

Министерство труда и социального развития Карачаево-Черкесской
Республики

П Р И К А З

"18" 05 2017 года

№ 90

г. Черкесск

**О мерах, направленных на реализацию требований постановления
Правительства Российской Федерации от 21 марта 2012 года № 211 "Об
утверждении перечня мер, направленных на обеспечение выполнения
обязанностей, предусмотренных Федеральным законом "О персональных
данных" и принятыми в соответствии с ним нормативными правовыми
актами, операторами, являющимися государственными или
муниципальными органами"**

В соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ
"О персональных данных" и во исполнение требований постановления
Правительства Российской Федерации от 21 марта 2012 года № 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" п р и к а з ы в а ю:

1. Назначить ответственным за организацию обработки персональных
данных Заместителя министра К.И. Хачирова.

2. Утвердить:

Правила обработки персональных данных в Министерстве труда и
социального развития Карачаево-Черкесской Республики согласно
приложению № 1 к настоящему приказу;

Правила рассмотрения запросов субъектов персональных данных или их
представителей согласно приложению № 2 к настоящему приказу;

Правила осуществления внутреннего контроля соответствия обработки
персональных данных требованиям к защите персональных данных в
Министерстве труда и социального развития Карачаево-Черкесской
Республики согласно приложению № 3 к настоящему приказу;

Правила работы с обезличенными данными в Министерстве труда и
социального развития Карачаево-Черкесской Республики согласно
приложению № 4 к настоящему приказу;

Перечень информационных систем персональных данных Министерства
труда и социального развития Карачаево-Черкесской Республики согласно
приложению № 5 к настоящему приказу;

Перечень персональных данных, обрабатываемых в Министерстве труда

и социального развития Карачаево-Черкесской Республики в связи с реализацией трудовых отношений согласно приложению № 6 к настоящему приказу;

Перечень персональных данных, обрабатываемых в Министерстве труда и социального развития Карачаево-Черкесской Республики в связи с оказанием государственных или муниципальных услуг и осуществлением государственных или муниципальных функций согласно приложению № 7 к настоящему приказу;

Перечень должностей служащих Министерства труда и социального развития Карачаево-Черкесской Республики, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных согласно приложению № 8 к настоящему приказу;

Перечень должностей служащих Министерства труда и социального развития Карачаево-Черкесской Республики, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным согласно приложению № 9 к настоящему приказу;

Должностную инструкцию ответственного за организацию обработки персональных данных в Министерстве труда и социального развития Карачаево-Черкесской Республики согласно приложению № 10 к настоящему приказу;

Типовое обязательство служащего Министерства труда и социального развития Карачаево-Черкесской Республики, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним служебного контракта прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных согласно приложению № 11 к настоящему приказу;

Типовую форму согласия на обработку персональных данных государственных гражданских служащих Министерства труда и социального развития Карачаево-Черкесской Республики и иных субъектов персональных данных согласно приложению № 12 к настоящему приказу;

Порядок доступа служащих Министерства труда и социального развития Карачаево-Черкесской Республики в помещения, в которых ведётся обработка персональных данных согласно приложению № 13 к настоящему приказу.

3. Ответственному за организацию обработки персональных данных:

1) организовать сбор обязательств служащих Министерства труда и социального развития Карачаево-Черкесской Республики прекратить обработку персональных данных, ставших известными им в связи с исполнением должностных обязанностей в случае расторжения с ними служебного контракта. Ознакомить сотрудников Министерства труда и социального развития Карачаево-Черкесской Республики, участвующих в обеспечении сбора указанных обязательств служащих Министерства труда и социального развития Карачаево-Черкесской Республики с настоящим приказом;

2) организовать хранение обязательств служащих Министерства труда и социального развития Карачаево-Черкесской Республики прекратить обработку

персональных данных, ставших известными им в связи с исполнением должностных обязанностей в случае расторжения с ними служебного контракта в личных делах указанных служащих;

3) организовать сбор согласия сотрудников (служащих) Министерства труда и социального развития Карачаево-Черкесской Республики на обработку персональных данных, указанного в приложении № 13 к настоящему приказу. Ознакомить сотрудников Министерства труда и социального развития Карачаево-Черкесской Республики, участвующих в обеспечении сбора согласий на обработку персональных данных сотрудников (служащих) Министерства труда и социального развития Карачаево-Черкесской Республики с настоящим приказом;

4) организовать хранение согласий на обработку персональных данных сотрудников (служащих) Министерства труда и социального развития Карачаево-Черкесской Республики в личных делах указанных сотрудников.

4. Приказ вступает в силу со дня его подписания.

5. Контроль исполнения настоящего приказа оставляю за собой.

Министр



М.Р. Кемов



ПРАВИЛА

обработки персональных данных в Министерстве труда и социального развития Карачаево-Черкесской Республики

1. Основные понятия

- В настоящем документе используются следующие основные понятия:
- автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники;
 - безопасность персональных данных – состояние защищённости персональных данных, при котором обеспечиваются их конфиденциальность, доступность и целостность при их обработке;
 - блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);
 - информационная система персональных данных – совокупность содержащихся в базах данных персональных данных, и обеспечивающих их обработку информационных технологий и технических средств;
 - конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания;
 - несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своим функциональному назначению и техническим характеристикам;
 - обработка персональных данных – любое действие (операция) или совокупность действий, 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 (в том числе

распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

оператор – 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 прямо или косвенно к определённом или определяемому физическому лицу (субъекту персональных данных);

предоставление персональных данных – действия, направленные на раскрытие персональных данных определённому лицу или определённому кругу лиц;

распространение персональных данных – действия, направленные на раскрытие персональных данных неопределённому кругу лиц;

технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приёма и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации;

трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу;

угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных;

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.

2. Общие положения

Настоящие правила разработаны для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных Министерства труда и социального развития

Карачаево-Черкесской Республики (далее – Министерство), а также защиты прав и свобод граждан при обработке их персональных данных в Министерстве, в том числе право на неприкосновенность частной жизни, личную и семейную тайну, а также разъяснение ответственности должностных лиц (служащих), имеющих доступ к персональным данным, за невыполнение требований норм и правил, регулирующих обработку и защиту персональных данных.

Настоящие правила устанавливают порядок обработки персональных данных субъектов персональных данных в Министерстве и направлены на выявление, предотвращение и профилактику нарушений законодательства Российской Федерации в сфере персональных данных.

Субъектами персональных данных в Министерстве являются:

1) граждане;

Настоящие правила определяют необходимый минимальный объём мер, соблюдение которых позволяет предотвратить утечку сведений, относящихся к персональным данным. При необходимости могут быть введены дополнительные меры, направленные на усиление защиты персональных данных.

Настоящие правила разработаны в соответствии со следующими нормативно-правовыми актами Российской Федерации:

- 1) Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных от 28 января 1981 года с поправками, одобренными Комитетом министров Совета Европы 15 июня 1999 года, ратифицированная Федеральным законом Российской Федерации от 19 декабря 2005 года № 160-ФЗ "О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных" в рамках, определяемых данным Федеральным законом, заявлений;
- 2) Конституция Российской Федерации;
- 3) Гражданский кодекс Российской Федерации;
- 4) Кодекс об Административных Правонарушениях Российской Федерации;
- 5) Трудовой кодекс Российской Федерации;
- 6) Уголовный кодекс Российской Федерации;
- 7) Федеральный закон от 27 июля 2004 года № 79-ФЗ "О государственной гражданской службе Российской Федерации";
- 8) Федеральный закон от 27 июля 2006 года № 152-ФЗ "О персональных данных" (далее – Федеральный закон № 152-ФЗ);
- 9) Федеральный закон от 27 июля 2006 года № 149-ФЗ "Об информации, информационных технологиях и о защите информации";
- 10) Перечень сведений конфиденциального характера, утвержденный Указом Президента Российской Федерации от 6 марта 1997 года № 188;
- 11) Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утверждённое постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687;

12) Перечень 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, утверждённый постановлением Правительства Российской Федерации от 21 марта 2012 года № 211;

13) Требования к защите персональных данных при их обработке в информационных системах персональных данных, утвержденные постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119.

