ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ
РЕСПУБЛИКИ КРЫМ
«ЦЕНТР ЗЕМЛЕУСТРОЙСТВА И КАДАСТРОВОЙ ОЦЕНКИ»

(ГБУ РК «ЦЗКО»)

Положение о порядке обработки и обеспечения безопасности персональных данных работников и заказчиков Государственного бюджетного учреждения Республики Крым «Центр землеустройства и кадастровой оценки»

1. Общие положения

1. Настоящее Положение разработано в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон), Постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Постановлением Правительства Российской Федерации от 17 ноября 2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», Федеральным законом от 03.07.2016 № 237-ФЗ «О государственной кадастровой оценке» и устанавливает единый порядок обработки персональных данных работников и заказчиков Государственного бюджетного учреждения Республики Крым «Центр землеустройства и кадастровой оценки» (далее – ГБУ РК «ЦЗКО», учреждение, оператор) и гарантии их конфиденциальности.

Цель разработки Положения – определение порядка обработки и защиты персональных данных работников и заказчиков учреждения и иных субъектов персональных данных, персональные данные которых подлежат обработке, на основании полномочий оператора; обеспечение защиты прав и свобод человека и гражданина, в том числе работника и заказчиков учреждения, при обработке их персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну, а также установление ответственности должностных лиц, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

1.1. В настоящем Положении используются следующие термины и понятия:

- **персональные данные** – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;
- **обработка персональных данных** – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных;
- **информационная система персональных данных (ИСПДн)** – информационная система, представляющая собой совокупность персональных

данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств;

• **обработка персональных данных без использования средств автоматизации (неавтоматизированная)** – обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

В состав персональных данных работников учреждения входят документы, содержащие информацию о паспортных данных, образовании, месте жительства, воинской обязанности, страховании, трудовой деятельности, фото и иные данные, необходимые для осуществления трудовых отношений.

В состав персональных данных заказчиков учреждения входят документы, содержащие информацию о паспортных данных, месте жительства, а также иные сведения, необходимые для оказания профильных услуг.

К персональным данным заказчиков учреждения относятся:

- сведения, содержащиеся в паспорте или ином документе, удостоверяющем личность;
- сведения, содержащиеся в свидетельстве о постановке на учет физического лица в налоговом органе на территории Российской Федерации;
- документ, содержащий сведения о месте проживания;
- сведения, содержащиеся в страховом свидетельстве государственного пенсионного страхования;
- иные сведения, необходимые для определения договорных отношений.

К персональным данным работников ГБУ РК «ЦЗКО» относятся:

- день, месяц, год рождения;
- гражданство;
- паспортные данные (серия, номер, кем и когда выдан);
- адрес регистрации и фактического проживания;
- сведения об образовании;
- сведения о квалификационной категории;
- сведения о прохождении курсов повышения квалификации;
- сведения о трудовой деятельности;
- сведения о государственных наградах и иных наградах и знаках отличия;
- информация о ежегодных оплачиваемых отпусках и отпусках без сохранения денежного содержания;
- информация о владении иностранными языками, степень владения;
- ИНН;
- пенсионное страховое свидетельство;
- сведения о льготах;
- сведения о составе семьи;
- данные страхового полиса ОМС;
- номера телефонов;
- адрес электронной почты;
- фотографии;

- сведения о здоровье;
- сведения о судимости;
- иные сведения.

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

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

Защита персональных данных представляет собой регламентированный технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и, в конечном счете, обеспечивающий достаточно надежную безопасность информации в процессе управленческой и производственной деятельности учреждения.

Защита персональных данных работников и заказчиков от неправомерного их использования или утраты должна быть обеспечена работодателем за счет его средств в порядке, установленном Федеральным законом № 152-ФЗ «О персональных данных» и иными нормативно-правовыми актами, регулирующими меры по защите персональных данных.

2. Основные условия проведения обработки персональных данных

2. 1. Обработка персональных данных осуществляется:

- после получения согласия субъекта персональных данных, за исключением случаев, предусмотренных Федеральным законом;
- после направления уведомления об обработке персональных данных в Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций, за исключением случаев, предусмотренных частью 2 статьи 22 Федерального закона;
- после принятия необходимых мер по защите персональных данных.

