

УТВЕРЖДЕНЫ

приказом министерства культуры
Ставропольского края
от «02» апреля 2013 г. № 177

ПРАВИЛА

обработки персональных данных, устанавливающие процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также определяющие для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований в министерстве культуры Ставропольского края

І. ОБЩИЕ ПОЛОЖЕНИЯ

1. Настоящие Правила обработки персональных данных в министерстве культуры Ставропольского края (далее – Правила) устанавливают единый порядок обработки персональных данных в министерстве культуры Ставропольского края (далее – министерство).

2. Обработка персональных данных в министерстве осуществляется в соответствии с Федеральным законом от 27 июля 2006 года №152-ФЗ «О персональных данных» (далее — Федеральный закон № 152-ФЗ), настоящими Правилами и другими нормативными правовыми актами, касающимися обработки персональных данных.

3. Основные понятия и термины, используемые в настоящих Правилах, применяются в том же значении, что и Федеральном законе № 152-ФЗ.

4. Целью настоящих Правил является обеспечение защиты персональных данных граждан от несанкционированного доступа, неправомерного их использования или утраты.

5. Настоящие Правила устанавливают и определяют:
процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных;
цели обработки персональных данных;
содержание обрабатываемых персональных данных для каждой цели обработки персональных данных;
категории субъектов, персональные данные которых обрабатываются;
сроки обработки и хранения обрабатываемых персональных данных;

порядок уничтожения обработанных персональных данных при достижении целей обработки или при наступлении иных законных оснований.

6. Основные условия обработки персональных данных:

6.1. Обработка персональных данных осуществляется после принятия необходимых мер по защите персональных данных, а именно:

после получения согласия субъекта персональных данных, за исключением случаев, предусмотренных пунктами 2-7, 9-11 части 1 статьи 6 Федерального закона № 152-ФЗ;

после направления уведомления об обработке персональных данных в Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Ставропольскому краю, за исключением случаев, предусмотренных частью 2 статьи 22 Федерального закона № 152-ФЗ.

6.2. Лица, допущенные к обработке персональных данных, в обязательном порядке под роспись знакомятся с настоящими Правилами и подписывают обязательство о неразглашении информации.

II. ПРОЦЕДУРЫ, НАПРАВЛЕННЫЕ НА ВЫЯВЛЕНИЕ И ПРЕДОТВРАЩЕНИЕ НАРУШЕНИЙ ЗАКОНОДАТЕЛЬСТВА В СФЕРЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

7. Меры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации:

7.1. Информационные ресурсы, содержащие персональные данные, созданные, приобретенные, накопленные в министерстве, а также полученные путем иных установленных законом способов, являются собственностью министерства и не могут быть использованы иначе, как с разрешения министра или в установленных законом случаях.

7.2. К мерам, направленным на выявление и предотвращение нарушений законодательства Российской Федерации в сфере обработки персональных данных относятся:

назначение ответственного за организацию обработки персональных данных в министерстве;

применение правовых, организационных и технических мер по обеспечению безопасности персональных данных в соответствии с частями 1 и 2 статьи 19 Федерального закона №152-ФЗ;

осуществление внутреннего контроля соответствия обработки персональных данных Федеральному закону № 152-ФЗ и принятыми в соответствии с ним нормативными правовыми актами, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора;

оценка вреда, который может быть причинён субъектам персональным данным в случае нарушения законодательства Российской Федерации и настоящих Правил;

ознакомление работников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных и настоящими Правилами;

запрет на обработку персональных данных лицами, не допущенными к их обработке;

запрет на обработку персональных данных под диктовку.

7.3. Документы, определяющие политику оператора в отношении обработки персональных данных, подлежат обязательному опубликованию.

7.4. За разглашение информации, содержащей персональные данные, нарушение порядка обращения с документами и машинными носителями информации, содержащими такую информацию, а также за нарушение режима защиты, обработки и порядка использования этой информации, работник может быть привлечен к дисциплинарной или иной ответственности, предусмотренной действующим законодательством.

8. Порядок обработки персональных данных в информационных системах персональных данных с использованием средств автоматизации:

8.1. Обработка персональных данных в информационных системах персональных данных с использованием средств автоматизации министерства осуществляется в соответствии с требованиями постановления Правительства Российской Федерации от 1 ноября 2012 года № 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.

