



**МИНИСТЕРСТВО
ИМУЩЕСТВА ЧЕЛЯБИНСКОЙ ОБЛАСТИ
ОБЛАСТНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ
«БЮРО ТЕХНИЧЕСКОЙ ИНВЕНТАРИЗАЦИИ
ЧЕЛЯБИНСКОЙ ОБЛАСТИ»**

454080, г. Челябинск, ул. С.Кривой, 75-а, тел./факс 8 (351)232-32-05, E-mail: oblcti@chel.surnet.ru
ОГРН 1247400027533, ИНН/КПП 7453361463 / 745301001

«01 » октября 2024 г.

№ 37

Об утверждении
Положения об обработке
персональных данных
и иных документов в сфере
их защиты

В соответствии с Трудовым кодексом Российской Федерации, частью 3 статьи 18.1 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных», в целях реализации Постановления Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»,

ПРИКАЗЫВАЮ:

1. Утвердить:

1) Положение об обработке персональных данных в областном государственном бюджетном учреждении «Бюро технической инвентаризации Челябинской области» (ПРИЛОЖЕНИЕ № 1);

2) Правила обработки персональных данных в областном государственном бюджетном учреждении «Бюро технической инвентаризации Челябинской области» (ПРИЛОЖЕНИЕ № 2);

3) Положение о порядке обработки персональных данных без использования средств автоматизации в областном государственном бюджетном учреждении «Бюро технической инвентаризации Челябинской области» (ПРИЛОЖЕНИЕ № 3);

4) Инструкцию по учету лиц, допущенных к работе с персональными данными в информационных системах областном государственном бюджетном учреждении «Бюро технической инвентаризации Челябинской области» (ПРИЛОЖЕНИЕ № 4);

5) Инструкцию по работе ответственного лица за организацию обработки персональных данных в областном государственном бюджетном учреждении «Бюро технической инвентаризации Челябинской области» (ПРИЛОЖЕНИЕ № 5);

6) Инструкцию по работе ответственного лица за обеспечение безопасности персональных данных в областном государственном бюджетном учреждении «Бюро технической инвентаризации Челябинской области» (ПРИЛОЖЕНИЕ № 6);

7) Правила рассмотрения запросов субъектов персональных данных или их представителей в областном государственном бюджетном учреждении «Бюро технической инвентаризации Челябинской области» (ПРИЛОЖЕНИЕ № 7);

8) Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и локальными актами областном государственном бюджетном учреждении «Бюро технической инвентаризации Челябинской области» (ПРИЛОЖЕНИЕ № 8);

9) Правила работы с обезличенными данными в областном государственном бюджетном учреждении «Бюро технической инвентаризации Челябинской области» (ПРИЛОЖЕНИЕ № 9);

10) Перечни персональных данных, обрабатываемых в областном государственном бюджетном учреждении «Бюро технической инвентаризации Челябинской области» в связи с реализацией служебных или трудовых отношений, а также в связи с выполнением государственного задания (ПРИЛОЖЕНИЕ № 10);

11) Перечень должностей работников областном государственном бюджетном учреждении «Бюро технической инвентаризации Челябинской области», ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных (ПРИЛОЖЕНИЕ № 11);

12) Инструкцию ответственного за организацию обработки персональных данных в областном государственном бюджетном учреждении «Бюро технической инвентаризации Челябинской области» (ПРИЛОЖЕНИЕ № 12);

13) Типовое обязательство работников областного государственного бюджетного учреждения «Бюро технической инвентаризации Челябинской области», непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним трудового договора прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей (ПРИЛОЖЕНИЕ № 13);

14) Типовую форму согласия на обработку персональных данных работников областного государственного бюджетного учреждения «Бюро технической инвентаризации Челябинской области», иных субъектов персональных данных, а также типовая форма разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные (ПРИЛОЖЕНИЕ № 14);

15) Порядок доступа работников областного государственного бюджетного учреждения «Бюро технической инвентаризации Челябинской области» в помещения, в которых ведется обработка персональных данных (ПРИЛОЖЕНИЕ № 15).

16) Инструкцию по работе со съемными носителями, содержащими персональные данные в областном государственном бюджетном учреждении «Бюро технической инвентаризации Челябинской области» (ПРИЛОЖЕНИЕ № 16).

17) Журнал резервного копирования ИСПДн в областном государственном бюджетном учреждении «Бюро технической инвентаризации Челябинской области» (ПРИЛОЖЕНИЕ № 17).

2. Назначить ответственным за организацию обработки персональных данных в областном государственном бюджетном учреждении «Бюро технической инвентаризации Челябинской области» - Курмашева Д.Р, начальника юридического отдела.

3. Назначить работников областного государственного бюджетного учреждения «Бюро технической инвентаризации Челябинской области» ответственными за обеспечение безопасности и обработку персональных данных в указанных информационных системах персональных данных (далее - ИСПДн):

- 1) Рябушкину О.А., главного бухгалтера (ИСПДн «1С Бухгалтерия»);
- 2) Прядкину О.П., главного специалиста по кадрам (ИСПДн «1С Кадры»);
4. Главному специалисту по кадрам Прядкиной О.П.:
 - 1) Ознакомить с приказом работников Учреждения;
 - 2) Обеспечить внесение изменений в должностные инструкции работников Учреждения в части обеспечения безопасности и обработки персональных данных в информационных системах персональных данных.
5. Контроль за исполнением данного приказа оставляю за собой.

Директор

А.Е. Бобраков

**Положение об обработке персональных данных в областном
государственном бюджетном учреждении
«Бюро технической инвентаризации Челябинской области»**

1. Общие положения

1.1. Настоящее Положение об обработке персональных данных (далее — Положение) в областном государственном бюджетном учреждении «Бюро технической инвентаризации Челябинской области» (далее – Учреждение) разработано в соответствии с Конституцией Российской Федерации от 25.12.1993, Гражданским кодексом Российской Федерации от 30.11.1994 № 51-ФЗ, Федеральным законом «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ, Федеральным законом «О персональных данных» от 27.07.2006 № 152-ФЗ, а также другими нормативно-правовыми актами, действующими на территории Российской Федерации.

1.2. Цель разработки Положения — определение порядка обработки персональных данных граждан, обратившихся в Учреждение и иных субъектов персональных данных, персональные данные которых подлежат обработке на основании полномочий Учреждения; обеспечение защиты прав и свобод человека и гражданина, в т.ч. граждан, обратившихся в Учреждение при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну, а также установление ответственности лиц, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

1.3. К любой информации, содержащей персональные данные субъекта, применяется режим конфиденциальности, за исключением:

- 1.3.1. обезличенных персональных данных;
- 1.3.2. общедоступных персональных данных.

1.4. Режим конфиденциальности персональных данных снимается в случаях их обезличивания и по истечении срока их хранения или продлевается

на основании заключения экспертной комиссии Учреждения, если иное не определено законом Российской Федерации.

2. Термины и определения

2.1. В настоящем документе используются следующие термины и их определения.

Безопасность персональных данных - состояние защищенности персональных данных, характеризующееся способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

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

Доступ к информации - возможность получения информации и ее использования.

Защищаемая информация - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация - присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

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

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

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 распространение без согласия субъекта персональных данных или наличия иного законного основания.

Носитель информации - физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Обезличивание персональных данных — действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

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.

Обработка персональных данных без использования средств автоматизации - обработка персональных данных, при которой такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

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

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

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

Субъект персональных данных - физическое лицо, которое может быть однозначно идентифицировано по персональным данным.

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

Целостность информации - состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право.

3. Состав персональных данных

3.1. Состав персональных данных, обрабатываемых в ИСПДн Учреждения, определяется «Перечнем персональных данных».

3.2. Перечень персональных данных утверждается Директором.

3.3. Директор определяет перечень лиц из числа сотрудников, уполномоченных на обработку персональных данных субъектов, обеспечивающих обработку персональных данных в соответствии с требованиями Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», других нормативных правовых актов Российской Федерации и несущих ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты этих персональных данных.

3.4. Документы со сведениями, содержащими персональные данные, обрабатываются на рабочих местах сотрудников, перечень которых определяется Директором.

3.5. Комплекс документов, сопровождающий процесс оформления трудовых отношений сотрудника Учреждения при его приеме, переводе и увольнении.