2.2. В учреждения приказом директора назначается сотрудник, ответственный за организацию обработки персональных данных и за защиту персональных данных, определяется перечень лиц, допущенных к обработке персональных данных.

2.3. Лица, допущенные к обработке персональных данных, в обязательном порядке под роспись знакомятся с настоящим Положением и подписывают обязательство о неразглашении информации, содержащей персональные данные.

2.4. При обработке персональных данных должны соблюдаться следующие общие требования:

- обработка персональных данных может осуществляться исключительно в целях выполнения работниками своих должностных обязанностей, контроля объема и качества выполняемой работы, соблюдения законодательства РФ и иных нормативно-правовых актов, необходимых для обеспечения безопасности персональных данных;

- при определении объема и содержания, обрабатываемых персональных данных необходимо руководствоваться Конституцией Российской Федерации, Федеральным законом № 152-ФЗ «О персональных данных» и иными нормативно-правовыми актами РФ о персональных данных;
- защита персональных данных работников и заказчиков учреждения от неправомерного их использования или утраты обеспечивается в порядке, установленном законодательством РФ в области защиты персональных данных;
- субъекты персональных данных должны быть ознакомлены с документами учреждения, устанавливающими порядок обработки персональных данных, а также с их правами и обязанностями в этой области.

2.5. Письменное согласие субъекта персональных данных, обработка персональных данных которого осуществляется оператором, должно включать в себя:

- фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);
- наименование или фамилию, имя, отчество и адрес оператора, получающего согласие субъекта персональных данных;
- цель обработки персональных данных;
- перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка будет поручена такому лицу;
- перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;
- срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;
- подпись субъекта персональных данных.

2.6. Запрещается:

- обрабатывать персональные данные в присутствии лиц, не допущенных к их обработке;
- осуществлять обработку персональных данных способом, при котором возможен доступ к персональным данным лиц, не допущенных к их обработке;
- обрабатывать персональные данные в целях, не указанных в настоящем Положении;
- обрабатывать персональные данные без принятия мер по их защите.

3. Передача и хранение персональных данных

3.1. При передаче персональных данных работников и заказчиков учреждения третьим лицам необходимо соблюдать следующие требования:

- не сообщать персональные данных работников и заказчиков учреждения третьей стороне без письменного согласия работников и заказчиков учреждения за исключением случаев, предусмотренных федеральными законами;
- не сообщать персональные данных работников и заказчиков учреждения в коммерческих целях без их письменного согласия;
- предупредить лиц, получивших персональные данные работников и заказчиков учреждения, 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, получившие персональные данные работников и заказчиков учреждения обязаны соблюдать режим конфиденциальности;
- осуществлять передачу персональных данных работников и заказчиков учреждения в пределах учреждения в соответствии с настоящим Положением.

3.2. Хранение и использование персональных данных:

- Персональные данные работников и заказчиков учреждения обрабатываются и хранятся в предназначенных для этого ИСПДн, а также в местах, утвержденных соответствующим приказом.
- Разрешать доступ к персональным данным работников и заказчиков учреждения только допущенным на основании соответствующего приказа лицам.

4. Доступ к персональным данным

4.1. Право доступа к персональным данным работников и заказчиков имеют:

- Директор;
- Первый заместитель директора;
- Заместитель директора;
- Главный бухгалтер;
- Главный инженер;
- Секретарь руководителя;
- Специалист по охране труда;
- Начальник отдела геодезии и картографии;
- Заместитель начальника отдела геодезии и картографии;
- Специалист отдела геодезии и картографии;
- Начальник отдела архивной службы;
- Специалист отдела архивной службы;
- Начальник отдела геоинформационных технологий;
- Заместитель начальника отдела геоинформационных технологий;
- Специалист отдела геоинформационных технологий;
- Начальник отдела кадастра;
- Заместитель начальника отдела кадастра;
- Инженер отдела кадастра;