В соответствии с законодательством Российской Федерации об обработке и защите персональных данных персональные данные субъектов являются конфиденциальной информацией.

В случаях, предусмотренных действующим законодательством, сведения о доходах, об имуществе и обязательствах имущественного характера гражданского служащего, его супруги (супруга) и несовершеннолетних детей могут размещаться на официальном сайте Министерства или предоставляться региональным средствам массовой информации по их запросам для последующего опубликования.

Порядок регистрации, учёта, оформления, тиражирования, хранения, использования и уничтожения документов и других материальных носителей персональных данных определяют законодательство Российской Федерации об обработке и защите персональных данных, а также действующие нормативные правовые акты Министерства.

Министерство является оператором персональных данных субъектов, указанных в настоящем документе. На основании соглашения (договора) Министерство может поручать обработку персональных данных третьим лицам, с согласия субъекта персональных данных, а в случае если иное предусмотрено действующим законодательством Российской Федерации, то и без их согласия. Существенным условием соглашения (договора) по обработке персональных данных является обязанность обеспечения этими лицами конфиденциальности и безопасности персональных данных субъектов.

В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьёй 24 Конституции Российской Федерации, Министерство вправе получать и обрабатывать данные о частной жизни гражданских служащих и(или) сотрудников Министерства только с их письменного согласия.

Министерство не имеет права получать и обрабатывать персональные данные субъекта о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных законодательством Российской Федерации.

Настоящие Правила вступают в силу с момента их утверждения и действуют до замены их новыми Правилами обработки персональных данных.

Все изменения в Правила вносятся приказом Министра.

3. Цель и содержание обработки персональных данных

Целями обработки персональных данных в Министерстве являются:

- 1) обработка в соответствии с трудовым законодательством;
- 2) выполнение функций министерства.

Цель "обработка в соответствии с трудовым законодательством" достигается посредством обработки персональных данных следующих категорий для следующих субъектов:

- 1) сотрудники:

место рождения, состав семьи, трудоспособность, семейное положение, профессия, фамилия, имя, отчество, образование, дата рождения, сведения о воинском учёте, контактные сведения, информация о трудовой деятельности, гражданство, паспортные данные, адрес, доходы, год рождения, номер банковского счета, ИНН, СНИЛС, судимость, состояние здоровья.

Цель "выполнение функций министерства" достигается посредством обработки персональных данных следующих категорий для следующих субъектов:

- 1) граждане:

размер пенсии, судебные решения о лишении родительских прав, постановления об опеке, свидетельство о рождении, фамилия, имя, отчество, год рождения, дата рождения, место рождения, адрес, контактные сведения, паспортные данные, состав семьи, степень родства, социальное положение, имущественное положение, доходы, информация о трудовой деятельности, ИНН, состояние здоровья, номер банковского счета, свидетельство о временной регистрации граждан Украины, гражданство, семейное положение, свидетельство о смерти, сведения о воинском учёте, образование, профессия, трудоспособность, СНИЛС.

4. Правила обработки персональных данных

Все персональные данные субъектов Министерство получает на законной основе.

Персональные данные ближайших родственников сотрудников (служащих), необходимые для ведения кадрового учёта, Министерство получает от самих сотрудников.

Обработка персональных данных осуществляется в соответствии с действующим законодательством Российской Федерации на основании согласия субъекта персональных данных. Форма согласия утверждается отдельным приказом.

Субъект персональных данных принимает решение о предоставлении своих персональных данных и даёт согласие на их обработку своей волей и в своём интересе.

Министерство оставляет за собой право не осуществлять свои функции в отношении субъекта персональных данных в случае предоставления неполных или недостоверных персональных данных, а также в случае отказа дать

письменное согласие на обработку персональных данных.

При установлении договорных отношений с субъектом персональных данных получение письменного согласия на обработку его персональных данных не требуется.

Получение персональных данных субъекта у третьих лиц возможно только при предварительном уведомлении субъекта и с его письменного согласия. Форма согласия утверждается отдельным приказом.

Персональные данные субъектов Министерства обрабатываются в структурных подразделениях в соответствии с исполняемыми функциями.

Доступ к персональным данным, обрабатываемым без использования средств автоматизации, осуществляется в соответствии со списком, утверждённым в порядке, определяемом в Министерстве.

Доступ к персональным данным, обрабатываемым в информационных системах персональных данных, осуществляется в соответствии со списком, утверждённым в порядке, определяемом в Министерстве.

Уполномоченные лица, допущенные к персональным данным субъектов Министерства, имеют право получать только те персональные данные субъекта, которые необходимы для выполнения конкретных функций, в соответствии с должностными инструкциями указанных лиц.

Обработка персональных данных, осуществляемая без использования средств автоматизации, должна выполняться в соответствии с требованиями "Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации" утверждённого Постановлением Правительства РФ от 15 сентября 2008 № 687.

Персональные данные при такой их обработке, должны обособляться от иной информации, в частности путём фиксации их на отдельных материальных носителях персональных данных, в специальных разделах или на полях форм (бланков).

Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки.

Хранение материальных носителей персональных данных осуществляется в специально оборудованных шкафах и сейфах. Места хранения определяются в соответствии с утверждённым Министром списком.

Персональные данные подлежат уничтожению либо обезличиванию в случаях достижения целей или в случае утраты необходимости в достижении этих целей, отзыва согласия субъекта персональных данных, выявления неправомерной обработки персональных данных, если иное не предусмотрено федеральным законом Российской Федерации.

В срок, не превышающий 7 рабочих дней со дня предоставления субъектом персональных данных или его законным представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, Министерство вносит в них необходимые изменения, а также уведомляет субъекта о внесённых изменениях.

Уничтожение персональных данных осуществляется в срок, не

превышающий 30 рабочих дней с момента достижения цели обработки персональных данных, если иное не предусмотрено федеральным законом Российской Федерации.

Уничтожение персональных данных осуществляется в срок, не превышающий 30 рабочих дней с момента отзыва согласия субъекта персональных данных.

Уничтожение персональных данных осуществляется в срок, не превышающий 7 рабочих дней с момента представления субъектом персональных данных или его законным представителем сведений, подтверждающих, что персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки.

Уничтожение персональных данных осуществляется в срок, не превышающий 10 рабочих дней с момента выявления неправомерной обработки персональных данных. Министерство уведомляет об этом субъекта или его законного представителя.

Уничтожение персональных данных на бумажных носителях осуществляет комиссия в составе руководителя и сотрудников структурного подразделения, обрабатывавшего персональные данные субъекта и установившего необходимость уничтожения персональных данных под контролем руководителя этого структурного подразделения.

Способ уничтожения материальных носителей персональных данных определяется комиссией. Допускается применение следующих способов:

- 1) сжигание;
- 2) шредирование (измельчение);
- 3) передача на специализированные полигоны (свалки);
- 4) химическая обработка.

При этом составляется "Акт уничтожения документов Министерства, содержащих персональные данные субъекта". Форма акта утверждается отдельным приказом.

При необходимости уничтожения большого количества материальных носителей или применения специальных способов уничтожения допускается привлечение специализированных организаций. В этом случае комиссия Министерства должна присутствовать при уничтожении материальных носителей персональных данных. При этом к акту уничтожения необходимо приложить накладную на передачу материальных носителей персональных данных, подлежащих уничтожению, в специализированную организацию.

Уничтожение полей баз данных Министерства, содержащих персональные данные субъекта, выполняется по заявке руководителя структурного подразделения, обрабатывавшего персональные данные субъекта и установившего необходимость их уничтожения.

Уничтожение полей баз данных Министерства, содержащих персональные данные субъекта, осуществляет комиссия, в состав которой входят лица, ответственные за администрирование автоматизированных систем, которым принадлежат базы данных, сотрудники структурного подразделения, обрабатывавшего персональные данные субъекта и

установившего необходимость их уничтожения.