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

3.5.1.1. паспорт или иной документ, удостоверяющий личность;

3.5.1.2. трудовую книжку, за исключением случаев, когда трудовой договор заключается впервые или сотрудник поступает на работу на условиях совместительства, либо трудовая книжка у сотрудника отсутствует в связи с ее утратой или по другим причинам;

3.5.1.3. страховое свидетельство государственного пенсионного страхования;

3.5.1.4. документы воинского учета - для военнообязанных и лиц, подлежащих воинскому учету;

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

3.5.1.6. свидетельство о присвоении ИНН (при его наличии у сотрудника).

3.5.2. При оформлении сотрудника в Учреждении заполняется унифицированная форма Т-2 «Личная карточка работника», в которой отражаются следующие анкетные и биографические данные сотрудника:

3.5.2.1. общие сведения (идентификационный номер налогоплательщика, номер страхового свидетельства государственного пенсионного страхования, пол, Ф.И.О. дата рождения, место рождения, гражданство, знание иностранного языка, образование, профессия, стаж работы, состояние в браке, состав семьи, серия, номер и дата выдачи паспорта, наименование органа, выдавшего паспорт, адрес и дата регистрации по месту жительства (месту пребывания), номер телефона); сведения о воинском учете;

3.5.2.2. данные о приеме на работу;

3.5.3. В дальнейшем в личную карточку вносятся:

3.5.3.1. сведения о переводах на другую работу;

3.5.3.2. сведения об аттестации;

3.5.3.3. сведения о повышении квалификации;

3.5.3.4. сведения о профессиональной переподготовке;

3.5.3.5. сведения о наградах (поощрениях), почетных званиях;

3.5.3.6. сведения об отпусках;

3.5.3.7. сведения о наличии/отсутствии судимости;

3.5.3.8. сведения о пребывании за границей, пребывании за границей ближайших родственников (место, время, цель пребывания);

3.5.3.9. сведения о социальных льготах.

3.5.4. В Учреждении создаются и хранятся следующие группы документов, содержащие персональные данные сотрудников в единичном или сводном виде:

3.5.4.1. документы, содержащие персональные данные сотрудников (комплексы документов, сопровождающие процесс оформления трудовых отношений при приеме на работу, переводе, увольнении; комплекс материалов по анкетированию, тестированию, проведению собеседований с кандидатом на должность; подлинники и копии приказов по личному составу; личные дела и трудовые книжки сотрудников; дела, содержащие основания к приказу по личному составу; дела, содержащие материалы аттестации сотрудников; служебных расследований; справочно-информационный банк данных по персоналу (картотеки, журналы); подлинники и копии отчетных, аналитических и справочных материалов, передаваемых руководству Учреждения, руководителям структурных подразделений; копии отчетов, направляемых в государственные органы статистики, налоговые инспекции, вышестоящие органы управления и другие учреждения);

3.5.4.2. документация по Учреждению, работе отделов (положения, должностные инструкции сотрудников, приказы);

3.5.4.3. документы по планированию, учету, анализу и отчетности в части работы с сотрудниками Учреждения.

3.6. Комплект документов, сопровождающий процесс работы гражданами.

3.6.1. Информация, представляемая гражданами либо их законными представителями в структурные подразделения Учреждения, должна иметь документальную форму. Граждане, либо их представители предъявляют следующие документы:

3.6.1.1. оригинал и ксерокопия документа, удостоверяющего личность и подтверждающего гражданство Российской Федерации

3.6.1.2. оригинал и ксерокопия документа, подтверждающего наличие среднего профессионального или высшего образования;

3.6.1.3. справка о наличии (отсутствии) судимости и (или) факта уголовного преследования или о прекращении уголовного преследования;

3.6.1.4. фотография;

3.6.1.5. копия документа, подтверждающего изменение фамилии, имени, отчества;

3.6.1.6. копия страхового свидетельства обязательного пенсионного страхования;

3.6.1.7. иные документы, предусмотренные действующим законодательством.

3.6.2. С целью выполнения обязательств по договорам гражданско-правового характера, в Учреждении обрабатываются следующие категории персональных данных граждан:

3.6.2.1. фамилия, имя, отчество;

3.6.2.2. дата рождения;

3.6.2.3. вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи;

3.6.2.4. адрес прописки, дата регистрации по месту жительства;

3.6.2.5. адрес фактического проживания

3.6.2.6. номер страхового свидетельства государственного пенсионного страхования

3.6.2.7. идентификационный номер налогоплательщика

3.6.2.8. номер контактного телефона или сведения о других способах связи

3.6.3. Данные из документов вносятся сотрудниками в электронном виде в ИСПДн. В бумажном виде впоследствии создаются, хранятся и передаются следующие группы документов, содержащие персональные данные граждан, обратившихся в Учреждение, в единичном или сводном виде

3.6.3.1. справки по месту требования в соответствии с законом;

3.6.3.2. иные документы, предусмотренные действующим законодательством

4. Порядок предоставления доступа к персональным данным

4.1. Допуск к персональным данным субъекта могут иметь только те сотрудники Учреждения, которым персональные данные необходимы в связи с исполнением ими своих трудовых обязанностей.

4.2. Процедура оформления допуска к персональным данным представляет собой следующую строгую последовательность действий:

4.2.1. ознакомление сотрудника под роспись с настоящим Положением, «Перечнем персональных данных...» и другими локальными нормативно-правовыми актами Учреждения, касающимися обработки персональных данных;

4.2.2. истребование с сотрудника «Обязательства о неразглашении информации ограниченного доступа»;

4.3. Каждый сотрудник должен иметь доступ к минимально необходимому набору персональных данных субъектов, необходимых ему для выполнения трудовых обязанностей.

4.4. Сотрудникам, не имеющим надлежащим образом оформленного допуска, доступ к персональным данным субъектов запрещается.

4.5. Любой субъект имеет право, за исключением случаев, предусмотренных законодательством:

4.5.1. на получение сведений о Учреждении в соответствии со ст. 14 № 152-ФЗ от 27.06.2006;

4.5.2. на ознакомление со своими персональными данными;

4.5.3. на уточнение, блокирование или уничтожение своих персональных данных в случае, если они являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленных Учреждением целей обработки.

4.6. В случае если Учреждение на основании договора поручает обработку персональных данных другому лицу, существенным условием договора должна являться обязанность обеспечения указанным лицом конфиденциальности персональных данных и безопасности персональных данных при их обработке.

5. Обработка персональных данных

5.1. Обработка персональных данных граждан, обратившихся в Учреждение, может осуществляться исключительно в целях осуществления деятельности, указанной в Положении о Учреждении, и в случаях, установленных законодательством Российской Федерации.

5.2. При определении объема и содержания обрабатываемых персональных данных Учреждение должно руководствоваться Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным законом «О персональных данных» от 27.07.2006 № 152-ФЗ и иными федеральными законами Российской Федерации.

5.3. Персональные данные субъектов обрабатываются и хранятся в помещениях Учреждения и на учтенных машинных носителях.

5.4. Персональные данные субъектов могут быть получены, обработаны и переданы на хранение как на бумажных носителях, так и в электронном виде - в

локальной компьютерной сети, в компьютерных программах и электронных базах данных.

5.5. При использовании типовых форм документов, обрабатываемых без использования средств автоматизации, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовая форма), должны соблюдаться следующие условия:

5.5.1. типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы), должны содержать:

5.5.1.1. сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации;

5.5.1.2. имя (наименование) и адрес Учреждения;

5.5.1.3. фамилию, имя, отчество и адрес субъекта персональных данных;

5.5.1.4. источник получения персональных данных;

5.5.1.5. сроки обработки персональных данных;

5.5.1.6. перечень действий с персональными данными, которые будут совершаться в процессе их обработки;

5.5.1.7. общее описание используемых Учреждением способов обработки персональных данных;

5.5.2. типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации, в тех случаях, когда существует необходимость получения письменного согласия на обработку персональных данных;

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

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

5.6. При ведении журналов (реестров, книг) без использования средств автоматизации, содержащих персональные данные, необходимые для однократного пропуска субъекта персональных данных на территорию, на

которой находится Учреждение, или в иных аналогичных целях, должны соблюдаться следующие условия:

5.6.1. необходимость ведения такого журнала (реестра, книги) должна быть предусмотрена актом Учреждения, содержащим:

5.6.1.1. сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации;

5.6.1.2. способы фиксации и состав информации, запрашиваемой у субъектов персональных данных;

5.6.1.3. перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги);

5.6.1.4. сроки обработки персональных данных;

5.6.1.5. сведения о порядке пропуска субъекта персональных данных на территорию, на которой находится Учреждение, без подтверждения подлинности персональных данных, сообщенных субъектом персональных данных;

5.6.2. копирование содержащейся в таких журналах (реестрах, книгах) информации не допускается;

5.6.3. персональные данные каждого субъекта персональных данных могут заноситься в такой журнал (книгу, реестр) не более 1 (одного) раза в каждом случае пропуска субъекта персональных данных на территорию, на которой находится Учреждение.

