также случаев предусмотренных федеральным законом;

3.5. Персональную ответственность за соблюдение всеми сотрудниками отдела кадров настоящей Инструкции, а также контроль за ее соблюдением возложен на начальника отдела кадров.

3.6. Все сотрудники отдела кадров должны быть ознакомлены с настоящей Инструкцией.

IV. Хранение персональных данных работников.

Хранение документов содержащих персональные данные работников осуществляется в негорюемых шкафах (сейфах), ключи от которых находятся у руководителя, а в его отсутствие у лица его замещающего.

V. Передача персональных данных работника.

5.1. При передаче персональных данных работника сотрудник ответственный за кадровое делопроизводство должен соблюдать следующие требования:

5.2. Не сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в случаях, установленных федеральным законом, а также не сообщать соответствующие сведения в коммерческих целях без письменного согласия работника;

5.3. При передаче персональных данных работников предупредить лиц, получающих персональные данные работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены.

5.4. Сотруднику ответственному за кадровое делопроизводство разрешается доступ только к тем персональным данным работников, которые необходимы для выполнения им его должностных обязанностей;

5.5. Сотрудник ответственный за кадровое делопроизводство не имеет права запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции;

VI. Ответственность.

Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

**ПЕРЕЧЕНЬ СВЕДЕНИЙ, СОСТАВЛЯЮЩИХ ПЕРСОНАЛЬНЫЕ ДАННЫЕ,
 ОБРАБАТЫВАЕМЫХ В ГКУ ТО «Центр хранения учетно-технической документации»**

№№ п/п	Наименование структурного подразделения	Категории субъектов ПДн	Описание обработки ПДн, источники ПДн, используемые носители ПДн
1.	Лицо, ответственное за кадровое делопроизводство	Персональные данные работников	<ul style="list-style-type: none"> - фамилия, имя, отчество; - пол; - дата и место рождения; - адрес места по прописке; - адрес проживания; - номера телефонов (домашний, сотовый) - гражданство; - паспортные данные; - ИНН; - свидетельство ОПС; - семейное положение; - сведения об образовании, повышении квалификации, профессиональной подготовке, ученая степень; - трудовой стаж; - награждения, поощрения; - сведения о воинском учете. - Трудовая книжка; - Приказы (распоряжения) по личному составу. - Сведения о трудовом договоре.
2.	Бухгалтерия	Персональные данные работников	<p>Оформление банковской карточки работника на основании письменного заявления, содержащего:</p> <p>Ф.И.О.; серия, номер паспорта.</p> <p>Составление и сдача отчетности в ИФНС, ПФР в электронном и бумажном виде, содержащей:</p> <ul style="list-style-type: none"> - Паспортные данные; - ИНН (Свидетельство о постановке на налоговый учет); - номер свидетельства ОПС; - образование/специальность; - данные по выплатам;

№№ п/п	Наименование структурного подразделения	Категории субъектов ПДн	Описание обработки ПДн, источники ПДн, используемые носители ПДн
			<ul style="list-style-type: none"> - система оплаты, оклад, аванс, ставка, стаж. <p>Расчет заработной платы работников:</p> <ul style="list-style-type: none"> - Ф.И.О.; <ul style="list-style-type: none"> - серия, номер паспорта; - должность, оклад - приказы (распоряжения) по личному составу - сведения о трудовом договоре.
		Персональные данные контрагентов	<p>Получение сведений о контрагентах определяется формой запроса.</p> <p>Сведения о физическом лице:</p> <ul style="list-style-type: none"> - Ф.И.О. - информация о паспортных данных; - ИНН (Свидетельство о постановке на налоговый учет);
		Персональные данные работников	<p>Расчет заработной платы работников:</p> <ul style="list-style-type: none"> - Ф.И.О.; <ul style="list-style-type: none"> - должность, оклад. - приказы по личному составу;

№№ п/п	Наименование структурного подразделения	Категории субъектов ПДн	Описание обработки ПДн, источники ПДн, используемые носители ПДн
3	Отдел учетно- технической документации	Персональные данные контрагентов	<p>Получение сведений о контрагентах определяется формой договора (заявлением).</p> <p>Сведения о физическом лице:</p> <ul style="list-style-type: none"> - Ф.И.О. - информация о паспортных данных; - ИНН (Свидетельство о постановке на налоговый учет); - Сведения о собственности (при необходимости); <p>Иные сведения, позволяющие идентифицировать субъекта персональных данных.</p> <p>Хранение, выдача, уничтожение документов, содержащих ПДн на бумажных носителях</p>
4	Все подразделения	<p>Персональные данные работников</p> <p>Персональные данные контрагентов</p>	<p>Общедоступные ПДн работников:</p> <ul style="list-style-type: none"> - Ф.И.О.; - структурное подразделение, должность; - внутренний телефон <p>Общедоступные ПДн контрагентов:</p> <ul style="list-style-type: none"> - Ф.И.О.; - место работы, должность; - контактный телефон