Уничтожение полей баз данных Министерства, содержащих персональные данные субъекта, достигается путём затирания информации на носителях информации (в том числе и резервных копиях) или путём механического нарушения целостности носителя информации, не позволяющего произвести считывание или восстановление персональных данных. При этом составляется "Акт уничтожения полей баз данных Министерства, содержащих персональные данные субъекта". Форма акта утверждается отдельным приказом.

Уничтожение архивов электронных документов и протоколов электронного взаимодействия может не производиться, если ведение и сохранность их в течение определённого срока предусмотрены соответствующими нормативными и (или) договорными документами.

При невозможности осуществления затирания информации на носителях допускается проведение обезличивания путём перезаписи полей баз данных, которые позволяют определить субъекта, данными, исключаящими дальнейшее определение субъекта.

Контроль выполнения процедур уничтожения персональных данных осуществляет ответственный за организацию обработки персональных данных в Министерстве.

Обработка биометрических персональных данных (фотография, отпечатки пальцев, сетчатки глаза и другое), в соответствии со статьёй 11 Федерального закона № 152, допускается при наличии согласия субъекта. Форма согласия утверждается отдельным приказом.

Решение, порождающее юридические последствия в отношении субъекта персональных данных или иным образом затрагивающее его права и законные интересы, может быть принято на основании исключительно автоматизированной обработки его персональных данных только при наличии согласия в письменной форме субъекта персональных данных.

Сотрудники (служащие) Министерства должны быть ознакомлены под роспись с требованиями законодательства Российской Федерации, касающимися обработки персональных данных, настоящими Правилами и другими документами Министерства, устанавливающими порядок обработки персональных данных субъектов, а также права и обязанности в этой области.

5. Передача персональных данных третьим лицам

При обработке персональных данных субъекта должны соблюдаться следующие требования:

1) не сообщать персональные данные субъекта третьей стороне без письменного согласия субъекта. Форма согласия утверждается отдельным приказом. Допускается совмещение формы согласия субъекта с типовыми формами документов, содержащими персональные данные субъекта, при условии соблюдения требований статьи 9 Федерального закона № 152;

2) предупреждать 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 режим конфиденциальности в отношении этих данных.

При необходимости трансграничной передачи персональных данных на территорию иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных данных, Министерство запрашивает согласие субъекта в письменной форме. Форма согласия утверждается отдельным приказом.

6. Права субъектов персональных данных

В целях обеспечения своих интересов субъекты имеют право:

- 1) получать полную информацию о своих персональных данных и обработке этих данных (в том числе автоматизированной);
- 2) осуществлять свободный бесплатный доступ к своим персональным данным, включая право получать копии любой записи, содержащей персональные данные субъекта, за исключением случаев, предусмотренных Федеральным законом;
- 3) требовать исключения или исправления неверных или неполных персональных данных, а также данных, обработанных с нарушением Федерального закона № 152-ФЗ. Субъект персональных данных, при отказе Министерства исключить или исправить персональные данные субъекта, имеет право заявлять в письменной форме о своём несогласии, обосновав соответствующим образом такое несогласие. Персональные данные оценочного характера субъект имеет право дополнить заявлением, выражающим его собственную точку зрения;
- 4) требовать от Министерства уведомления всех лиц, которым ранее были сообщены неверные или неполные персональные данные субъекта, обо всех произведённых в них изменениях или исключениях из них;
- 5) обжаловать в суде любые неправомерные действия или бездействие Министерства при обработке и защите персональных данных субъекта.

7. Порядок действий в случае запросов надзорных органов

В соответствии с частью 4 статьи 20 Федерального закона № 152 Министерство сообщает в уполномоченный орган по защите прав субъектов персональных данных по его запросу информацию, необходимую для осуществления деятельности указанного органа, в течение тридцати дней с даты получения такого запроса.

Сбор сведений для составления мотивированного ответа на запрос надзорных органов осуществляет ответственный за организацию обработки персональных данных в Министерстве при необходимости с привлечением сотрудников (служащих) Министерства.

В течение установленного законодательством срока ответственный за

организацию обработки персональных данных в Министерстве подготавливает и направляет в уполномоченный орган мотивированный ответ и другие необходимые документы.

8. Защита персональных данных субъекта

Защиту персональных данных субъектов от неправомерного их использования или утраты Министерство обеспечивает за счёт собственных средств в порядке, установленном законодательством Российской Федерации.

При обработке персональных данных должны быть приняты необходимые организационные и технические меры по обеспечению их конфиденциальности.

Технические меры защиты персональных данных при их обработке техническими средствами устанавливаются в соответствии с:

1) РД ФСТЭК России – "Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных". Утверждены приказом ФСТЭК России № 21 от 18 февраля 2013 года;

2) специальными требованиями и рекомендациями по технической защите конфиденциальной информации (СТР-К), утвержденными приказом Гостехкомиссии России от 30 августа 2002 года № 282;

3) внутренними документами Министерства, действующими в сфере обеспечения информационной безопасности.

Защита персональных данных предусматривает ограничение к ним доступа.

Ответственные за организацию обработки персональных данных, администрирование средств и механизмов защиты, техническое обслуживание информационных систем персональных данных назначаются приказом Министра.

Руководитель структурного подразделения Министерства, осуществляющего обработку персональных данных:

1) несёт ответственность за организацию защиты персональных данных в структурном подразделении;

2) организует изучение уполномоченными сотрудниками нормативных правовых актов по защите персональных данных и требует их неукоснительного исполнения;

3) обеспечивает режим конфиденциальности в отношении персональных данных, обрабатываемых в структурном подразделении (отделе);

4) контролирует порядок доступа к персональным данным в соответствии с функциональными обязанностями сотрудников подразделения.

Сотрудники (служащие), допущенные к персональным данным дают письменное обязательство о неразглашении таких данных.

9. Обязанности лиц, допущенных к обработке персональных данных

Лица, допущенные к работе с персональными данными, обязаны:

1) знать законодательство Российской Федерации в области обработки и защиты персональных данных, нормативные документы Министерства по защите персональных данных;

2) сохранять конфиденциальность персональных данных;

3) обеспечивать сохранность закреплённых за ними носителей персональных данных;

4) контролировать срок истечения действия согласий на обработку персональных данных и, при необходимости дальнейшей обработки персональных данных, обеспечивать своевременное получение новых согласий или прекращение обработки персональных данных;

5) докладывать своему непосредственному руководителю структурного подразделения обо всех фактах и попытках несанкционированного доступа к персональным данным и других нарушениях.

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

Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, привлекаются к материальной, административной, уголовной и гражданско-правовой ответственности на основании судебного решения, а также к дисциплинарной ответственности в соответствии с действующим законодательством Российской Федерации.

К данным лицам могут быть применены следующие дисциплинарные взыскания:

1) замечание;

2) выговор;

3) предупреждение о неполном должностном соответствии;

4) увольнение с гражданской службы.

ПРИЛОЖЕНИЕ № 2

УТВЕРЖДЕНЫ
приказом Министра труда и
социального развития
Карачаево-Черкесской Республики
от "8" 05 2017 года № 90

ПРАВИЛА рассмотрения запросов субъектов персональных данных или их представителей

При устном обращении либо письменном запросе субъекта персональных данных или его законного представителя на доступ к персональным данным субъекта, Министерство труда и социального развития Карачаево-Черкесской Республики (далее – Министерство) руководствуется требованиями статей 14, 18 и 20 Федерального закона Российской Федерации от 27 июля 2006 года № 152 "О персональных данных".

Доступ субъекта персональных данных или его законного представителя к персональным данным субъекта Министерство предоставляет только под контролем ответственного за организацию обработки персональных в Министерстве.

Обращение субъекта персональных данных или его законного представителя фиксируется в журнале учёта обращений граждан по вопросам обработки персональных данных. Порядок ведения журнала и ответственные за ведение определяются приказом руководителя Министерства. Рекомендуемая форма журнала приведена в приложении № 1.