5.7. При обработке персональных данных допущенные к ним лица обязаны соблюдать нижеперечисленные требования:

5.7.1. Персональные данные не могут быть использованы в целях причинения имущественного и/или морального вреда субъектам персональных данных, затруднения реализации прав и свобод граждан РФ.

5.7.2. Сотрудники должны быть ознакомлены под расписку с нормативными документами Учреждения, устанавливающими порядок обработки персональных данных субъектов, а также их права и обязанности в этой области.

5.7.3. Субъекты персональных данных, не являющиеся сотрудниками Учреждения, имеют право ознакомиться с нормативными документами Учреждения, устанавливающими порядок обработки персональных данных субъектов, а также их права и обязанности в этой области.

5.7.4. В случае выявления недостоверных персональных данных субъекта или неправомерных действий с ними сотрудников Учреждения при обращении или по запросу гражданина, являющегося субъектом персональных данных, или его законного представителя, либо уполномоченного органа по защите прав субъектов персональных данных, необходимо осуществить блокирование персональных данных, относящихся к соответствующему гражданину, с момента такого обращения или получения такого запроса на период проверки.

5.7.5. В случае подтверждения факта недостоверности персональных данных на основании документов, представленных субъектом персональных данных, или его законным представителем, либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов необходимо уточнить персональные данные и снять их блокирование.

5.7.6. В случае выявления неправомерных действий с персональными данными в срок, не превышающий трех рабочих дней с даты такого выявления, необходимо устранить допущенные нарушения. В случае если обеспечить правомерность обработки персональных данных невозможно, Учреждение в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных Учреждение обязано уведомить субъекта персональных данных, или его законного представителя, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, - также указанный орган.

5.8. Получение персональных данных;

5.8.1. Обработка специальных категорий персональных данных субъектов персональных данных в Учреждении осуществляется без согласия лиц, являющихся субъектами персональных данных, обрабатываемых в целях обеспечения кадровой работы и реализации полномочий Учреждения, в соответствии с подпунктом 2.3 пункта 2 части 2 статьи 10, части 3 статьи 10 Федерального закона «О персональных данных» и положениями Трудового кодекса РФ.

5.8.2. Учреждение не имеет права получать, обрабатывать и приобщать к личному делу работника Учреждения персональные данные, не предусмотренные пунктами 3.5.1, 3.5.2, 3.5.3 настоящего Положения, в том

числе касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, иных сведений, касающихся личной жизни.

5.8.3. Персональные данные следует получать лично у субъекта персональных данных. Субъект самостоятельно принимает решение о предоставлении своих персональных данных и дает письменное согласие на их обработку Учреждением в случаях, предусмотренных законодательством Российской Федерации.

5.8.4. В случае возникновения необходимости получения персональных данных у третьей стороны следует известить об этом субъекта заранее, получить его письменное согласие и сообщить ему о целях, предполагаемых источниках и способах получения персональных данных.

5.8.5. Сотрудник Учреждения должен сообщить о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа субъекта дать письменное согласие на их получение.

5.8.6. Сотрудник Учреждения должен проверять достоверность персональных данных, сверяя данные, предоставленные субъектом или его законным представителем, с имеющимися у субъекта или его законного представителя документами.

5.8.7. При принятии решений, затрагивающих интересы субъекта персональных данных, не допускается основываться на персональных данных, полученных исключительно в результате их автоматизированной обработки или электронного получения.

5.9. Хранение персональных данных

5.9.1. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъект персональных данных, не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

5.9.2. Хранение персональных данных субъектов осуществляется на бумажных и электронных носителях, доступ к которым ограничен.

5.9.3. Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях без использования средств автоматизации.

5.9.4. Личные дела хранятся в бумажном виде в папках, прошитые и пронумерованные по страницам. Личные дела хранятся в специально

отведенной секции сейфа или металлического шкафа, обеспечивающего защиту от несанкционированного доступа.

5.9.5. Сотрудники, хранящие персональные данные на бумажных носителях, обеспечивают их защиту от несанкционированного доступа и копирования согласно «Положению об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утвержденному постановлением Правительства РФ 15 сентября 2008 № 687.

5.9.6. Безопасность персональных данных при их обработке с использованием технических и программных средств обеспечивается с помощью системы защиты персональных данных, включающей в себя организационные меры и средства защиты информации, удовлетворяющие устанавливаемым в соответствии с законодательством РФ требованиям, обеспечивающим защиту информации.

5.10. При передаче персональных данных субъекта Учреждения обязано соблюдать нижеперечисленные требования:

5.10.1. Передавать персональные данные субъектов допускается только тем сотрудникам, которые имеют допуск к обработке персональных данных.

5.10.2. Не сообщать персональные данные субъекта третьей стороне без письменного согласия субъекта, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта, а также в случаях, предусмотренных Трудовым кодексом Российской Федерации и иными федеральными законами.

5.10.3. Предупредить лиц, получающих персональные данные субъекта, 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, обязаны соблюдать требования конфиденциальности.

5.10.4. Не сообщать персональные данные субъекта в коммерческих целях без его письменного согласия.

5.10.5. Не запрашивать информацию о состоянии здоровья сотрудника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения им трудовой функции. Информация запрашивается с письменного согласия субъекта персональных данных.

5.10.6. Передавать персональные данные субъекта представителям субъектов в порядке, установленном законодательством Российской Федерации, и ограничивать эту информацию только теми персональными данными субъекта, которые необходимы для выполнения указанными представителями их функций.

5.11. Конфиденциальность персональных данных;

5.11.1. Учреждение обеспечивает конфиденциальность персональных данных, за исключением случаев обезличивания персональных данных и в отношении общедоступных персональных данных.

5.11.2. Все меры конфиденциальности при сборе, обработке и хранении персональных данных субъекта распространяются как на бумажные, так и на электронные (машинные) носители информации.

5.11.3. Все сотрудники, имеющие доступ к персональным данным субъектов, обязаны подписать соглашение о неразглашении персональных данных.

5.12. Уничтожение персональных данных

5.12.1. Персональные данные субъектов хранятся не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

5.12.2. Документы, содержащие персональные данные, подлежат хранению и уничтожению в порядке, предусмотренном законодательством Российской Федерации, а также нормативными документами Учреждения.

5.12.3. Уничтожение носителей информации (как бумажных, так и машинных) производится по решению Директора .

5.12.4. Вывод из эксплуатации машинного носителя производится путем его форматирования, либо путем его механического повреждения в присутствии ответственного за обеспечение безопасности персональных данных.

5.12.5. Бумажные носители персональных данных уничтожаются в бумагорезательной машине, а также путем сжигания.

6. Права и обязанности субъектов персональных данных и Учреждения

6.1. В целях обеспечения защиты персональных данных субъекты имеют право:

6.1.1. получать полную информацию о своих персональных данных и обработке этих данных (в том числе автоматизированной);

6.1.2. осуществлять свободный бесплатный доступ к своим персональным данным, включая право получать копии любой записи, содержащей персональные данные, за исключением случаев, предусмотренных законодательством Российской Федерации;

6.1.3. требовать исключения или исправления неверных или неполных персональных данных, а также данных, обработанных с нарушением законодательства Российской Федерации;

6.1.4. при отказе Учреждения или уполномоченного им лица исключить или исправить персональные данные субъекта - заявить в письменной форме о своем несогласии, представив соответствующее обоснование;

6.1.5. дополнить персональные данные оценочного характера заявлением, выражающим собственную точку зрения;

6.1.6. требовать от Учреждения или уполномоченного им лица уведомления всех лиц, которым ранее были сообщены неверные или неполные персональные данные субъекта, обо всех произведенных в них изменениях или исключениях из них;

6.1.7. обжаловать в судебном порядке любые неправомерные действия или бездействие Учреждения или уполномоченного им лица при обработке и защите персональных данных субъекта.