- Начальник административно-хозяйственного отдела;
- Специалист административно-хозяйственного отдела;
- Начальник финансово-экономического отдела;
- Ведущий экономист финансово-экономического отдела;
- Ведущий специалист по труду и заработной плате финансово-экономического отдела;
- Специалист финансово-экономического отдела;
- Начальник отдела оценки недвижимого имущества;
- Ведущий специалист отдела оценки недвижимого имущества;
- Начальник отдела мониторинга и территориально-ценового зонирования;
- Специалист отдела мониторинга и территориально-ценового зонирования;
- Заведующий сектором контроля и сметно-договорной работы;
- Специалист сектора контроля и сметно-договорной работы;
- Заведующий сектором автоматизации производства;
- Администратор вычислительной техники сектора автоматизации производства;
- Заведующий сектором организации и контроля закупочной деятельности;
- Специалист сектора организации и контроля закупочной деятельности;
- Начальник отдела правового обеспечения;
- Ведущий юрисконсульт отдела правового обеспечения;
- Юрисконсульт отдела правового обеспечения;
- Начальник отдела кадровой работы и делопроизводства;
- Ведущий специалист отдела кадровой работы и делопроизводства.

Директор ГБУ РК «ЦЗКО», первый заместитель директора и заместитель директора имеют право доступа к следующим персональным данным:

- Персональные данные работников учреждения (ФИО, адрес, контактные данные и т.д.);
- Собственные персональные данные;
- Персональные данные работников учреждения (ФИО, адрес, контактные данные и т.д.).

Работники отдела кадровой работы и делопроизводства, имеют право доступа к следующим персональным данным:

- Персональные данные работников учреждения (ФИО, адрес, контактные данные и т.д.);
- Собственные персональные данные.

Главный бухгалтер имеет право доступа к следующим персональным данным:

- Персональные данные работников учреждения (ФИО, контактные данные, банковские реквизиты и т.д.);
- Собственные персональные данные;
- Персональные данные заказчиков учреждения (ФИО, контактные данные, банковские реквизиты и т.д.).

Специалист по охране труда имеет право доступа к следующим персональным данным:

- Персональные данные работников учреждения (ФИО, контактные данные, т.д.);
- Собственные персональные данные.

Секретарь руководителя имеет право доступа к следующим персональным данным:

- Персональные данные заказчиков учреждения (ФИО, контактные данные);
- Собственные персональные данные.

Главный инженер имеет доступа к следующим персональным данным:

- Персональные данные работников учреждения (ФИО, контактные данные, т.д.);
- Персональные данные заказчиков учреждения (ФИО, контактные данные);
- Собственные персональные данные.

Работники административно-хозяйственного отдела имеют право доступа к следующим персональным данным:

- Собственные персональные данные;
- Персональные данные заказчиков учреждения (ФИО, контактные данные).

Работники финансово-экономического отдела имеют право доступа к следующим персональным данным:

- Персональные данные заказчиков учреждения (ФИО, контактные данные);
- Персональные данные работников учреждения (ФИО, контактные данные, т.д.);
- Собственные персональные данные.

Работники сектора автоматизации производства имеют право доступа к следующим персональным данным:

- Собственные персональные данные;
- Персональные данные заказчиков учреждения (ФИО, контактные данные);
- Персональные данные работников учреждения (ФИО, контактные данные, т.д.).

Работники отдела правового обеспечения имеют право доступа к следующим персональным данным:

- Собственные персональные данные;
- Персональные данные заказчиков учреждения (ФИО, контактные данные);
- Персональные данные работников учреждения (ФИО, контактные данные, т.д.).

Работники сектора организации и контроля закупочной деятельности имеют право доступа к следующим персональным данным:

- Собственные персональные данные;
- Персональные данные клиентов учреждения (ФИО, контактные данные).

Работники сектора организации и контроля закупочной деятельности имеют право доступа к следующим персональным данным:

- Собственные персональные данные;
- Персональные данные заказчиков учреждения (ФИО, контактные данные).

Работники отдела геодезии и картографии имеют право доступа к следующим персональным данным:

- Собственные персональные данные;
- Персональные данные заказчиков учреждения (ФИО, контактные данные).

Работники отдела кадастра имеют право доступа к следующим персональным данным:

- Собственные персональные данные;
- Персональные данные заказчиков учреждения (ФИО, контактные данные).