Запрос субъекта персональных данных или его законного представителя фиксируется в журнале учета запросов граждан по вопросам обработки персональных данных. Порядок ведения журнала и ответственные за ведение определяются приказом руководителя Министерства. Рекомендуемая форма журнала приведена в приложении № 2.

Ответственный за организацию обработки персональных данных принимает решение о предоставлении доступа субъекту персональных данных или его законному представителю к персональным данным указанного субъекта.

В случае, если данных предоставленных субъектом или его законным представителем не достаточно для установления его личности или предоставление персональных данных нарушает конституционные права и свободы других лиц ответственный за организацию обработки персональных данных подготавливает мотивированный ответ, содержащий ссылку на

положение части 8 статьи 14 Федерального закона Российской Федерации от 27 июля 2006 года № 152 "О персональных данных" или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий тридцати рабочих дней со дня обращения субъекта персональных данных или его законного представителя либо от даты получения запроса субъекта персональных данных или его законного представителя.

Для предоставления доступа субъекта персональных данных или его законного представителя к персональным данным субъекта ответственный за организацию обработки персональных данных привлекает сотрудника (сотрудников) структурного подразделения, обрабатывающего персональные данные субъекта по согласованию с руководителем этого структурного подразделения.

Сведения о наличии персональных данных Министерства предоставляет субъекту персональных данных или его законному представителю в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных. Контроль предоставления сведений субъекту или его законному представителю осуществляет ответственный за организацию обработки персональных данных.

Сведения о наличии персональных данных должны быть предоставлены субъекту персональных данных или его законному представителю при ответе на запрос в течение тридцати дней от даты получения запроса субъекта персональных данных или его законного представителя.

ПРИЛОЖЕНИЕ № 1
к ПРИЛОЖЕНИЮ № 2
утверждённому приказом Министра
труда и социального развития
Карачаево-Черкесской Республики
от "18" 05 2017 года №90

Министерство труда и социального развития Карачаево-Черкесской Республики

ЖУРНАЛ

учета обращений граждан по вопросам обработки персональных данных

Журнал начал " " 20__ года Журнал завершен " " 20__ года

Заместитель министра

/К.И. Хачиров/

На ___ листах

ПРИЛОЖЕНИЕ № 2
к ПРИЛОЖЕНИЮ № 2
утверждённому приказом Министра
труда и социального развития
Карачаево-Черкесской Республики
от "18" 05 2017 года № 90

Министерство труда и социального развития Карачаево-Черкесской Республики

ЖУРНАЛ

учета запросов граждан по вопросам обработки персональных данных

Журнал начат " _____ " _____ 20__ года Журнал завершен " _____ " _____ 20__ года
Заместитель министра _____ /К.И. Хачиров/ _____
На _____ листах

ПРИЛОЖЕНИЕ № 3

УТВЕРЖДЕНЫ

приказом Министра труда и
социального развития

Карачаево-Черкесской Республики
от "18" 05 2017 года № 90

ПРАВИЛА

**осуществления внутреннего контроля соответствия обработки
персональных данных требованиям к защите персональных данных в
Министерстве труда и социального развития Карачаево-Черкесской
Республики**

1. Общие положения

Настоящие правила разработаны в соответствии с положениями Федерального закона от 27 июля 2006 года № 152-ФЗ "О персональных данных" и требованиями по соблюдению 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, утверждённых постановлением Правительства Российской Федерации от 21 марта 2012 года № 211, и определяют порядок организации и осуществления контроля выполнения соответствия обработки персональных данных требованиям к защите персональных данных в структурных подразделениях Министерства труда и социального развития Карачаево-Черкесской Республики (далее – Министерство).

Правила обязательны для исполнения всеми должностными лицами Министерства, осуществляющими контроль состояния защиты персональных данных.

Контроль выполнения соответствия обработки персональных данных требованиям к защите персональных данных в структурных подразделениях Министерства осуществляется с целью определения наличия несоответствий между требуемым уровнем защиты персональных данных и его фактическим состоянием, правильности обработки персональных данных ответственными лицами в структурных подразделениях, а также выработать меры по их устранению и недопущению в дальнейшем.

Контроль осуществляет ответственный за организацию обработки персональных данных в Министерстве.

Контроль проводится в форме плановых и внеплановых проверок. Внеплановые проверки могут быть контрольными и по частным вопросам.

Контрольные проверки проводятся для установления полноты выполнения рекомендаций плановых проверок.

Проверки по частным вопросам охватывают отдельные направления по защите персональных данных и могут проводиться в случаях, когда стали известны факты несанкционированного доступа, утечки либо утраты персональных данных субъектов министерства или нарушения требований по обработке и защите персональных данных.

Проверки осуществляются ответственным за организацию обработки персональных данных в Министерстве либо комиссией, образуемой Министром.

Сроки проведения контрольных проверок доводятся руководителям проверяемых структурных подразделений не позднее, чем за 24 часа до начала проверки.

Проверки по частным вопросам могут проводиться без уведомления руководителей проверяемых подразделений (отделов).

Периодичность и сроки проведения плановых проверок подразделений Министерства устанавливаются планом, утверждаемым Министром. Сроки проведения плановых проверок доводятся руководителям проверяемых структурных подразделений (отделов) не позднее, чем за 10 суток до начала проверки.

2. Порядок подготовки к проверке

Проверка проводится на основании приказа Министра. Ответственный за организацию обработки персональных данных в Министерстве подготавливает предложения по составу комиссии. Проект приказа о проверке подготавливает ответственный за организацию обработки персональных данных в Министерстве.

Проверяющие лица обязаны получить у руководителей проверяемых структурных подразделений информацию об условиях обработки персональных данных, необходимую для достижения целей проверки. Перед началом проверки они должны изучить материалы предыдущих проверок данного структурного подразделения.

3. Порядок проведения проверки

По прибытию в структурное подразделение для проведения проверки председатель комиссии прибывает к руководителю проверяемого структурного подразделения Министерства, представляется ему и представляет других прибывших на проверку лиц.

Руководитель проверяемого структурного подразделения обязан оказывать содействие комиссии по проверке и в случае необходимости определяет должностное лицо, ответственное за сопровождение проверки.

На период проведения контрольных мероприятий обработку персональных данных необходимо по возможности прекращать. Допуск

проверяющих лиц к конкретным информационным ресурсам, защищаемым сведениям и техническим средствам должен исключать ознакомление проверяющих лиц с конкретными персональными данными.

Общий порядок проведения проверки включает следующее:

1) получение документов о распределении обязанностей по обработке и защите персональных данных, выявление ответственных за обработку и защиту персональных данных и установление факта ознакомления сотрудников проверяемого структурного подразделения со своей ответственностью;

2) получение при содействии сотрудников проверяемого структурного подразделения документов, касающихся обработки и защиты персональных данных в данном структурном подразделении;

3) анализ полученной документации;

4) непосредственная проверка выполнения установленного порядка обработки и защиты персональных данных и требований законодательства Российской Федерации в области защиты персональных данных.

При этом согласовываются конкретные вопросы по объёму, содержанию, срокам проведения проверки, а также каких должностных лиц структурного подразделения необходимо привлечь к проверке и какие объекты следует посетить.

В ходе осуществления контроля выполнения требований по обработке и защите персональных данных в проверяемом структурном подразделении Министерства рассматриваются в частности следующие показатели:

1) в части общей организации работ по обработке персональных данных:

а) соответствие информации, указанной в уведомлении об обработке персональных данных и в положении о порядке обработки персональных данных Министерства, реальному положению дел;

б) соответствие обрабатываемой и собираемой информации (персональных данных), их полнота, в соответствии с нормативными правовыми актами и локальными актами, принятыми в Министерстве;

в) наличие нормативных документов по защите персональных данных;

г) знание нормативных документов сотрудниками (служащими), имеющими доступ к персональным данным;

д) полнота и правильность выполнения требований нормативных документов Министерства сотрудниками (служащими), имеющими доступ к персональным данным;

е) наличие документов, определяющих состав сотрудников, ответственных за организацию защиты персональных данных в подразделении, соответствие этих документов реальному штатному составу подразделения, а также подтверждение факта ознакомления ответственных сотрудников с данными документами;

ж) уровень подготовки сотрудников, ответственных за организацию защиты персональных данных в подразделении;

з) наличие согласий на обработку персональных данных субъектов персональных данных. Соответствие объёма персональных данных и сроков

обработки целям обработки персональных данных.