6.2. Субъект персональных данных или его законный представитель обязуется предоставлять персональные данные, соответствующие действительности.

6.3. Для защиты персональных данных субъектов Учреждения:

6.3.1. обеспечивает защиту персональных данных субъекта от неправомерного их использования или утраты в порядке, установленном законодательством Российской Федерации;

6.3.2. производит ознакомление субъекта или его представителей с настоящим Положением и его правами в области защиты персональных данных под расписку;

6.3.3. по запросу производит ознакомление субъекта персональных данных, не являющегося сотрудником, или в случае недееспособности субъекта, его законных представителей с настоящим Положением и его правами в области защиты персональных данных;

6.3.4. осуществляет передачу персональных данных субъекта только в соответствии с настоящим Положением и законодательством Российской Федерации;

6.3.5. предоставляет персональные данные субъекта только уполномоченным лицам и только в той части, которая необходима им для выполнения их трудовых обязанностей в соответствии с настоящим положением и законодательством Российской Федерации;

6.3.6. обеспечивает субъекту свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей его персональные данные, за исключением случаев, предусмотренных законодательством Российской Федерации;

6.3.7. по требованию субъекта или его законного представителя предоставляет ему информацию о его персональных данных и обработке этих данных.

7. Организация защиты персональных данных

7.1. Защита персональных данных субъекта от неправомерного их использования или утраты обеспечивается Учреждением за счет своих средств, если иное не предусмотрено законодательством РФ.

7.2. В Учреждении защите подлежат все сведения, содержащие персональные данные субъектов, в том числе:

7.2.1. зафиксированные в бумажных документах;

7.2.2. зафиксированные в электронных документах на технических средствах, включая внешние носители;

7.2.3. речевая (акустическая) информация, содержащая персональные данные;

7.2.4. текстовая и графическая видовая информация, содержащая персональные данные;

7.2.5. информация, представленная в виде информативных электрических сигналов, физических полей, содержащая персональные данные.

7.3. Защита персональных данных должна вестись по трем взаимодополняющим направлениям:

7.3.1. Проведение организационных мероприятий:

7.3.1.1. разработка и внедрение внутренних организационно-распорядительных документов, регламентирующих обработку и защиту персональных данных субъектов, в том числе порядок доступа в помещения и к персональным данным;

7.3.1.2. ознакомление сотрудников с законодательством Российской Федерации и внутренними нормативными документами, получение обязательств, касающихся обработки персональных данных;

7.3.1.3. проведение обучения сотрудников вопросам защиты персональных данных.

7.3.2. Программно-аппаратная защита:

7.3.2.1. разработка модели угроз безопасности персональных данных;

7.3.2.2. внедрение программно-аппаратных средств защиты информации, прошедших в соответствии с Федеральным законом № 184 от 27.12.2002 «О техническом регулировании» оценку соответствия;

7.3.2.3. организация учета носителей персональных данных.

7.3.3. Инженерно-техническая защита:

7.3.3.1. установка сейфов или запирающихся шкафов для хранения носителей персональных данных;

7.3.3.2. установка усиленных дверей, сигнализации, режима охраны здания и помещений, в которых обрабатываются персональные данные.

7.4. Определение конкретных мер, общую организацию, планирование и контроль выполнения мероприятий по защите персональных данных осуществляет ответственный за обеспечение безопасности персональных данных в соответствии с законодательством в области защиты персональных данных и локальными нормативно-правовыми актами Учреждения.

7.5. Организацию и контроль защиты персональных данных в Учреждении осуществляет ответственный за организацию обработки персональных данных Учреждения.

8. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных

8.1. Сотрудники Учреждения, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, несут дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.

8.2. Разглашение персональных данных субъекта (передача их посторонним лицам, в том числе другим сотрудниками, не имеющим к ним доступ), их публичное раскрытие, утрата документов и иных носителей, содержащих персональные данные субъекта, а также иные нарушения обязанностей по их защите и обработке, установленных настоящим

Положением, локальными нормативно-правовыми актами (приказами, распоряжениями) Учреждения, влечет наложение на сотрудника, имеющего доступ к персональным данным, дисциплинарных взысканий в виде: замечания, выговора, увольнения.

8.3. Сотрудники Учреждения, имеющий доступ к персональным данным субъекта и совершивший указанный дисциплинарный проступок, несет полную материальную ответственность в случае причинения его действиями ущерба Учреждению (в соответствии с п.7 ст. 243 Трудового кодекса РФ).

8.4. Кодексом Российской Федерации об административных правонарушениях предусмотрены следующие составы административных правонарушений:

8.4.1. статья 5.27 нарушение законодательства о труде и об охране труда;

8.4.2. статья 5.39 неправомерный отказ в предоставлении гражданину и (или) организации информации, предоставление которой предусмотрено федеральными законами, несвоевременное ее предоставление либо предоставление заведомо недостоверной информации;

8.4.3. статья 13.11 нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных);

8.4.4. часть 2 статья 13.12 использование несертифицированных информационных систем, баз и банков данных, а также несертифицированных средств защиты информации, если они подлежат обязательной сертификации (за исключением средств защиты информации, составляющей государственную тайну);

8.4.5. статья 13.14 разглашение информации, доступ к которой ограничен федеральным законом (за исключением случаев, если разглашение такой информации влечет уголовную ответственность), лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей, за исключением случаев, предусмотренных частью 1 статьи 14.33 Кодекса;

8.4.6. часть 1 статья 19.5 невыполнение в установленный срок законного предписания (постановления, представления, решения) органа (должностного лица), осуществляющего государственный надзор (контроль), об устранении нарушений законодательства (Роскомнадзор);

8.4.7. статья 19.7 непредставление или несвоевременное представление в государственный орган (должностному лицу) сведений (информации),

представление которых предусмотрено законом и необходимо для осуществления этим органом (должностным лицом) его законной деятельности, а равно представление в государственный орган (должностному лицу) таких сведений (информации) в неполном объеме или в искаженном виде (уведомление Роскомнадзора).

8.5. Уголовным кодексом РФ предусмотрены следующие преступления в области персональных данных:

8.5.1. часть 1 статьи 137 незаконное собирание или распространение персональных данных либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации;

8.5.2. часть 2 статьи 137 те же деяния, совершенные лицом с использованием своего служебного положения;

8.5.3. статья 140 неправомерный отказ должностного лица в предоставлении собранных в установленном порядке документов и материалов, непосредственно затрагивающих права и свободы гражданина, либо предоставление гражданину неполной или заведомо ложной информации, если эти деяния причинили вред правам и законным интересам граждан;

8.5.4. статья 272 неправомерный доступ к охраняемой законом компьютерной информации (в т.ч. к персональным данным).

8.6. В соответствии с Трудовым кодексом РФ:

8.6.1. статья 90 ответственность за нарушение норм, регулирующих обработку и защиту персональных данных работника;

8.6.2. статья 192 за совершение дисциплинарного проступка, то есть неисполнение или ненадлежащее исполнение работником по его вине возложенных на него трудовых обязанностей, работодатель имеет право применить дисциплинарные взыскания;

8.6.3. по инициативе работодателя может быть расторгнут трудовой договор в случае разглашения персональных данных другого работника (в п. 6 ст. 81 ТК РФ)

Директор

А.Е. Бобраков

Правила обработки персональных данных в Учреждении

1. Обработка персональных данных должна осуществляться на законной и справедливой основе.
2. Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.
3. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.
4. Обработке подлежат только персональные данные, которые отвечают целям их обработки.
5. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.
6. При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Должны быть приняты необходимые меры по удалению или уточнению неполных или неточных данных.
7. Обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных.
8. Меры, направленные на выявление и предотвращение нарушений, предусмотренных законодательством:
 - 1) Осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных Федеральному закону от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее - Федеральный закон) и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике Учреждения имущества и природных ресурсов

Челябинской области (далее - Учреждение) в отношении обработки персональных данных, локальным актам Учреждения;

2) Оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона, соотношение указанного вреда и принимаемых Учреждением мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом;

3) Ознакомление работников Учреждения, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику Учреждения в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.