**Перечень работников ГКУ ТО «Центр хранения учетно-технической документации»,
 имеющих доступ к обработке персональных данных с разграничением прав доступа**

Должность	ФИО	Категория	Полномочия	Доступ
Руководитель	Смирнова Анастасия Михайловна	Пользователь с правом записи	Общее руководство	Персональные данные на бумажных носителях: - Пдн контрагентов -Пдн работников
Начальник отдела учетно- технической документации	Филимонцев Алексей Александрович	Пользователь с правом записи	Прием запросов Подготовка ответов, справок, информации по запросам Выдача документов	Персональные данные на бумажных носителях: персональные данные контрагентов
Специалист по запросам (документоведен ие) отдела учетно- технической документации	Уженцев Андрей Борисович Нестерова Светлана Аркадьевна Ермолаева Евгения Сергеевна Черногорцева Ольга Григорьевна Загайнова Виталия Геннадьевна Громова Лариса Михайловна Пригульнова Татьяна Геннадьевна Афониная Ирина Владиславовна	Пользователь с правом записи	Прием запросов Подготовка ответов, справок, информации по запросам Выдача документов	Персональные данные на бумажных носителях: персональные данные контрагентов
Инженер отдела учетно- технической документации	Матвеева Наталья Анатольевна	Пользователь с правом записи	Прием запросов Подготовка ответов, справок, информации по запросам Выдача	Персональные данные на бумажных носителях: персональные данные

			документов	контрагентов
Архивариус отдела учетно- технической документации	Юшкова Сурия Фуатовна Оникиенко Ирина Николаевна Вильцева Нина Михайловна Каранчук Юлия Михайловна Герего Ирина Валентиновна Ганиева Юлия Тальгатовна	Пользователь с правом записи	- Хранение документов в архиве; - Подшивка документов в дела; - Выдача архивных документов в пользование - Уничтожение архивных документов	Персональные данные на бумажных носителях: персональные данные контрагентов
Делопроизводител ь	Косинцева Любовь Геннадьевна	Пользователь с правом записи	Прием запросов Подготовка ответов, справок, информации по запросам Выдача документов Отправка корреспонденции	Персональные данные на бумажных носителях: персональные данные контрагентов

Приложение №8 к
Приказу ГКУ ТО «Центр хранения
учетно-технической документации»
от 04.07.2017 г. № 3/3

Перечень помещений ГКУ ТО «Центр хранения учетно-технической документации», где осуществляется обработка персональных данных

Наименование отдела	№ кабинета	Адрес
Отдел учетно-технической документации	2,4,5 – 2 эт. Кабинет приема запросов — 1 эт.	г. Тюмень, ул. 50 лет Октября, д.57Б
Приемная руководителя, кабинет руководителя	1- приемная — 2 эт.	г. Тюмень, ул. 50 лет Октября, д.57Б

Приложение №9 к
 Приказу ГКУ ТО «Центр хранения
 учебно-технической документации»
 от 04.07.2017 г. № 3/3

Журнал учета машинных носителей информации содержащих персональные данные

Учетный номер	Дата постановки на учет	Подпись принявшего на учет	Вид, модель и серийный номер носителя информации	Отметка о получении носителя	Место установки и использования носителя информации	Категория информации на носителе	Ответственный за хранение	Отметка об обратном приеме	Отметка об отправке*	Дата	Откуда поступил

* Куда направлен, N и дата сопроводительного письма, уничтожения (N и дата акта)
 ** N и дата сопроводительного письма

Приложение №10 к
Приказу ГКУ ТО «Центр хранения
учетно-технической документации»
от 04.07.2017 г. № 3/3

ЖУРНАЛ УЧЕТА ПРОВОДИМЫХ КОНТРОЛЬНЫХ МЕРОПРИЯТИЙ

№ П/П	ФИО контролера	Цель контрольных мероприятий	ФИО проверяемых должностных лиц	Результаты контроля/выявленные замечания	Отметки об устанении замечаний

ЖУРНАЛ УЧЕТА ПРОВОДИМЫХ КОНТРОЛЬНЫХ МЕРОПРИЯТИЙ

Приложение №11 к
Приказу ГКУ ТО «Центр хранения
учетно-технической документации»
от 07.07.2017 г. № 3/3

Журнал учета обращений субъектов персональных данных

№ п/п	Дата, вх. № обращения	Сведения о запрашивающем лице	Краткое содержание обращения	Правовое основание	Принятые меры	Подпись ответственного лица	Дата и исх. № ответа (в делопро-изводстве)

Приложение №13 к
Приказу ГКУ ТО «Центр хранения
учетно-технической документации»
от 07.07.2017 г. № 33

Журнал учета лиц имевших доступ к сведениям ПДн в период трудовой деятельности

№ п/п	Наименование информационной системы ПДн	Период трудовой деятельности (дата, № приказа)		Должность	ФИО
		Принят	Уволен		