2) в части защиты персональных данных в информационных системах персональных данных (далее - ИСПДн):

а) соответствие средств вычислительной техники ИСПДн показателям, указанным в документации на ИСПДн;

б) структура и состав локальных вычислительных сетей, организация разграничения доступа пользователей к сетевым информационным ресурсам, порядок защиты охраняемых сведений при передаче (обмене) персональных данных в сети передачи данных;

в) соблюдение установленного порядка использования средств вычислительной техники ИСПДн;

г) наличие и эффективность применения средств и методов защиты персональных данных, обрабатываемых на средствах вычислительной техники;

д) соблюдение требований, предъявляемых к паролям на информационные ресурсы;

е) соблюдение требований и правил антивирусной защиты средств вычислительной техники;

ж) контроль журналов учёта носителей персональных данных. Сверка основного журнала с дублирующим (если требуется ведение дублирующего учёта носителей);

з) тестирование реализации правил фильтрации межсетевого экрана, процесса регистрации, процесса идентификации и аутентификации запросов, процесса идентификации и аутентификации администратора межсетевого экрана, процесса регистрации действий администратора межсетевого экрана, процесса контроля за целостностью программной и информационной части, процедуры восстановления настроек межсетевого экрана.

3) в части защиты информационных ресурсов и помещений:

а) правильность отнесения обрабатываемой информации к персональным данным;

б) правильность установления уровня защищенности персональных данных в информационной системе;

в) закрепление гражданско-правовой ответственности в сфере информационной безопасности и соблюдения режима конфиденциальности персональных данных в правилах внутреннего трудового распорядка, положениях о структурных подразделениях Министерства, должностных инструкциях сотрудников (служащих) и трудовых договорах;

г) порядок передачи персональных данных органам государственной власти, местного самоуправления и сторонним организациям (контрагентам);

д) действенность принимаемых мер по защите охраняемых сведений в ходе подготовки материалов к открытому опубликованию и при изготовлении рекламной продукции;

е) состояние конфиденциального делопроизводства, соблюдение установленного порядка подготовки, учёта, использования, хранения и уничтожения документов, содержащих персональные данные;

ж) выполнение требований по правильному оборудованию защищаемых помещений и предотвращению утечки охраняемых сведений при проведении мероприятий конфиденциального характера;

з) соответствие защищаемых помещений их техническим паспортам.

Более подробно вопросы, подлежащие проверке, могут раскрываться в отдельных документах (методических рекомендациях, технологических картах, памятках и т.п.).

Во время проведения проверки, выявленные нарушения требований по обработке и защите персональных данных должны быть по возможности устранены. Проверяющие лица могут дать рекомендации по устранению на месте отмечаемых нарушений и недостатков.

Недостатки, которые не могут быть устранены на месте, включаются в итоговый документ по результатам проверки.

4. Оформление результатов проверки

Результаты проверки оформляются:

1) актом - при проведении проверки комиссией;

2) служебной запиской - при проведении проверки назначенными специалистами.

Акт и/или служебная записка составляется в двух экземплярах и подписывается членами комиссии.

Один экземпляр хранится у ответственного за организацию обработки персональных данных Министерства. Второй экземпляр хранится в Министерстве в установленном порядке. Копия акта о проверке остается в проверяемом структурном подразделении.

Результаты проверок структурных подразделений периодически обобщаются ответственным за организацию обработки персональных данных в Министерстве и доводятся до руководителей структурных подразделений. При необходимости принятия решений по результатам проверок структурных подразделений на имя Министра готовятся соответствующие служебные записки.

ПРИЛОЖЕНИЕ № 4

УТВЕРЖДЕНЫ
приказом Министра труда и
социального развития
Карачаево-Черкесской Республики
от "18" 05 2017 года № 90

ПРАВИЛА работы с обезличенными данными в Министерстве труда и социального развития Карачаево-Черкесской Республики

Настоящие правила разработаны в соответствии с положениями Федерального закона Российской Федерации от 27 июля 2006 года № 152-ФЗ "О персональных данных" и требованиями по соблюдению 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, утверждённых постановлением Правительства Российской Федерации от 21 марта 2012 года № 211, и определяют порядок работы с обезличенными данными в структурных подразделениях (отделах) Министерства труда и социального развития Карачаево-Черкесской Республики (далее – Министерство).

Правила обязательны для исполнения всеми должностными лицами Министерства, допущенными к персональным данным.

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

Персональные данные подлежат уничтожению либо обезличиванию в случаях достижения целей обработки или в случае утраты необходимости в их достижении.

Порядок обезличивания включает в себя замену идентифицирующей информации о субъекте, например, одновременно фамилии, имени и отчества на произвольный код (далее – идентификатор).

В случае, если обезличенные персональные данные используются в статистических или иных исследовательских целях, сроки обработки и хранения персональных данных устанавливаются руководством Министерства исходя из служебной необходимости, получение согласия субъекта на обработку его персональных данных в данном случае не требуется на основании пункта 9 части 1 статьи 6 Федерального закона от 27 июля 2006 года № 152-ФЗ "О персональных данных".

Методы и способы защиты информации от несанкционированного доступа для обеспечения безопасности обезличенных персональных данных в информационных системах и целесообразность их применения определяются ответственным за организацию обработки персональных данных в Министерстве индивидуально для каждой информационной системы персональных данных.

ПРИЛОЖЕНИЕ № 5

УТВЕРЖДЕН
 приказом Министра труда и
 социального развития
 Карачаево-Черкесской Республики
 от "18" 05 2017 года № 90

ПЕРЕЧЕНЬ
информационных систем персональных данных
Министерства труда и социального развития Карачаево-Черкесской
Республики

№	Наименование ИСПДн	Категория ИСПДн	Уровень защищенности персональных данных	Использование СКЗИ для обеспечения безопасности персональных данных
1	2	3	4	5
1	Адресно-социальная помощь	ИСПДн-С	третий	используются
2	Бухгалтерия и Кадры	ИСПДн-И	четвертый	используются
3	Работа с населением	ИСПДн-И	четвертый	используются

ПРИЛОЖЕНИЕ № 6

УТВЕРЖДЕН
приказом Министра труда и
социального развития
Карачаево-Черкесской Республики
от "18" "05" 2017 года № 90

ПЕРЕЧЕНЬ

персональных данных, обрабатываемых в Министерстве труда и социального развития Карачаево-Черкесской Республики в связи с реализацией трудовых отношений

1. Фамилия, имя, отчество, дата и место рождения, гражданство.
2. Владение иностранными языками и языками народов Российской Федерации.
3. Образование (когда и какие образовательные учреждения закончил, номера дипломов, направление подготовки или специальность по диплому, квалификация по диплому).
4. Послевузовское профессиональное образование (наименование образовательного или научного учреждения, год окончания), учёная степень, учёное звание (когда присвоены, номера дипломов, аттестатов).
5. Выполняемая работа с начала трудовой деятельности (включая военную службу, работу по совместительству, предпринимательскую деятельность).
6. Классный чин федеральной государственной гражданской службы, гражданской службы субъекта Российской Федерации, муниципальной службы, дипломатический ранг, воинское, специальное звание, классный чин правоохранительной службы (кем и когда присвоены).
7. Государственные награды, иные награды и знаки отличия (кем награждён и когда).
8. Степень родства, фамилии, имена, отчества, даты рождения близких родственников (отца, матери, братьев, сестёр и детей), а также мужа (жены).
9. Места рождения, места работы и домашние адреса близких родственников (отца, матери, братьев, сестёр и детей), а также мужа (жены).
10. Адрес регистрации и фактического проживания.
11. Дата регистрации по месту жительства.
12. Паспортные данные (серия, номер, кем и когда выдан).
13. Номер телефона.
14. Отношение к воинской обязанности, сведения по воинскому учёту (для граждан, пребывающих в запасе, и лиц, подлежащих призыву на военную службу).
15. Идентификационный номер налогоплательщика.