9. Обеспечение безопасности персональных данных достигается, в частности:

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

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

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

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

5) учетом машинных носителей персональных данных;

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

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

8) установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также

обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных.

10. Целями обработки персональных данных работников являются

- 1) соблюдение порядка и правил приема на работу;
- 2) использование в деятельности с применением средств автоматизации или без таких средств, включая хранение этих данных в архивах и размещение в информационно-телекоммуникационных сетях с целью предоставления доступа к ним;
- 3) заполнение базы данных автоматизированной информационной системы в целях повышения эффективности и быстрого поиска, проведения мониторинговых исследований, формирования статистических и аналитических отчетов;
- 4) обеспечение личной безопасности работников.

11. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обработываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом

12. В случае выявления неправомерной обработки персональных данных, осуществляемой Учреждением или лицом, действующим по поручению Учреждения, Учреждение срок, не превышающий 3 (трех) рабочих дней с даты этого выявления, обязано прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению Учреждения, в случае, если обеспечить правомерность обработки персональных данных невозможно, Учреждение в срок, не превышающий 10 (десяти) рабочих дней с даты выявления неправомерной обработки персональных данных, обязано уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных Учреждение обязано уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя

либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

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

14. В случае отзыва субъектом персональных данных согласия на обработку своих персональных данных Учреждение обязано прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий трех рабочих дней с момента поступления указанного отзыва, если иное не предусмотрено соглашением между Учреждением и субъектом персональных данных. Об уничтожении персональных данных Учреждение обязано уведомить субъекта персональных данных.

15. В случае отсутствия возможности уничтожения персональных данных в течение сроков, указанных выше, Учреждение осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения) и обеспечивает уничтожение персональных данных в срок не более чем 6 (шесть) месяцев, если иной срок не установлен федеральными законами.

16. Пользователи информационных систем персональных данных обязаны:

1) при отсутствии визуального контроля за рабочей станцией: доступ к компьютеру должен быть немедленно заблокирован. Для этого необходимо

нажать одновременно комбинацию клавиш <Ctrl><Alt> и выбрать опцию <Блокировка>.

2) во время работы располагать экран монитора экран монитора так, чтобы затруднить посетителям просмотр отображаемой информации. Шторы и жалюзи на окнах должны быть закрыты.

17. Требования к распечатыванию информации:

1) бракованные бумажные носители и черновики документов, содержащие персональные данные, должны быть уничтожены.

2) при отсутствии пользователя на рабочем месте либо в присутствии лиц, не имеющих допуска к ресурсам информационных систем персональных данных, все документы, содержащие персональные данные, должны быть недоступны для просмотра и иного их использования.

18. Пользователям информационных систем персональных данных запрещается:

1) разглашать защищаемую информацию третьим лицам.

2) копировать защищаемую информацию на неучтенные внешние носители.

3) подключать к информационной системе персональных данных личные внешние носители и мобильные устройства.

4) отключать (блокировать) средства защиты информации.

5) самостоятельно устанавливать или модифицировать программное и аппаратное обеспечение, изменять установленный порядок функционирования технических и программных средств.

Директор

А.Е.Бобраков

**Положение о порядке обработки персональных данных
без использования средств автоматизации в Учреждении**

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

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

3. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ. В этих целях необходимо осуществлять хранение персональных данных в запираемых шкафах или ящиках, ключ от которых должен находиться у сотрудника, имеющего право доступа к персональным данным, находящимся в этих шкафах (ящиках), дубликаты ключей должны храниться у начальника отдела государственной службы и кадров.

4. Шкафы или ящики, в которых хранятся документы, содержащие персональные данные, по окончании рабочего дня запираются сотрудниками, ответственными за учет и хранение документов.

5. Конфиденциальные документы должны пересылаться (доставляться) между организациями в соответствующим образом оформленных запечатанных пакетах.

6. Размножение и отправка документов, содержащих персональные данные, осуществляется только с согласия субъекта персональных данных, за исключением случаев, предусмотренных законодательством Российской Федерации.

7. При обнаружении утраты документов, разглашения информации и признаков несанкционированного ознакомления с конфиденциальными документами, сотрудник обязан доложить ответственному за организацию обработки персональных данных Учреждения, далее по распоряжению директора проводится служебное расследование.

8. Утрата конфиденциальных документов, разглашение информации ограниченного доступа, незаконное ознакомление с информацией ограниченного доступа, влечет ответственность, установленную действующим законодательством Российской Федерации.

Директор

А.Е.Бобраков

**Инструкция по учету лиц, допущенных к работе
с персональными данными в информационных системах Учреждения**

1. Настоящая Инструкция определяет порядок учета лиц, допущенных к работе с персональными данными в информационных системах.
2. В журнале указываются сведения о проведении инструктажа пользователей информационных систем персональных данных правилам работы с системой защиты персональных данных.
3. Основанием для допуска сотрудника к персональным данным является «Список лиц, доступ которых к персональным данным необходим для выполнения трудовых обязанностей», утверждаемый директором.
4. Основанием для прекращения допуска сотрудника к персональным данным является исключение сотрудника из перечня сотрудников, допущенных к персональным данным.
5. Журнал ведется специалистом по защите информации.
6. Учет лиц, допущенный к работе с персональными данными в информационных системах Учреждения должен вестись в журнале (ОБРАЗЕЦ № 1).

Директор

А.Е. Бобраков

**Форма Журнала учета лиц, допущенных к работе
с персональными данными в информационных системах Учреждения**

[illegible]

Инструкция по работе ответственного лица за организацию обработки персональных данных в Учреждении

В области автоматизированной обработки персональных данных Ответственный обязан:

- взаимодействовать со специалистом по защите информации и ответственным за обеспечение безопасности персональных данных по вопросам обеспечения и выполнения требований обработки персональных данных;
- контролировать осуществление мероприятий по установке и настройке средств защиты;
- осуществлять контроль за порядком учета, создания, хранения и использования резервных копий и машинных носителей, содержащих персональные данные.

В области обработки персональных данных без использования средств автоматизации Ответственный обязан:

- контролировать порядок обработки бумажных носителей персональных данных;
- осуществлять проверки наличия документов, содержащих персональные данные.

В области информирования сотрудников Ответственный обязан:

- доводить до сведения сотрудников Учреждения положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;
- осуществлять методическое руководство сотрудников, имеющих санкционированный доступ к персональным данным, в вопросах обеспечения безопасности персональных данных;
- организовывать повышение квалификации сотрудников в области защиты персональных данных.

В области работы с субъектами персональных данных Ответственный обязан:

- разъяснять субъекту персональных данных юридические последствия отказа предоставления его персональных данных;

- организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.

В области контроля сотрудников Ответственный обязан:

- планировать мероприятия по организации обеспечения безопасности персональных данных;

- организовывать и осуществлять периодический контроль пользователей по соблюдению ими режима конфиденциальности, правил работы со съемными машинными носителями информации, выполнению организационных мер по защите информации, а также принимать участие в проведении проверок уполномоченными структурами;

- организовывать работы по плановому контролю работоспособности технических средств защиты персональных данных, охраны объекта, средств защиты информации от несанкционированного доступа.

В области учета лиц, имеющих доступ к персональным данным, Ответственный обязан:

- знать и предоставлять на утверждение Директору изменения к списку лиц, доступ которых к персональным данным необходим для выполнения ими своих трудовых обязанностей;

- участвовать в определении полномочий пользователей ИСПДн (оформлении разрешительной системы доступа), минимально необходимых им для выполнения трудовых обязанностей.

- выполнять иные мероприятия, требуемые нормативными документами по защите персональных данных.

При выявлении факта несанкционированного доступа Ответственный обязан:

- по возможности пресечь дальнейший несанкционированный доступ к персональным данным;

- доложить Директору служебной запиской о факте несанкционированного доступа, его результате (успешный, неуспешный) и предпринятых действиях.