8.2. При эксплуатации автоматизированных информационных систем необходимо соблюдать следующие требования:

к работе допускаются только лица, назначенные соответствующим приказом по министерству;

на персональных электронных вычислительных машинах (далее – ПЭВМ), дисках, папках и файлах, на которых обрабатываются и хранятся сведения о персональных данных, должны быть установлены пароли (идентификаторы);

на период обработки защищаемой информации в помещении могут находиться только лица, допущенные в установленном порядке к обрабатываемой информации;

допуск других лиц в указанный период может осуществляться с разрешения министра или первого заместителя, отвечающего за защиту информации в министерстве.

8.3. Руководители подразделений министерства, работники министерства (пользователи информации) обязаны контролировать и выполнять предусмотренные в министерстве меры по защите информации, содержащей персональные данные.

8.4. Руководители подразделений министерства обязаны:

участвовать в подготовке перечня персональных данных, обрабатываемых на ПЭВМ подразделения;

готовить к утверждению списки работников, которых по своим должностным обязанностям необходимо допустить к работе с персональными данными в информационной системе министерства;

контролировать целевое использование работниками ресурсов сети "Интернет";

контролировать выполнение пользователями общих правил работы на ПЭВМ и в локальной вычислительной сети министерства (далее — ЛВС);

выборочно контролировать характер исходящей информации, направляемой пользователями по электронной почте другим адресатам и принимать оперативные меры к соблюдению ими установленных требований по защите персональных данных;

при обнаружении нарушений установленных требований по защите персональных данных, в результате которых вскрыты факты их разглашения, прекратить работы на рабочем месте, где обнаружены нарушения, доложить министру и поставить в известность начальника отдела правовой и кадровой работы;

инициировать служебные расследования по фактам разглашения информации, содержащей персональные данные, или утери документов, содержащих такую информацию, по фактам нарушений пользователями правил, установленных для работы с персональными данными в ЛВС, а также нарушений требований по защите информации;

обеспечивать условия для работы специалистов по защите информации при проверке в подразделении эффективности предусмотренных мер защиты информации;

8.5. При приеме на работу работник предупреждается об ответственности за разглашение сведений, содержащих персональные данные, которые станут ему известными в связи с предстоящим выполнением своих служебных обязанностей.

8.6. Пользователь обязан:

знать правила работы в ЛВС и принятые меры по защите ресурсов ЛВС (в части, его касающейся);

при работе на своей рабочей станции (ПЭВМ) и в ЛВС выполнять только служебные задания;

перед началом работы на ПЭВМ проверить свои рабочие папки на жестком магнитном диске, рабочие дискеты и CD-диски на отсутствие вирусов с помощью штатных средств антивирусной защиты, убедиться в исправности своей рабочей станции;

при сообщениях тестовых программ о появлении вирусов немедленно прекратить работу, доложить администратору сети и своему непосредственному начальнику;

при обработке информации, содержащей персональные данные, использовать только зарегистрированные машинные носители информации (далее – МНИ);

при необходимости использования магнитных носителей, поступивших из других подразделений, учреждений, предприятий и организаций, прежде всего, провести проверку этих носителей на отсутствие вирусов;

выполнять предписания администратора сети и ответственного за защиту информации в министерстве;

представлять для контроля свою рабочую станцию (ПЭВМ) руководителю подразделения и администратору сети;

сохранять в тайне свой индивидуальный пароль, периодически изменять его и не сообщать другим лицам;

вводить пароль и другие учетные данные, убедившись, что клавиатура находится вне поля зрения других лиц;

учет, размножение, обращение печатных материалов, содержащих персональные данные, проводить в соответствии с Инструкцией по делопроизводству в министерстве культуры Ставропольского края;

при обнаружении различных неисправностей в работе компьютерной техники или ЛВС, недокументированных свойств в программном обеспечении, нарушений целостности пломб (наклеек, печатей), несоответствии номеров на аппаратных средствах сообщить администратору сети и поставить в известность руководителя подразделения.

Пользователю при работе запрещается:

играть в компьютерные игры;

приносить различные компьютерные программы и пытаться установить их на локальный диск компьютера без уведомления администратора сети;

перенастраивать программное обеспечение компьютера;

самостоятельно вскрывать комплектующие рабочей станции (ПЭВМ);

запускать на своей рабочей станции (ПЭВМ) или другой рабочей станции сети любые системные или прикладные программы, кроме установленных специалистами по защите информации или администратором сети;

изменять или копировать файл, принадлежащий другому пользователю, не получив предварительно разрешения владельца файла;

оставлять включенной без присмотра свою рабочую станцию (ПЭВМ), не активизировав средства защиты от несанкционированного доступа (временную блокировку экрана и клавиатуры);