16. Номер страхового свидетельства обязательного пенсионного страхования.

17. Наличие (отсутствие) судимости.

18. Результаты обязательных предварительных (при поступлении на работу) и периодических медицинских осмотров (обследований), а также обязательного психиатрического освидетельствования.

19. Сведения о последнем месте государственной или муниципальной службы.

ПРИЛОЖЕНИЕ № 7

УТВЕРЖДЕН
приказом Министра труда и
социального развития
Карачаево-Черкесской Республики
от "18" "05" 2017 года № 90

ПЕРЕЧЕНЬ

персональных данных, обрабатываемых в Министерстве труда и социального развития Карачаево-Черкесской Республики в связи с оказанием государственных и осуществлением государственных функций

1. Состав семьи.
2. Фамилия, имя, отчество.
3. Адрес.
4. Контактные сведения.
5. Паспортные данные.
6. Состояние здоровья.
7. Степень родства.
8. Размер пенсии.
9. Судебные решения о лишении родительских прав.
10. Постановления об опеке.
11. Свидетельство о рождении.
12. Год рождения.
13. Дата рождения.
14. Место рождения.
15. Социальное положение.
16. Имущественное положение.
17. Доходы.
18. Информация о трудовой деятельности.
19. ИНН.
20. Номер банковского счета.
21. Свидетельство о временной регистрации граждан Украины.
22. Гражданство.
23. Свидетельство о смерти.
24. Сведения о воинском учете.
25. Профессия.
26. СНИЛС.
27. Трудоспособность.
28. Семейное положение.
29. Образование.

ПРИЛОЖЕНИЕ № 8

УТВЕРЖДЕН
приказом Министра труда и
социального развития
Карачаево-Черкесской Республики
от "18" 05 2017 года № 90

ПЕРЕЧЕНЬ

**должностей служащих Министерства труда и социального развития
Карачаево-Черкесской Республики, ответственных за проведение
мероприятий по обезличиванию обрабатываемых персональных данных**

№ п/п	Структурное подразделение (отдел)	Должность служащего
1	2	3
1	Информационно-аналитический отдел	Начальник

ПРИЛОЖЕНИЕ № 9

УТВЕРЖДЕН
 приказом Министра труда и
 социального развития
 Карачаево-Черкесской Республики
 от "18" 05 2017 года № 90

ПЕРЕЧЕНЬ

**должностей служащих Министерства труда и социального развития
 Карачаево-Черкесской Республики, замещение которых предусматривает
 осуществление обработки персональных данных либо осуществление
 доступа к персональным данным**

№ п/п	Структурное подразделение (отдел)	Должность служащего
1	2	3
1	Информационно-аналитический отдел	Начальник
2	Организационно-правовой отдел	Начальник, Консультант, Консультант - юрист, Ведущий специалист - эксперт, Ведущий специалист - эксперт - юрист
3	Отдел бухгалтерского учета и отчетности	Начальник, Ведущий консультант, Консультант, Ведущий специалист - эксперт
4	Планово-финансовый отдел	Начальник, Ведущий консультант, Консультант, Главный специалист - эксперт, Ведущий специалист - эксперт
5	Отдел по социальной защите ветеранов, инвалидов и пожилых людей	Начальник, Заместитель начальника, Консультант
6	Отдел по проблемам семьи, материнства и детства	Начальник, Ведущий консультант, Ведущий специалист - эксперт, Заместитель начальника, Старший специалист
7	Отдел по вопросам охраны труда и трудовых отношений	Начальник, Консультант
8	Отдел организации назначения и выплаты субсидий и мер социальной поддержки по оплате жилищно-коммунальных услуг	Начальник, Ведущий специалист - эксперт
9	Администрация	Министр, Первый заместитель министра, Заместитель министра, Консультант

УТВЕРЖДЕНА
приказом Министра труда и
социального развития
Карачаево-Черкесской Республики
от "18" 05 2017 года № 90

ДОЛЖНОСТНАЯ ИНСТРУКЦИЯ
ответственного за организацию обработки персональных данных в
Министерстве труда и социального развития Карачаево-Черкесской
Республики

1. Общие положения

Ответственный за организацию обработки персональных данных (далее – Ответственный) является сотрудником Министерства труда и социального развития Карачаево-Черкесской Республики (далее – Министерство).

Ответственный назначается приказом Министра.

Ответственный в вопросах организации обработки персональных данных подчиняется непосредственно Министру и проводит мероприятия по защите персональных данных в интересах Министерства.

Ответственный в своей деятельности руководствуется:

- 1) Конституцией Российской Федерации;
- 2) Федеральными законами Российской Федерации и нормативными правовыми актами органов государственной власти по вопросам защиты персональных данных;
- 3) Государственными стандартами Российской Федерации в области защиты информации;
- 4) Руководящими и нормативными правовыми документами Федеральной Службы по техническому и экспортному контролю России;
- 5) Локальными нормативными актами Министерства по защите персональных данных;
- 6) Правилами внутреннего трудового распорядка.

Деятельность Ответственного осуществляется согласно плану мероприятий по защите персональных данных Министерства на год.

2. Задачи

На Ответственного возложены следующие задачи:

- 1) организация внутреннего контроля за соблюдением сотрудниками (служащими) Министерства норм законодательства Российской Федерации по

обработке персональных данных, в том числе требований, предъявляемых к защите персональных данных;

2) разработка, внедрение и актуализация локальных актов по вопросам обработки персональных данных;

3) доведение до сведения сотрудников (служащих) Министерства, непосредственно осуществляющих обработку персональных данных, положений законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных, и проведение обучения указанных сотрудников;

4) осуществление контроля приёма и обработки обращений и запросов субъектов персональных данных или их законных представителей по вопросам обработки персональных данных и внесение предложений по организации приёма и обработки таких обращений и запросов;

5) осуществление рассмотрения обращений и запросов субъектов персональных данных или их законных представителей по вопросам обработки персональных данных и организация предоставления субъектам персональных данных или их законным представителям информации, предусмотренной Федеральным законом Российской Федерации от 27 июля 2006 года № 152-ФЗ "О персональных данных";

б) организация комплексной защиты объектов информатизации Министерства, а именно:

а) информационных ресурсов, представленных в виде документированной информации на магнитных, оптических носителях, информативных физических полей, информационных массивов и баз данных, содержащих персональные данные субъектов Министерства;

б) средств и систем информатизации (средств вычислительной техники, информационно-вычислительных комплексов, локальных вычислительных сетей и корпоративных информационных систем), программных средств (операционных систем, систем управления базами данных, другого общесистемного и прикладного программного обеспечения), автоматизированных систем управления информационными, управленческими и технологическими процессами, систем связи и передачи данных, технических средств приёма, передачи и обработки информации (звукозаписи, звукоусиления, звуковоспроизведения, переговорных устройств и других технических средств обработки графической, смысловой и буквенно-цифровой информации), используемых для реализации процессов ведения деятельности, обработки информации, содержащей персональные данные субъектов Министерства.

7) организация защиты персональных данных субъектов Министерства;

8) разработка и проведение организационных мероприятий, обеспечивающих безопасность объектов защиты Министерства, своевременное выявление и устранение возможных каналов утечки информации;

9) организация проведения работ по технической защите информации на объектах информатизации, в информационно-вычислительных сетях, системах и средствах связи и телекоммуникаций Министерства;

10) реализация технических мер, обеспечивающих своевременное выявление возможных технических каналов утечки информации в структурных подразделениях (отделах) Министерства;

11) методическое руководство системой обеспечения информационной безопасности Министерства;

12) организация контроля состояния и проведение оценки эффективности системы обеспечения информационной безопасности персональных данных, а также реализация мер по её совершенствованию;

13) внедрение в информационную инфраструктуру Министерства современных методов и средств обеспечения информационной безопасности.