Директор

А.Е. Бобраков

**Инструкция по работе ответственного лица
за обеспечение безопасности персональных данных в Учреждении**

Ответственный обязан:

- обеспечивать выполнение режимных и организационных мероприятий на месте эксплуатации ИСПДн, а также следить за выполнением требований по условиям размещения средств вычислительной техники и их сохранностью;
- знать и предоставлять ответственному за организацию обработки персональных данных изменения к списку лиц, доступ которых к персональным данным необходим для выполнения трудовых обязанностей;
- проводить инструктаж и консультации пользователей по соблюдению режима конфиденциальности;
- участвовать в определении полномочий пользователей ИСПДн (оформлении разрешительной системы доступа), минимально необходимых им для выполнения трудовых обязанностей;
- организовывать периодический контроль пользователей по соблюдению ими режима конфиденциальности, правил работы со съемными машинными носителями информации, выполнению организационных мер по защите информации, а также принимать участие в проведении проверок уполномоченными структурами;
- взаимодействовать со специалистом по защите информации по вопросам обеспечения и выполнения требований обработки персональных данных;
- контролировать осуществление мероприятий по установке и настройке средств защиты;
- организовывать работы по плановому контролю работоспособности технических средств защиты персональных данных, охраны объекта, средств защиты информации от несанкционированного доступа;
- по указанию руководства своевременно и точно отражать изменения в локальных нормативно-правовых актах по управлению средствами защиты информации в ИСПДн и по правилам обработки персональных данных;

- знать перечень и условия обработки персональных данных в Учреждении;
- знать перечень установленных в подразделении технических средств, входящих в состав информационных систем, и перечень задач, решаемых с их использованием;
- обеспечивать соблюдение сотрудниками утвержденного порядка проведения работ по установке и модернизации аппаратных и программных средств компьютеров и серверов из состава информационных систем;
- осуществлять контроль за порядком учета, создания, хранения и использования машинных (выходных) документов, содержащих персональные данные;
- при выявлении возможных каналов неправомерного вмешательства в процесс функционирования информационных систем и осуществления несанкционированного доступа к персональным данным и техническим средствам из состава информационных систем подразделения, сообщать о них директору;
- инструктировать сотрудников по вопросам обеспечения информационной безопасности и правилам работы с применяемыми средствами защиты информации;
- знать законодательство РФ о персональных данных, следить за его изменениями;
- проводить разбирательства и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, нарушения правил работы с документами, содержащими персональные данные, или по другим нарушениям, которые могут привести к снижению уровня защищенности персональных данных;
- выполнять иные мероприятия, требуемые нормативными документами по защите персональных данных.

Директор

А.Е. Бобраков

Правила рассмотрения запросов субъектов персональных данных или их представителей в Учреждении

1. Настоящими Правилами рассмотрения запросов субъектов персональных данных или их представителей определяются порядок учета (регистрации), рассмотрения запросов субъектов персональных данных или их представителей (далее - запросы).

2. Настоящие Правила разработаны в соответствии Федеральным законом от 27.07.2006 № 152 ФЗ «О персональных данных» (далее - Федеральный закон), Федеральным законом от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации», Трудовым кодексом Российской Федерации, Постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации», Постановлением Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» и другими нормативными правовыми актами.

3. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

- 1) подтверждение факта обработки персональных данных;
- 2) правовые основания и цели обработки персональных данных;
- 3) цели и применяемые способы обработки персональных данных;
- 4) наименование и место нахождения, сведения о лицах (за исключением работников Учреждения), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Учреждением или на основании федерального закона;

5) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

6) сроки обработки персональных данных, в том числе сроки их хранения;

7) порядок осуществления субъектом персональных данных прав, предусмотренных настоящим Федеральным законом;

8) информацию об осуществленной или о предполагаемой трансграничной передаче данных;

9) иные сведения, предусмотренные Федеральным законом или другими федеральными законами.

4. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с частью 8 статьи 14 Федерального закона.

5. Субъект персональных данных вправе требовать уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

6. Сведения, указанные в части 7 статьи 14 Федерального закона, должны быть предоставлены субъекту персональных данных в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

7. Сведения, указанные в части 7 статьи 14 Федерального закона, предоставляются субъекту персональных данных или его представителю при обращении либо при получении запроса субъекта персональных данных или его представителя.

8. Субъект персональных данных вправе обратиться в Учреждение повторно или направить повторный запрос в целях получения сведений, указанных в части 7 статьи 14 Федерального закона, а также в целях ознакомления с обрабатываемыми персональными данными, в случае, если такие сведения и

(или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду с необходимыми сведениями должен содержать обоснование направления повторного запроса.

9. Учреждение вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным частями 4 и 5 статьи 14 Федерального закона. Такой отказ должен быть мотивированным.

10. Учреждение обязано сообщить субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя либо в течение тридцати дней с даты получения запроса субъекта персональных данных или его представителя.

11. В случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или персональных данных субъекту персональных данных или его представителю при их обращении, либо при получении запроса субъекта персональных данных или его представителя, уполномоченные работники Учреждения обязаны дать в письменной форме мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 Федерального закона или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий тридцати дней со дня обращения субъекта персональных данных или его представителя, либо с момента получения запроса субъекта персональных данных или его представителя.

12. Учреждение обязано предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных.

13. В срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными

или неактуальными, уполномоченные работники Учреждения обязаны внести в них необходимые изменения.

14. В срок, не превышающий семи рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, уполномоченные работники Учреждения обязаны уничтожить такие персональные данные.

15. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя либо по запросу субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных уполномоченные работники Учреждения обязаны осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных с момента такого обращения или получения указанного запроса на период проверки.

16. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя, либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных уполномоченные работники Учреждения обязаны осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных, с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

17. В случае подтверждения факта неточности персональных данных уполномоченные работники Учреждения на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязаны уточнить персональные данные в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

18. В случае выявления неправомерной обработки персональных данных уполномоченные работники Учреждения в срок, не превышающий трех рабочих

дней с момента этого выявления, обязаны прекратить неправомерную обработку персональных данных. В случае, если обеспечить правомерность обработки персональных данных невозможно, уполномоченные работники Учреждения в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязаны уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных уполномоченные работники Учреждения обязаны уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя, либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

Директор

А.Е.Бобраков

**Правила осуществления внутреннего контроля соответствия обработки
персональных данных
требованиям к защите персональных данных, установленным
Федеральным законом «О персональных
данных», принятыми в соответствии с ним нормативными правовыми
актами и локальными актами Учреждения**

1. Настоящими Правилами осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее - Правила) в Учреждении определяются процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных; основания, порядок, формы и методы проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.

2. Настоящие Правила разработаны в соответствии Федеральным законом от 27.07.2006 № 152 ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации», Постановлением Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» и другими нормативными правовыми актами.

3. В настоящих Правилах используются основные понятия, определенные в статье 3 Федерального закона от 27.07.2006 № 152 ФЗ «О персональных данных».

4. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям в Учреждении организовывается проведение периодических проверок условий обработки персональных данных.

5. Проверки осуществляются ответственным за организацию обработки персональных данных в Учреждении либо комиссией, образуемой приказом Директора.

6. В проведении проверки не может участвовать работник Учреждения, прямо или косвенно заинтересованный в её результатах.

7. Проверки соответствия обработки персональных данных установленным требованиям в Учреждении проводятся на основании утвержденного ежегодного плана осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям или на основании поступившего в Учреждение письменного заявления о нарушениях правил обработки персональных данных (внеплановые проверки). Проведение внеплановой проверки организуется в течение трех рабочих дней с момента поступления соответствующего заявления.

8. При проведении проверки соответствия обработки персональных данных установленным требованиям должны быть полностью, объективно и всесторонне установлены:

- 1) порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке, необходимых для выполнения требований к защите персональных данных;
- 2) порядок и условия применения средств защиты информации;
- 3) эффективность принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
- 4) состояние учета машинных носителей персональных данных;
- 5) соблюдение правил доступа к персональным данным;
- 6) наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер;
- 7) мероприятия по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

8) осуществление мероприятий по обеспечению целостности персональных данных.