оставлять без личного присмотра на рабочем месте или где бы то ни было свое персональное устройство идентификации (при наличии), магнитные носители и распечатки, содержащие персональные данные;

допускать к подключенной в сеть рабочей станции (ПЭВМ) посторонних лиц;

производить копирование для временного хранения информации, содержащей персональные данные, на неучтенные носители;

работать на рабочей станции сети с информацией, содержащей персональные данные, при обнаружении неисправностей станции;

умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты информации,

которые могут привести к утечке, блокированию, искажению или утере информации, содержащей персональные данные;

отсылать по электронной почте информацию личного или коммерческого характера для решения личных проблем, а также информацию по просьбе третьих лиц без согласования с руководителем подразделения;

запрашивать и получать из сети "Интернет" материалы развлекательного характера (игры, клипы и т.д.);

запрашивать и получать из сети "Интернет" программные продукты, кроме случаев, связанных со служебной необходимостью. При этом необходимо согласование с руководителем своего подразделения и администратором сети;

входить в другие компьютерные системы через сеть без разрешения администратора сети.

8.7. Работники не могут использовать в личных целях персональные данные, ставшие известными им вследствие выполнения служебных обязанностей.

9. Порядок обработки персональных данных без использования средств автоматизации:

9.1. 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 данных) на электронных носителях информации.

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

9.3. При неавтоматизированной обработке персональных данных на бумажных носителях:

не допускается фиксация на одном бумажном носителе персональных данных, цели обработки которых, заведомо несовместимы;

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;

дела с документами, содержащими персональные данные, должны иметь внутренние описи документов с указанием цели обработки и категории персональных данных.

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

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;

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);

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

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

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

9.6. 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).

9.7. При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению отдельной обработки персональных данных, в частности:

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;

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.

9.8. Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления

или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях, либо путем изготовления нового материального носителя с уточненными персональными данными.

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

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

III. ЦЕЛИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

10. Целью обработки персональных данных является:

осуществление возложенных на министерство федеральным законодательством, законодательством Ставропольского края и Положением о министерстве культуры Ставропольского края, утвержденным постановлением Правительства Ставропольского края от 16 августа 2012 г. № 296-п, полномочий и обязанностей по обеспечению проведения на территории Ставропольского края государственной политики и осуществлением управления, нормативно-правового регулирования в области культуры;

организация деятельности министерства для обеспечения соблюдения законов и иных нормативных правовых актов, реализации права на труд, права на пенсионное обеспечение и медицинское страхование работников министерства.

IV. СОДЕРЖАНИЕ ОБРАБАТЫВАЕМЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ

11. К персональным данным, обрабатываемым для достижения целей, указанных в подпункте 1 пункта 10 настоящих Правил (осуществление функций, полномочий и обязанностей по решению вопросов установленной сферы деятельности) относятся:

анкетные данные, включая адрес места жительства и проживания;

паспортные данные или данные иного документа, удостоверяющего личность и гражданство (включая серию, номер, дату выдачи, наименование органа, выдавшего документ);

сведения на родственников (когда это необходимо в случаях, установленных законом);

сведения о состоянии здоровья и наличии заболеваний (когда это необходимо в случаях, установленных законом);

сведения об отношении к воинской обязанности;

сведения об идентификационном номере налогоплательщика;
сведения о номере и серии страхового свидетельства государственного пенсионного страхования;
сведения о реквизитах банковского счета;
сведения о социальных льготах и о социальном статусе.

12. К персональным данным, обрабатываемым для достижения целей, указанных в подпункте 2 пункта 10 настоящих Правил (организация деятельности министерства для обеспечения соблюдения законов и иных нормативных правовых актов, реализации права на труд, права на пенсионное обеспечение и медицинское страхование работников министерства) относятся:

анкетные и биографические данные гражданина, включая адрес места жительства и проживания, контактный (сотовый) телефон;

паспортные данные или данные иного документа, удостоверяющего личность и гражданство (включая серию, номер, дату выдачи, наименование органа, выдавшего документ);

сведения об образовании, квалификации и о наличии специальных знаний или специальной подготовки (включая серию, номер, дату выдачи диплома, свидетельства, аттестата или другого документа об окончании образовательного учреждения, дату начала и завершения обучения);

сведения о трудовой деятельности, опыте работы, занимаемой должности, трудовом стаже, повышении квалификации и переподготовках;

сведения о номере, серии, дате выдачи трудовой книжки (вкладыша в неё) и записях в ней, содержание и реквизиты трудового договора (контракта);

сведения о составе семьи и наличии иждивенцев, их месте работы или учебы;

информация о допуске к государственной тайне;

