

Утверждены приказом
МБУК «Централизованная
библиотечная система города
Пятигорска»

от «_11_» __апреля__ 2019_ г.
№ __23-осн__

ПРАВИЛА ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В В МУНИЦИПАЛЬНОМ БЮДЖЕТНОМ УЧРЕЖДЕНИИ КУЛЬТУРЫ «ЦЕНТРАЛИЗОВАННАЯ БИБЛИОТЕЧНАЯ СИСТЕМА ГОРОДА ПЯТИГОРСКА»

I. ОБЩИЕ ПОЛОЖЕНИЯ

1. Настоящие Правила обработки персональных данных в муниципального бюджетного учреждения культуры «Централизованная библиотечная система города Пятигорска» (далее – МБУК ЦБС) устанавливают единый порядок обработки персональных данных в муниципального бюджетного учреждения культуры «Централизованная библиотечная система города Пятигорска» (далее – МБУК ЦБС).

2. Обработка персональных данных в библиотеке 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 в 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 персональных данных.

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 библиотеке, а также полученные путем иных установленных законом способов, являются собственностью библиотеки и не могут быть использованы иначе, как с разрешения директора 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 библиотеке;
- 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 принятым в

соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора;

- оценка вреда, который может быть причинен субъектам персональных данных 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 на официальном сайте библиотеки.

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 библиотеки 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 библиотеке;
- 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 директора.

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

8.4. Руководители подразделений библиотеки 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 библиотеки; контролировать целевое использование работниками ресурсов сети «Интернет»; контролировать выполнение пользователями общих правил работы на ПЭВМ и в локальной вычислительной сети библиотеки (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 директору и поставить в известность лицо, ответственное за организацию обработки персональных данных; 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 библиотеке; 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; 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 отдела автоматизации; 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 перс ных должен использоваться отдельный материальный носитель для каждой категории персональных данных.

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 банных) на электронных носителях информации.

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

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 библиотеку федеральным законодательством, законодательством Ставропольского края и Уставом библиотеки, утвержденным приказом министерства культуры Ставропольского края, функций, полномочий и обязанностей по организации библиотечного обслуживания населения Ставропольского края, а также соблюдение пропускного режима, установленного правилами пользования библиотекой; обеспечение сохранности библиотечного фонда; обеспечение представления государственной статистической отчетности; организация деятельности библиотеки для обеспечения кадровой работы, в том числе в целях исполнения определенных сторонами условий трудового договора, обучения и карьерного роста, учета результатов исполнения работниками должностных обязанностей, обеспечения работникам библиотеки установленных законодательством Российской Федерации условий труда, гарантий и компенсаций.

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 организации библиотечного обслуживания населения Ставропольского края), относятся: фамилия, имя, отчество; число, месяц, год рождения; вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи; адрес; номер контактного телефона или сведения о других способах связи; сведения об образовании; сведения о месте работы или учебы; должность.

12. К персональным данным, обрабатываемым для достижения целей, указанных в подпункте 2 пункта 10 настоящих Правил (организация деятельности библиотеки для обеспечения кадровой работы), относятся: фамилия, имя, отчество; год рождения; месяц рождения; дата рождения; место рождения; информация о гражданстве; вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи; адрес; номер контактного телефона или сведения о других способах связи; реквизиты страхового свидетельства государственного пенсионного страхования; идентификационный номер налогоплательщика; реквизиты свидетельства государственной регистрации актов гражданского состояния; семейное положение; сведения о трудовой деятельности (место работы, должность, профессия); сведения о воинском учете и реквизиты документов воинского учета; сведения об образовании; сведения об ученой степени; информация о владении иностранными языками, степень владения; фотография; сведения о прежнем месте работы; информация, содержащаяся в трудовом договоре, дополнительных соглашениях к трудовому договору; сведения о пребывании за границей; данные о государственных наградах, иных наградах, знаках отличия; сведения о профессиональной переподготовке и (или) повышении квалификации; информация о ежегодных оплачиваемых отпусках, учебных отпусках и отпусках без сохранения заработной платы; сведения о доходах; номер расчетного счета; иные персональные данные, необходимые для достижения целей, предусмотренных в подпункте 2 пункта 10 настоящих Правил.

V. КАТЕГОРИИ СУБЪЕКТОВ, ПЕРСОНАЛЬНЫЕ ДАННЫЕ КОТОРЫХ ОБРАБАТЫВАЮТСЯ

13. К субъектам, персональные данные которых обрабатываются, относятся: граждане, обратившиеся в библиотеку за предоставлением во временное пользование библиотечных фондов и по другим вопросам, касающимся установленной сферы деятельности (пользователи библиотеки); граждане, работающие (работавшие) в библиотеке (работники), а также

граждане с ними связанные, чьи данные необходимо обрабатывать в соответствии с трудовым и иным законодательством.

VI. СРОКИ ОБРАБОТКИ И ХРАНЕНИЯ ОБРАБАТЫВАЕМЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ

14. Обработка персональных данных работников библиотеки осуществляется в течение всего периода работы в библиотеке. Обработка персональных данных пользователей библиотеки осуществляется в течение всего периода обслуживания пользователей в библиотеке.

15. Сроки хранения документов на бумажных носителях, содержащих персональные данные работников библиотеки, определяются в соответствии с Перечнем типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения, утвержденным приказом Министерства культуры Российской Федерации от 25 августа 2010 г. № 558 (далее - Перечень архивных документов). Документы на бумажных носителях, содержащие персональные данные пользователей библиотеки, хранятся в отделе контроля, регистрации и учета в течение пяти лет с момента последней перерегистрации пользователя с последующим уничтожением.

16. Срок хранения персональных данных, внесенных в информационные системы персональных данных библиотеки, должен соответствовать сроку хранения бумажных оригиналов.

17. Если срок хранения персональных данных не установлен законодательством Российской Федерации, нормативными правовыми актами Ставропольского края, нормативными правовыми актами библиотеки 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

18. Под уничтожением обработанных персональных данных понимаются 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.

19. 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.

20. Уничтожение производится путем сожжения, дробления, растворения, химического разложения или превращения в мягкую бесформенную массу или порошок. Допускается уничтожение документов путем измельчения в бумажную сечку. Уничтожение обработанных персональных данных производится комиссионно, с составлением соответствующего акта. Состав комиссии назначается приказом директора. В комиссию назначаются лица, допущенные к работе с персональными данными и являющиеся экспертами в различных областях деятельности библиотеки, имеющие непосредственное отношение к уничтожаемым материалам. На документальные материалы, отобранные комиссией для уничтожения, составляется Акт о выделении к уничтожению документов, который подписывается членами комиссии и утверждается директором. Отобранные и включенные в Акт о выделении к уничтожению документов документальные материалы после их сверки членами комиссии хранятся отдельно от других материалов. Уничтожение должно производиться в возможно короткий срок после утверждения директором Акта о выделении к уничтожению документов. По окончании процедуры уничтожения составляется соответствующий Акт об уничтожении документов, содержащих персональные данные.

21. 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.

22. Уничтожение по окончании срока обработки персональных данных на электронных носителях производится путем механического нарушения целостности носителя, не позволяющего произвести считывание или восстановление персональных данных, или удалением с электронных носителей методами и средствами гарантированного удаления остаточной информации.