9. Ответственный за организацию обработки персональных данных в Учреждении (комиссия) имеет право:

1) запрашивать у работников Учреждения информацию, необходимую для реализации полномочий;

2) требовать от уполномоченных на обработку персональных данных работников уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;

3) принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства Российской Федерации;

4) вносить Директору предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке;

5) вносить Директору предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в отношении обработки персональных данных.

10. В отношении персональных данных, ставших известными ответственному за организацию обработки персональных данных в Учреждении (комиссии) в ходе проведения мероприятий внутреннего контроля, должна обеспечиваться конфиденциальность персональных данных.

11. Проверка должна быть завершена не позднее чем через месяц со дня принятия решения о её проведении. О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, директору докладывает ответственный за организацию обработки персональных данных либо председатель комиссии, в форме письменного заключения.

12. Директор обязан контролировать своевременность и правильность её проведения.

Директор

А.Е.Бобраков

Правила работы с обезличенными данными в Учреждении

1. Настоящие Правила работы с обезличенными персональными данными разработаны с учетом Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и постановления Правительства РФ от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

2. Настоящие Правила определяют порядок работы с обезличенными данными Учреждения и утверждаются Директором.

3. Настоящие правила используют следующие термины и определения в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»:

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

- 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;

- обезличивание персональных данных - действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

4. Обезличивание персональных данных может быть проведено с целью ведения статистических данных, снижения ущерба от разглашения защищаемых

персональных данных, снижения класса информационных систем персональных данных и по достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

5. Способы обезличивания при условии дальнейшей обработки персональных данных:

- замена части сведений идентификаторами;
- обобщение - понижение точности некоторых сведений (например, «Место жительства» может состоять из страны, индекса, города, улицы, дома и квартиры, а может быть указан только город)
- другие способы.

6. Перечень должностей государственных гражданских служащих, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных, приведен в Приложении к настоящим Правилам;

7. Решение о необходимости обезличивания персональных данных принимает директор Учреждения;

8. Руководители структурных подразделений, непосредственно осуществляющие обработку персональных данных, готовят предложения по обезличиванию персональных данных, обоснование такой необходимости и способ обезличивания;

9. Сотрудники подразделений, обслуживающих базы данных с персональными данными, совместно с ответственным за организацию обработки персональных данных, осуществляют непосредственное обезличивание выбранным способом.

10. Обезличенные персональные данные не подлежат разглашению и нарушению конфиденциальности.

11. Обезличенные персональные данные могут обрабатываться с использованием и без использования средств автоматизации.

12. При обработке обезличенных персональных данных с использованием средств автоматизации необходимо соблюдение:

- парольной политики;
- антивирусной политики;
- правил работы со съемными носителями (если они используются);
- правил резервного копирования;

- правил доступа в помещения, где расположены элементы информационных систем;

13. При обработке обезличенных персональных данных без использования средств автоматизации необходимо соблюдение:

- правил хранения бумажных носителей;
- правил доступа к ним и в помещения, где они хранятся.

Директор

А.Е. Бобраков

**Перечни персональных данных, обрабатываемых в Учреждении
в связи с реализацией служебных или трудовых отношений,
а также в связи с выполнением государственного задания**

1. Настоящий Перечень разработан в соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и постановления Правительства РФ от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

2. Перечень персональных данных, обрабатываемых в связи с реализацией служебных (трудовых) отношений.

- 1) Фамилия, имя, отчество (в том числе прежние).
- 2) Дата, место рождения.
- 3) Данные документа, удостоверяющего личность (серия, номер, дата выдачи, наименование органа, выдавшего документ).
- 4) Гражданство.
- 5) Адрес места жительства (по паспорту и фактический), дата регистрации по указанному месту жительства.
- 6) Номер телефона.
- 7) Данные заграничного паспорта (если имеется).
- 8) Сведения о наличии/отсутствии судимостей.
- 9) Сведения об образовании, квалификации (серия, номер, дата выдачи документов об окончании образовательного учреждения, наименование образовательного учреждения, ученая степень, ученое звание, владение иностранными языками и другие сведения).
- 10) Сведения о трудовой деятельности (наименование, адрес и телефон организации, период занятости, занимаемые должности по всем предыдущим местам трудовой занятости, сведения об оформленных допусках к государственной тайне и другие сведения).

11) Реквизиты трудовой книжки и записи в ней.

12) Сведения о воинском учете военнообязанных лиц (серия, номер и дата выдачи, наименование органа, выдавшего военный билет, воинское звание, полное кодовое наименование военно-учетной специальности, категория запаса, категория годности, данные о постановке/снятии с воинского учета и другие данные).

13) Сведения о семейном положении (состояние в браке, реквизиты свидетельства о заключении брака, фамилия, имя, отчество, паспортные данные супруга(и), степень родства, фамилия, имя, отчество, место и дата рождения, место работы/обучения ближайших родственников и другие сведения).

14) Сведения о доходах и обязательствах имущественного характера.

15) Сведения о доходах и обязательствах имущественного характера супруга(и) и несовершеннолетних детей.

16) Номер и серия свидетельства обязательного пенсионного страхования.

17) Реквизиты идентификационного номера налогоплательщика.

18) Реквизиты страхового полиса медицинского страхования.

19) Сведения о поощрениях, государственных и ведомственных наградах (наименование, реквизиты подтверждающего документа).

20) Материалы по внутренним служебным проверкам в отношении работника.

21) Сведения о социальных льготах и социальном статусе.

22) Сведения о временной нетрудоспособности.

3. Перечень персональных данных, обрабатываемых в связи с выполнением государственного задания:

1) Персональные данные граждан, предусмотренные Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», поступающие в Учреждение в пределах полномочий, предоставленных Челябинской области, в соответствии с действующим законодательством.

2) Персональные данные, указываемые гражданами при письменном обращении в Учреждение.

Директор

А.Е. Бобраков

Перечень должностей

**Учреждения, ответственных за проведение мероприятий по обезличиванию
обрабатываемых персональных данных**

1. Директор
2. Главанный бухгалтер
3. Главный специалист по кадрам

Инструкция ответственного за организацию обработки персональных данных в Учреждении

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

2. Настоящая инструкция закрепляет обязанности, права и ответственность лица, ответственного за организацию обработки персональных данных в Учреждении.

3. Лицо, ответственное за организацию обработки персональных данных, в своей работе руководствуется Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», иными нормативными правовыми актами, настоящей Инструкцией, а также иными локальными нормативными актами Учреждения, регламентирующими вопросы обработки персональных данных.

4. Лицо, ответственное за организацию обработки персональных данных в Учреждении обязано:

1) осуществлять внутренний контроль за соблюдением работниками Учреждения законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;

2) доводить до сведения работников Учреждения положения законодательства Российской Федерации о персональных данных, локальных

актов по вопросам обработки персональных данных, требований к защите персональных данных;

3) своевременно уведомлять федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере информационных технологий и связи, об обработке персональных данных.

4) взаимодействовать со специалистом по защите информации и ответственным за обеспечение безопасности персональных данных по вопросам обеспечения и выполнения требований обработки персональных данных;

5) организовывать работы по плановому контролю работоспособности технических средств защиты персональных данных, охраны объекта, средств защиты информации от несанкционированного доступа;

6) выполнять иные мероприятия, требуемые нормативными документами по защите персональных данных.

5. Лицо, ответственное за организацию обработки персональных данных в Учреждении, имеет право:

1) принимать решения в пределах своей компетенции;

2) требовать от работников Учреждения соблюдения действующего законодательства, а также локальных нормативных актов Учреждения о персональных данных;

3) контролировать в Учреждении осуществление мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами;

4) взаимодействовать со структурными подразделениями Учреждения по вопросам обработки персональных данных.

6. Лицу, ответственному за организацию обработки персональных данных в Учреждении, запрещается:

1) использовать сведения, содержащие персональные данные, в неслужебных целях;

2) передавать сведения, содержащие персональные данные, по незащищенным каналам связи без использования средств технической защиты информации;

3) копировать документы и другие носители информации, содержащие персональные данные, а также фиксировать сведения из них без письменного разрешения Директора Учреждения;

4) выносить документы и другие носители информации, содержащие персональные данные, за пределы помещений Учреждения без письменного разрешения Директора Учреждения.