Работники отдела геоинформационных технологий имеют право доступа к следующим персональным данным:

- Собственные персональные данные;
- Персональные данные заказчиков учреждения (ФИО, контактные данные).

Работники отдела архивной службы имеют право доступа к следующим персональным данным:

- Собственные персональные данные;
- Персональные данные заказчиков учреждения (ФИО, контактные данные).

Работники отдела архивной службы имеют право доступа к следующим персональным данным:

- Собственные персональные данные;
- Персональные данные заказчиков учреждения (ФИО, контактные данные).

Работники отдела мониторинга и территориально-ценового зонирования имеют право доступа к следующим персональным данным:

- Собственные персональные данные;
- Персональные данные заказчиков учреждения (ФИО, контактные данные).

Работники сектора контроля и сметно-договорной работы имеют право доступа к следующим персональным данным:

- Собственные персональные данные;
- Персональные данные заказчиков учреждения (ФИО, контактные данные).

4.6. Работники и заказчики учреждения имеют право:

- получать доступ к своим персональным данным и ознакамливаться с ними, включая право на безвозмездное получение копий любой записи, содержащей персональные данные;
- требовать уточнения, исключения или исправления неполных, неверных, устаревших, недостоверных, незаконно полученных или не являющих необходимыми персональных данных;
- получать сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ; перечень обрабатываемых персональных данных и источник их получения; сроки обработки персональных данных, в том числе сроки их хранения; сведения о том, какие юридические последствия для субъекта персональных данных может повлечь за собой обработка его персональных данных;
- требовать произвести извещение всех лиц, которым ранее были сообщены неверные или неполные персональные данные, обо всех произведенных в них исключениях, исправлениях или дополнениях;
- обжаловать в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке неправомерные действия или бездействия, допущенные при обработке и защите персональных данных;
- передача информации третьей стороне возможна только при письменном согласии работников и заказчиков учреждения.

5. Обязанности работников, имеющих доступ к персональным данным работников и заказчиков, по их хранению и защите

5.1. Работники, имеющие доступ к персональным данным работников и заказчиков учреждения обязаны:

5.1.1. Не сообщать персональные данные работников и заказчиков учреждения третьей стороне без письменного на то согласия субъекта персональных данных, кроме случаев, когда в соответствии с федеральными законами такого согласия не требуется;

5.1.2. Использовать персональные данные работников и заказчиков учреждения, полученные только от них лично или с письменного согласия законного представителя;

5.1.3. Обеспечить защиту персональных данных работников и заказчиков учреждения от их неправомерного использования или утраты, в порядке, установленном законодательством Российской Федерации;

5.1.4. Ознакомить работников и заказчиков учреждения с настоящим Положением, их правами и обязанностями в области защиты персональных данных, путем размещения настоящего Положения в открытом доступе на сайте ГБУ РК «ЦЗКО»;

5.1.5. Соблюдать требование конфиденциальности персональных данных работников и заказчиков учреждения;

5.1.6. Исключать или исправлять по письменному требованию работника или заказчиков учреждения недостоверные или неполные персональные данные, а также данные, обработанные с нарушением требований законодательства;

5.1.7. Передавать только те персональные данные работников или заказчиков уполномоченным работникам правоохранительных органов, которые необходимы для выполнения указанными лицами их функций;

5.1.8. Обеспечить работникам и заказчиков учреждения свободный доступ к их персональным данным, включая право на получение копий любой записи, содержащей его персональные данные;

5.1.9. Предоставить по требованию субъекта полную информацию о его персональных данных и обработке этих данных.

5.2. Лица, имеющие доступ к персональным данным работников и заказчиков учреждения не вправе:

– Получать и обрабатывать персональные данные работников и заказчиков учреждения об их религиозных и иных убеждениях, личной жизни;

– Предоставлять персональные данные работников и заказчиков учреждения третьим лицам в коммерческих целях.

5.3. При принятии решений, затрагивающих интересы работников и заказчиков учреждения, запрещается основываться на персональных данных, полученных исключительно в результате их автоматизированной обработки или электронного получения.