сведения и заключения о состоянии здоровья установленной формы об отсутствии у гражданина заболеваний, препятствующих поступлению на государственную гражданскую службу или ее прохождению;

сведения и заключения установленной формы об отсутствии медицинских противопоказаний для работы со сведениями составляющими государственную тайну;

сведения об отношении к воинской обязанности;

сведения о доходах и обязательствах имущественного характера, в том числе супруги (супруга) и несовершеннолетних детей;

сведения об идентификационном номере налогоплательщика;

сведения о социальных льготах и о социальном статусе;

сведения о страховом полисе обязательного (добровольного) медицинского страхования;

сведения о номере и серии страхового свидетельства государственного пенсионного страхования;

реквизиты банковского счета;

национальность;

фотография.

V. КАТЕГОРИИ СУБЪЕКТОВ, ПЕРСОНАЛЬНЫЕ ДАННЫЕ КОТОРЫХ ОБРАБАТЫВАЮТСЯ

13. К субъектам, персональные данные которых обрабатываются, относятся:

граждане, обратившиеся в министерство с жалобами, заявлениями и по другим вопросам, касающимся установленной сферы деятельности;

граждане, претендующие на замещение должности государственной гражданской службы и должности технического (рабочего) персонала в министерстве;

граждане, замещающие (замещавшие) должности государственной гражданской службы, должности не отнесенные к государственной гражданской службе и должности технического (рабочего) персонала в министерстве.

VI. СРОКИ ОБРАБОТКИ И ХРАНЕНИЯ ОБРАБАТЫВАЕМЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ

14. Сроки обработки и хранения персональных данных определяются:

Приказом Минкультуры Российской Федерации от 25 августа 2010 г. № 558 «Об утверждении «Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения»;

сроком исковой давности;

иными требованиями законодательства Российской Федерации, нормативными правовыми актами Ставропольского края, нормативными правовыми актами министерства.

15. Особенности хранения персональных данных:

Если срок хранения персональных данных не установлен законодательством Российской Федерации, нормативными правовыми актами Ставропольского края, нормативными правовыми актами министерства или договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, то хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных.

VII. ПОРЯДОК УНИЧТОЖЕНИЯ ОБРАБОТАННЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ

16. Под уничтожением обработанных персональных данных понимаются действия, в результате которых невозможно восстановить содержание пер-

сональных данных в информационной системе персональных данных, или в результате которых уничтожаются материальные носители персональных данных.

17. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено действующим законодательством.

18. Порядок уничтожения обработанных персональных данных:

Уничтожению подлежат утратившие практическое значение и не имеющие исторической или иной ценности носители информации, содержащие персональные данные. При уничтожении таких носителей должно быть исключено ознакомление с ними посторонних лиц, неполное или случайное их уничтожение.

Уничтожение производится путем сжигания, расплавления, дробления, растворения, химического разложения или превращения в мягкую бесформенную массу или порошок. Допускается уничтожение документов путем измельчения в бумажную сечку. Магнитные и фотографические носители уничтожаются сжиганием, дроблением, расплавлением и другими способами, исключающими возможность их восстановления.

Уничтожение обработанных персональных данных производится комиссионно, с составлением соответствующего акта. Состав комиссии назначается приказом министра сроком на 1 год. В комиссию назначаются лица, допущенные к работе с персональными данными и являющиеся экспертами в различных областях деятельности министерства, имеющие непосредственное отношение к уничтожаемым материалам.

На документальные материалы, отобранные комиссией для уничтожения, составляется акт об уничтожении документов, который подписывается членами комиссии и утверждается министром.

Отобранные и включенные в акт об уничтожении документальные материалы после их сверки членами комиссии хранятся отдельно от других материалов.

Уничтожение документальных материалов, до утверждения акта об уничтожении документов министром, запрещается.

Уничтожение должно производиться в возможно короткий срок после утверждения министром акта об уничтожении документов.

19. Без оформления акта уничтожаются: испорченные бумажные и технические носители, черновики, проекты документов и другие материалы, образовавшиеся при исполнении документов, содержащих персональные данные.

В процедуру уничтожения документов и носителей информации без составления акта входит проведение следующих мероприятий:

разрывание листов, разрушение магнитного или иного технического носителя в присутствии исполнителя и руководителя подразделения, допущенных к обработке персональных данных;

накапливание остатков носителей в опечатываемом ящике (урне);

физическое уничтожение остатков носителей несколькими сотрудниками подразделения, допущенными к работе с персональными данными;

внесение отметок об уничтожении в учетные формы документов и носителей.