7. За ненадлежащее исполнение или неисполнение настоящей Инструкции, а также за нарушение требований законодательства о персональных данных лицо, ответственное за организацию обработки персональных данных в Учреждении, несет предусмотренную законодательством Российской Федерации ответственность.

Директор

А.Е.Бобраков

Типовое обязательство работника Учреждения, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним служебного контракта или трудового договора прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей

Я, _____

(фамилия, имя, отчество, должность)

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

В соответствии со статьей 7 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» я уведомлен(а) о том, что персональные данные являются конфиденциальной информацией и я обязан(а) не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, ставших известными мне в связи с исполнением должностных обязанностей.

Ответственность, предусмотренная Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и другими федеральными законами, мне разъяснена.

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

СОГЛАСИЕ
на обработку персональных данных

Я _____,

_____ (фамилия, имя, отчество Субъекта)
документ удостоверяющий личность _____ № _____,
(вид документа)

выдан _____
_____ (кем и когда)

зарегистрированный (ая) по адресу: _____

_____ даю свое согласие ОГБУ «БТИ ЧО» (454080, г.Челябинск, ул.С.Кривой, 75/А) – именуемому далее Оператор на обработку Оператором своих персональных данных, то есть совершение, в том числе, следующих действий: обработку (включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, обезличивание, блокирование, уничтожение персональных данных), при этом общее описание вышеуказанных способов обработки данных приведено в Федеральном законе от 27.07.2006 № 152-ФЗ, а также на передачу такой информации третьим лицам, в случаях, установленных нормативными документами вышестоящих органов, законодательством, договорными обязательствами Оператора, связанными с трудовыми отношениями Субъекта.

Перечень персональных данных, передаваемых на обработку:

- фамилия, имя, отчество;
- дата рождения;
- паспортные данные;
- сведения об образовании;
- сведения о занимаемой должности;
- контактный телефон (домашний, сотовый, рабочий);
- фактический адрес проживания;
- адрес размещения офиса;
- прочие.

1. Настоящее согласие действует бессрочно.

2. Настоящее согласие может быть отозвано Субъектом в любой момент по соглашению сторон.

3. В случае неправомерного использования предоставленных данных соглашение отзывается письменным заявлением субъекта персональных данных.

4. Субъект по письменному запросу имеет право на получение информации, касающейся обработки его персональных данных (в соответствии с п.4 ст.14 Федерального закона от 27.06.2006 № 152-ФЗ).

« ____ » _____ 202__ г.

Подпись

ФИО

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.

« ____ » _____ 202__ г.

Подпись

ФИО

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

Мне,

разъяснены юридические последствия отказа предоставить свои персональные данные областному государственному бюджетному учреждению «Бюро технической инвентаризации Челябинской области».

В соответствии со статьями 57, 65, 69 Трудового кодекса Российской Федерации, определен перечень персональных данных, которые я, как субъект персональных данных, обязан представить в Учреждение в связи с поступлением на работу.

Мне, как субъекту персональных данных, разъяснено что:

- без представления обязательных для заключения трудового договора документов и сведений, трудовой договор не может быть заключен;

- на основании пункта 11 статьи 77 Трудового кодекса Российской Федерации трудовой договор прекращается вследствие нарушения установленных правил его заключения, если это нарушение исключает возможность продолжение трудовых (служебных) отношений.

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

**Порядок доступа служащих Учреждения в помещения, в которых ведется
обработка персональных данных**

1. Настоящий порядок доступа работников в помещения Учреждения, в которых ведется обработка персональных данных (далее - порядок) устанавливает единые требования к доступу работников в служебные помещения в целях предотвращения нарушения прав субъектов персональных данных, обрабатываемых в Учреждении, и обеспечения соблюдения требований законодательства о персональных данных.

2. Служебными помещениями, в которых ведётся обработка персональных данных, являются кабинеты № 206 и 208 в здании по адресу г.Челябинск, ул. Сони Кривой, 75А (далее - служебные помещения).

3. В целях обеспечения соблюдения требований к ограничению доступа в служебные помещения Учреждения двери в служебные помещения оборудуются запирающими устройствами и закрываются на замок в отсутствии сотрудников данных подразделений. Работники Учреждения, осуществляющие обработку персональных данных не вправе передавать ключи от служебных помещений третьим лицам, кроме Директора Учреждения.

4. В случае выявления поломки замка Работник незамедлительно информирует об этом Директора и ответственного за организацию обработки персональных данных в Учреждении. В нерабочее время дверь со сломанным замком опечатывается.

5. В служебные помещения, где размещены технические средства, с помощью которых осуществляется обработка персональных данных, а также хранятся носители информации, допускаются только работники Учреждения, уполномоченные на обработку этих персональных данных установленным способом. Другие работники могут находиться в указанных служебных помещениях только для выполнения поручений и получения информации, необходимой для исполнения служебных обязанностей, или в случаях, когда рабочее место работника расположено в одном из служебных помещений.

6. Работники Учреждения, обнаружившие попытку проникновения посторонних лиц в служебное помещение, немедленно сообщают об этом ответственному за организацию обработки персональных данных в Учреждении.

7. Работники Учреждения несут персональную ответственность за соблюдение требований, установленных настоящими Правилами.

8. Не допускается нахождение сотрудников Учреждения в помещениях в нерабочее для них время.

9. Нахождение посетителей Учреждения в помещениях допускается только в рабочее время.

10. Посетители пропускаются в помещения ИСПДн Учреждения в рабочее время в сопровождении сотрудников, допущенных к обработке персональных данных.

11. В помещениях, в которых происходит обработка и хранение персональных данных, запрещено использование не предусмотренных трудовыми обязанностями технических устройств, фотографирование, видеозапись, звукозапись, в том числе с использованием мобильных телефонов.

12. Для исключения возможности бесконтрольного проникновения в помещения и к установленному в них оборудованию посторонних лиц, двери в отсутствие штатных сотрудников запираются на ключ. Помещения должны быть оборудованы специальными инженерными- средствами, такими как усиленные двери, охранная сигнализация и т.п.

13. Сотрудники по окончании рабочего дня обязаны убрать все документы в столы, шкафы и сейфы, закрыть окна и форточки, отключить от сети аппаратуру, радиоточки, электроприборы и освещение.

14. Окна помещений, в которых ведется обработка персональных данных, должны быть оборудованы шторами или жалюзи.

15. Уборка помещений ИСПДн должна производиться под контролем сотрудника, допущенного к обработке персональных данных в этом помещении.

16. Во время уборки в помещении должна быть приостановлена работа с персональными данными, должны быть выключены или заблокированы все АРМ, на которых обрабатываются персональные данные. Носители, содержащие персональные данные, должны быть убраны в закрытые шкафы или сейфы.

Директор

А.Е. Бобраков

Инструкция по работе со съемными носителями в Учреждении

1. Съемными накопителями являются:

- USB-накопители (флеш-диски);
- съемные накопители на жестких магнитных дисках (НЖМД);
- дискеты; диски;

и т.д.

2. Перед использованием съемный носитель должен быть проверен антивирусными средствами на наличие вирусов.

3. Хранение съемных накопителей должно осуществляться в местах не доступных для посторонних лиц, также для должностных лиц оператора, не имеющих полномочий на обработку персональных данных для выполнения должностных обязанностей.

4. Учет съемных накопителей должен вестись в Журнале учета съемных носителей (ОБРАЗЕЦ № 1).

5. Уничтожение съемных носителей персональных данных выполняет специалист по защите информации.

Директор

А.Е. Бобраков

ОБРАЗЕЦ

ЖУРНАЛ
учета съемных носителей в Учреждении

№ п/п	Регистрационный номер или маркировка носителя	Тип носителя и его емкость	Дата поступления	Расписка в получении (Ф.И.О., подпись, дата)	Расписка в обратном приеме (Ф.И.О., подпись, дата)	Место хранения	Дата и номер акта об уничтожении	Примечание
1	2	3	4	5	6	7	8	9

ЖУРНАЛ
резервного копирования информационных систем персональных данных в Учреждении

№	Название информационной системы персональных данных	Дата создания резервной копии	ФИО ответственного за резервную копию	Подпись ответственного за резервную копию