3. Функции

Для решения поставленных задач Ответственный осуществляет следующие функции:

1) участие в разработке и внедрении правовых, организационных и технических мер по комплексному обеспечению безопасности персональных данных;

2) контроль обеспечения соблюдения режима конфиденциальности при обработке персональных данных и внесение предложений по соблюдению такого режима;

3) разработка планов по защите персональных данных на объектах Министерства;

4) контроль выполнения мер по защите персональных данных, анализ материалов контроля, выявление недостатков и нарушений. Разработка и реализация мер по их устранению;

5) контроль выполнения плановых заданий, договорных обязательств, а также сроков, полноты и качества работ по защите персональных данных, выполняемых контрагентами;

6) разработка и внесение предложений по обеспечению финансирования работ по защите персональных данных, в том числе выполняемых по договорам;

7) участие в проведении работ по технической защите информации на объектах информатизации Министерства. Оценка эффективности принятых мер по технической защите информации;

8) внесение предложений по обеспечению выбора, установке, настройке и эксплуатации средств защиты информации в соответствии с организационно-распорядительной и эксплуатационной документацией;

9) контроль организации режима обеспечения безопасности помещений, в которых происходит обработка персональных данных, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в такие помещения, а также внесение предложений по обеспечению безопасности таких помещений;

10) участие в организации доступа сотрудников (служащих) Министерства к персональным данным в соответствии с возложенными на них

должностными обязанностями и подготовка предложений по организации такого доступа;

11) разработка и внедрение локальных актов, определяющих перечень сотрудников Министерства, имеющих доступ к персональным данным;

12) контроль размещения устройств ввода (отображения) информации, исключающего её несанкционированный просмотр;

13) проведение оценки вреда, который может быть причинён субъектам персональных данных в случае нарушения законодательства по защите персональных данных;

14) участие в разработке и реализации политики по работе с инцидентами информационной безопасности, в части обработки персональных данных;

15) внесение предложений по актуализации внутренней организационно-распорядительной документации по защите персональных данных при изменении существующих и выходе новых нормативных правовых документов по вопросам обработки персональных данных и подготовка соответствующих необходимых проектов документов.

4. Права

Ответственный имеет право:

1) осуществлять контроль за деятельностью структурных подразделений (отделов) Министерства по выполнению ими требований по защите персональных данных;

2) составлять акты, докладные записки, отчёты для рассмотрения руководством Министерства, при выявлении нарушений порядка обработки персональных данных;

3) принимать необходимые меры при обнаружении несанкционированного доступа к персональным данным, как сотрудниками (служащими) Министерства, так и третьими лицами, и докладывать о принятых мерах Министру с предоставлением информации о субъектах, нарушивших режим доступа;

4) вносить на рассмотрение Министру предложения, акты, заключения о приостановлении работ в случае обнаружения каналов утечки (или предпосылок к утечке) информации ограниченного доступа;

5) давать структурным подразделениям (отделам) Министерства, а также отдельным специалистам обязательные для исполнения указания по вопросам, входящим в компетенцию Ответственного;

6) запрашивать и получать от всех структурных подразделений (отделов) Министерства сведения, справочные и другие материалы, необходимые для осуществления деятельности Ответственного;

7) составлять акты и другую техническую документацию о степени защищённости объектов информатизации;

8) готовить и вносить предложения: на проведение работ по защите персональных данных; о привлечении к проведению работ по оценке эффективности защиты персональных данных на объектах Министерства (на

договорной основе) учреждений и организаций, имеющих лицензию на соответствующий вид деятельности; о закупке необходимых технических средств защиты и другой спецтехники, имеющих в обязательном порядке сертификат соответствия;

9) осуществлять визирование договоров с контрагентами с целью правового обеспечения передачи им персональных данных субъектов Министерства в ходе выполнения работ по этим договорам;

10) представлять интересы Министерства при осуществлении государственного контроля и надзора за обработкой персональных данных Уполномоченным органом по защите прав субъектов персональных данных.

5. Взаимоотношения(служебные связи)

Ответственный выполняет свои задачи осуществляя взаимодействие со всеми структурными подразделениями (отделами) Министерства.

Для выполнения своих функций и реализации предоставленных прав Ответственный взаимодействует с территориальными и региональными подразделениями Федеральной службы по техническому и экспортному контролю России, Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций, Федеральной службы безопасности Российской Федерации, Министерства внутренних дел Российской Федерации и другими представителями исполнительной власти и организациями, предоставляющими услуги и выполняющими работы в области защиты персональных данных на законном основании.

6. Ответственность

Ответственный несёт ответственность за надлежащее и своевременное выполнение возложенных задач и функций по организации обработки персональных данных в Министерстве в соответствии с положениями законодательства Российской Федерации в области персональных данных.

УТВЕРЖДЕНО
приказом Министра труда и
социального развития
Карачаево-Черкесской Республики
от "18" "05" 2017 года № 90

ТИПОВОЕ ОБЯЗАТЕЛЬСТВО

служащего Министерства труда и социального развития
Карачаево-Черкесской Республики, непосредственно осуществляющего
обработку персональных данных, в случае расторжения с ним служебного
контракта прекратить обработку персональных данных, ставших
известными ему в связи с исполнением должностных обязанностей

Я, _____, проживающий(-ая) по адресу
Ф.И.О.

_____ паспорт
серии _____, номер _____, выдан _____

"__" ____ года,

работая в должности _____ в
Министерстве труда и социального развития Карачаево-Черкесской
Республики (далее – Министерство труда и социального развития
Карачаево-Черкесской Республики), в период настоящих трудовых отношений
и в течение 5 лет после их окончания, в соответствии с Федеральным законом
Российской Федерации от 27 июля 2006 года № 152-ФЗ "О персональных
данных", обязуюсь:

1) не раскрывать третьим лицам и не распространять персональные
данные субъектов Министерства труда и социального развития
Карачаево-Черкесской Республики, полученные при исполнении мной
должностных обязанностей;

2) прекратить обработку персональных данных, ставших известными мне
в связи с исполнением должностных обязанностей, и передать все носители
персональных данных субъектов Министерства труда и социального развития
Карачаево-Черкесской Республики (документы, накопители данных в
электронном виде, кино- и фото-негативы, позитивы, и прочее)
Ответственному за организацию обработки персональных данных
Министерства труда и социального развития Карачаево-Черкесской
Республики.

Я понимаю, что разглашение персональных данных субъектов
Министерства труда и социального развития Карачаево-Черкесской
Республики, может нанести ущерб субъектам персональных данных.

Я предупреждён(а) о том, что в случае разглашения или утраты мною сведений, относящихся к персональным данным субъектов Министерства труда и социального развития Карачаево-Черкесской Республики, я несу ответственность в соответствии со статьей 90 Трудового Кодекса Российской Федерации и могу быть привлечён(а) к материальной, гражданско-правовой, административной и уголовной ответственности, в соответствии с действующим законодательством Российской Федерации.