6. Порядок определения защищаемой информации

– ГБУ РК «ЦЗКО», в пределах своих полномочий, установленных в соответствии с федеральными законами, создает ИСПДн, в целях оптимизации и автоматизации процессов обработки персональных данных работников и заказчиков учреждения.

– В учреждении на основании «Перечня сведений конфиденциального характера», утвержденного Указом Президента РФ от 06.03.1997 г. № 188, определяется и утверждается перечень сведений ограниченного доступа, не

относящихся к государственной тайне (далее – конфиденциальной информации) и перечень ИСПДн.

– Для каждой ИСПДн определяются цели и порядок обработки персональных данных, утверждается перечень обрабатываемых персональных данных.

7. Порядок обработки персональных данных в ИСПДн с использованием средств автоматизации

7.1. Обработка персональных данных в ИСПДн с использованием средств автоматизации осуществляется в соответствии с требованиями Постановления Правительства РФ от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», нормативных и руководящих документов уполномоченных федеральных органов исполнительной власти.

7.2. Оператором осуществляется классификация ИСПДн в соответствии с Постановлением Правительства РФ от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» в зависимости от категории обрабатываемых данных и их количества.

7.3. Не допускается обработка персональных данных в ИСПДн с использованием средств автоматизации при отсутствии:

– утвержденных организационно-распорядительных документов о порядке эксплуатации ИСПДн, инструкции пользователя ИСПДн, инструкции администратора информационной безопасности, и других нормативных и методических документов;

– настроенных средств защиты от несанкционированного доступа, средств антивирусной защиты, резервного копирования информации и других программных и технических средств в соответствии с требованиями безопасности информации;

– охраны и организации режима допуска в помещения, предназначенные для обработки персональных данных.

8. Порядок обработки персональных данных без использования средств автоматизации

8.1. Обработка персональных данных без использования средств автоматизации (далее – неавтоматизированная обработка персональных данных) может осуществляться в виде документов на бумажных носителях и в электронном виде (файлы, базы банных) на электронных носителях информации.

8.2. При неавтоматизированной обработке различных категорий персональных данных должен использоваться отдельный материальный носитель для каждой категории персональных данных.

8.3. При неавтоматизированной обработке персональных данных на бумажных носителях:

• не допускается фиксация на одном бумажном носителе персональных данных, цели обработки, которых заведомо не совместимы, если иное не предусмотрено федеральным законом;

- персональные данные должны обособляться от иной информации, в частности путем фиксации их на отдельных бумажных носителях, в специальных разделах или на полях форм (бланков);
- документы, содержащие персональные данные, формируются в дела в зависимости от цели обработки персональных данных.

8.4. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее – типовые формы), должны соблюдаться следующие условия:

а) типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели неавтоматизированной обработки персональных данных, имя (наименование) и адрес оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки персональных данных;

б) типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на неавтоматизированную обработку персональных данных, при необходимости получения письменного согласия на обработку персональных данных;

в) 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;

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

8.5. Неавтоматизированная обработка персональных данных в электронном виде осуществляется на внешних электронных носителях информации.

8.6. При отсутствии технологической возможности осуществления неавтоматизированной обработки персональных данных в электронном виде на внешних носителях информации необходимо принимать организационные (охрана помещений) и технические меры (установка сертифицированных средств защиты информации), исключающие возможность несанкционированного доступа к персональным данным лиц, не допущенных к их обработке.

8.7. Электронные носители информации, содержащие персональные данные, учитываются в журнале учета съемных носителей персональных данных.

8.8. При несовместимости целей неавтоматизированной обработки персональных данных, зафиксированных на одном электронном носителе, если электронный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:

а) при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих

распространению и использованию, и используется (распространяется) копия персональных данных;

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

8.9. Документы и внешние электронные носители информации, содержащие персональные данные, должны храниться в служебных помещениях в надежно запираемых шкафах (сейфах). При этом должны быть созданы надлежащие условия, обеспечивающие их сохранность.

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

9. Ответственность должностных лиц

9.1. Работники, допущенные к персональным данным, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несут дисциплинарную административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством Российской Федерации.