" ____ " _____ 2017 года

(подпись)

(инициалы, фамилия)

ПРИЛОЖЕНИЕ № 12

УТВЕРЖДЕНО
приказом Министра труда и
социального развития
Карачаево-Черкесской Республики
от "18" 05 2017 года № 90

Министру
труда и социального развития Карачаево-Черкесской Республики

М.Р. Кемову

СОГЛАСИЕ

**на обработку персональных данных государственных гражданских
служащих Министерства труда и социального развития
Карачаево-Черкесской Республики и иных субъектов персональных**

Я, _____, проживающий (-ая) по
адресу _____,
паспорт серии _____, номер _____, выдан _____

"__" _____ года, в соответствии с Федеральным законом
Российской Федерации от 27 июля 2006 года № 152-ФЗ "О персональных
данных", даю согласие Министерству труда и социального развития
Карачаево-Черкесской Республики, расположенному по адресу 369000,
Карачаево-Черкесская республика, г. Черкесск, пл. Ленина, Дом
Правительства, на обработку моих персональных данных, а именно:

<i>ФИО</i>	<i>Адрес</i>	<i>Образование</i>
<i>Дата рождения</i>	<i>Паспортные данные</i>	<i>Доходы</i>
<i>Место рождения</i>	<i>Семейное положение</i>	<i>Профессия</i>

(ненужное зачеркнуть)

и другие:

(перечислить дополнительные категории персональных данных)

В целях

(указать цели обработки)

Перечень допустимых действий, осуществляемых с персональными

данными: сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, обезличивание, блокирование, уничтожение;

Министерство труда и социального развития Карачаево-Черкесской Республики может осуществлять автоматизированную/ смешанную/ неавтоматизированную обработку персональных данных без (с) применения (ем) ЭВМ, без (с) передачи(ей) по внутренней сети и без (с) передачи(ей) по сети интернет.

Согласие вступает в силу со дня его подписания и действует в течение _____. Действие настоящего согласия прекращается досрочно в случае принятия оператором решения о прекращении обработки персональных данных и/или уничтожения документов, содержащих персональные данные.

Согласие может быть отозвано мною в любое время на основании моего письменного заявления.

" ____ " _____ 20__ года

(подпись)

(инициалы, фамилия)

УТВЕРЖДЕН
приказом Министра труда и
социального развития
Карачаево-Черкесской Республики
от "18" 05 2017 года № 90

ПОРЯДОК
доступа служащих Министерства труда и социального развития
Карачаево-Черкесской Республики в помещения, в которых ведётся
обработка персональных данных

1. Общие положения

Настоящий порядок разработан в целях обеспечения безопасности персональных данных, средств вычислительной техники информационных систем персональных данных, материальных носителей персональных данных, а также обеспечения внутриобъектового режима.

Документ устанавливает правила доступа в помещения в рабочее и нерабочее время, а также в нештатных ситуациях.

Объектами охраны Министерства труда и социального развития Карачаево-Черкесской Республики (далее – Министерство) являются:

1) помещения, в которых происходит обработка персональных данных как с использованием средств автоматизации, так и без таковых, в том числе серверные помещения;

2) помещения, в которых хранятся материальные носители персональных данных и резервные копии персональных данных;

3) помещения, в которых установлены криптографические средства, предназначенные для шифрования персональных данных, в том числе носители ключевой информации (далее спецпомещения).

Бесконтрольный доступ посторонних лиц в указанные помещения исключён.

Посторонними лицами считаются сотрудники Министерства, не допущенные к обработке персональных данных и лица, не являющиеся сотрудниками Министерства.

К спецпомещениям, предъявляются дополнительные требования по безопасности, указанные в разделе 4.

Ответственность за соблюдение положений настоящего порядка несут сотрудники структурных подразделений, допущенные в помещения, являющиеся объектами охраны, а также их руководители.

Контроль соблюдения требований настоящей инструкции обеспечивает

сотрудник, назначенный ответственным за организацию обработки персональных данных в Министерстве.

Ограждающие конструкции объектов охраны должны предполагать существенные трудности для нарушителя по их преодолению.

Например: металлические решётки на окнах, металлическая дверь, система контроля и управления доступа и так далее.

2. Правила доступа в помещения, в которых ведётся обработка персональных данных

Доступ посторонних лиц в помещения, в которых ведётся обработка персональных данных, а также хранятся материальные носители персональных данных и резервные копии персональных данных, должен осуществляться только ввиду служебной необходимости и под контролем сопровождающего лица, из числа сотрудников, допущенных к обработке персональных данных.

При этом должны быть приняты меры, исключаящие ознакомление посторонних лиц с персональными данными. Пример: мониторы повернуты в сторону от посетителей, документы убраны в стол, либо находятся в непрозрачной папке (накрыты чистыми листами бумаги).

При возникновении чрезвычайных ситуаций природного и техногенного характера, аварий, катастроф, стихийных бедствий, а также ситуаций, которые могут создавать угрозу жизни и здоровью граждан, в целях оказания помощи гражданам, предотвращения, ликвидации предпосылок и последствий нештатной ситуации, может осуществляться доступ в помещения, в которых ведётся обработка персональных данных лиц из числа сотрудников Министерства, не допущенных к обработке персональных данных.

В нерабочее время все окна и двери в помещениях (в том числе в смежные помещения), в которых ведётся обработка персональных данных, должны быть надёжно закрыты, материальные носители персональных данных должны быть убраны в запираемые шкафы (сейфы), компьютеры выключены либо заблокированы.

Доступ сотрудников в помещения, в которых ведётся обработка персональных данных в нерабочее время, допускается по распоряжению руководства Министерства.

3. Правила доступа в серверные помещения

Доступ в серверные помещения, в которых ведётся обработка персональных данных осуществляется в соответствии со списком, утверждённым в Министерстве.

Уборка серверных помещений происходит только под контролем лица, из указанных в утверждённом списке.

Доступ в серверные помещения посторонних лиц допускается по согласованию с ответственным за обеспечение безопасности информационных систем персональных.

Нахождение в серверных помещениях посторонних лиц без сопровождающего запрещено.

При возникновении чрезвычайных ситуаций природного и техногенного характера, аварий, катастроф, стихийных бедствий, а также других ситуаций, которые могут создавать угрозу жизни и здоровью граждан, доступ в серверные помещения, в целях оказания помощи гражданам, предотвращения, ликвидации предпосылок и последствий нештатной ситуации, может осуществляться без согласования с ответственным за обеспечение безопасности информационных систем персональных.

Доступ сотрудников в серверные помещения в нерабочее время допускается по распоряжению руководства Министерства.

4. Правила доступа в спецпомещения

Спецпомещения выделяют с учётом размеров контролируемых зон, регламентированных эксплуатационной и технической документацией к криптосредствам. Помещения должны иметь прочные входные двери с замками, гарантирующими надёжное закрытие помещений в нерабочее время. Окна помещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в спецпомещения посторонних лиц, необходимо оборудовать металлическими решётками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в спецпомещения.

Расположение спецпомещения, специальное оборудование и организация режима в спецпомещениях должны исключить возможность неконтролируемого проникновения или пребывания в них посторонних лиц, а также просмотра посторонними лицами ведущихся там работ.

Для предотвращения просмотра извне спецпомещений их окна должны быть защищены.

Спецпомещения должны быть оснащены входными дверьми с замками. Должно быть обеспечено постоянное закрытие дверей спецпомещений на замок и открытие только для санкционированного прохода, а также опечатывание спецпомещений по окончании рабочего дня или оборудование спецпомещений соответствующими техническими устройствами, сигнализирующими о несанкционированном вскрытии спецпомещений.

Доступ в спецпомещения осуществляется в соответствии с перечнем лиц, имеющих право доступа в помещения, где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ, утверждённым приказом Министра.

Доступ иных лиц в спец помещения может осуществляться под контролем лиц, имеющих право допуска в спецпомещения.

При возникновении чрезвычайных ситуаций природного и техногенного характера, аварий, катастроф, стихийных бедствий, а также ситуаций, которые могут создавать угрозу жизни и здоровью граждан, в целях оказания помощи

гражданам, предотвращения, ликвидации предпосылок и последствий нештатной ситуации, может осуществляться доступ в спецпомещения иных лиц их числа сотрудников Министерства.

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

При утрате ключа от входной двери в спецпомещение замок необходимо заменить или переделать его секрет с изготовлением к нему новых ключей с документальным оформлением.

Доступ сотрудников в спецпомещения в нерабочее время допускается на основании служебных записок (или иных видов разрешающих документов), подписанных Министром.

Нахождение в спецпомещениях посторонних лиц в нерабочее время запрещается.