АДМИНИСТРАЦИЯ ТАМБОВСКОЙ ОБЛАСТИ
ТАМБОВСКОЕ ОБЛАСТНОЕ ГОСУДАРСТВЕННОЕ КАЗЕННОЕ УЧРЕЖДЕНИЕ
«МНОГОФУНКЦИОНАЛЬНЫЙ ЦЕНТР ПРЕДОСТАВЛЕНИЯ ГОСУДАРСТВЕННЫХ И МУНИЦИПАЛЬНЫХ УСЛУГ»
(ТОГКУ «МФЦ»)

ПРИКАЗ

(с изм. от 09.07.2015 № 345-од)

« 26» ____06_____201 5г. № 31

г. Тамбов

Об утверждении документов по организации работ
по защите персональных данных в ТОГКУ «МФЦ»

Во исполнение требований Трудового Кодекса РФ, Федерального закона Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных», Постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», нормативно-методического документа «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)», утвержденного приказом Гостехкомиссии России от 30.08.2002 № 282, руководящих документов ФСТЭК РФ по защите информации, содержащей персональные данные и в целях обеспечения защиты информации и режима безопасности персональных данных работников учреждения и лиц, обращающихся за получением государственных и муниципальных услуг в ТОГКУ «МФЦ»,

ПРИКАЗЫВАЮ:

1. Приказы директора ТОГКУ «МФЦ» от 25.12. 2013 № 41 «Об утверждении списка лиц, имеющих право самостоятельного доступа в помещение», от 25.12.2013 № 43 «Об утверждении Положения об организации и проведении работ и Политики обработки персональных данных», от 15.04.2015 № 20.1-од «Об утверждении Положения о работе с персональными данными работников ТОГКУ «МФЦ» и Положения о работе с персональными данными физических лиц, обращающихся к работникам МФЦ за предоставлением услуг по принципу «одного окна» признать утратившими силу.

2. Утвердить Положение о порядке обработки персональных данных (ПДн) в ТОГКУ «МФЦ» (Приложению № 1).

3. Утвердить Правила обработки ПДн в ТОГКУ «МФЦ» (Приложение № 2.)

4.Утвердить Список лиц, допущенных к обработке ПДн и имеющих право самостоятельного доступа в помещения, в которых ведется обработка ПДн (Приложение № 3).

5. Утвердить Правила запросов субъектов ПДн и их представителей с приложением типовых форм документов (Приложение № 4).

6. Утвердить Правила осуществления внутреннего контроля соответствия обработки ПДн требованиям к защите ПДн в ТОГКУ «МФЦ» (Приложение № 5).

7. Утвердить Правила работы с обезличенными ПДн в ТОГКУ «МФЦ» (Приложение № 6).

8. Утвердить форму Согласия работников ТОГКУ «МФЦ» на обработку ПДн (Приложение № 7).

9. Утвердить форму Обязательства работника ТОГКУ «МФЦ»о неразглашении ПДн субъекта (Приложение № 8.)

10. Утвердить Перечень ПДн, обрабатываемых в связи с реализацией трудовых отношений (Приложение № 9).

11. Утвердить Перечень ПДн, обрабатываемых в связи с оказанием государственных услуг (Приложение № 10).

12. Утвердить Перечень должностей работников ТОГКУ «МФЦ», ответственных за проведение мероприятий по обезличиванию обрабатываемых ПДн (Приложение № 11).

13. Утвердить Перечень должностей работников, имеющих доступ к ПДн работников учреждения (Приложение № 12).

14. Утвердить Перечень должностей работников, имеющих доступ к ПДн заявителей (Приложение № 13).

15. Утвердить Порядок доступа работников МФЦ в помещения, в которых ведется обработка ПДн (Приложение № 14).

16. Утвердить Лист ознакомления работников ТОГКУ «МФЦ» с документами, устанавливающими порядок обработки ПДн в учреждении (Приложение № 15).

17. Утвердить Инструкцию пользователя автоматизированной системы при работе с ПДн (Приложение № 16).

18. Утвердить Парольную политику ТОГКУ «МФЦ» (Приложение № 17).

19. Секретарю руководителя (С.Е. Салыкина) ознакомить с настоящим приказом заинтересованных лиц под роспись.

Директор ТОГКУ «МФЦ» Н.Д. Тихонова

ПРИЛОЖЕНИЕ № 1
УТВЕРЖДЕНО
приказом ТОГКУ «МФЦ»
от _____ № _____

Положение
об обработке персональных данных в ТОГКУ «МФЦ»

1. Общие положения

1.1. Положение об обработке персональных данных в ТОГКУ «МФЦ» (далее - Положение) разработано в соответствии с Трудовым кодексом Российской Федерации, Федеральным законом от 27 июля 2004 г. № 79-ФЗ "О государственной гражданской службе Российской Федерации", Федеральным законом от 27 июля 2006 г. № 149-ФЗ "Об информации, информационных технологиях и защите информации», Федеральным законом от 27 июля 2006 г. № 152-ФЗ "О персональных данных", постановлением Правительства Российской Федерации от 06 июля 2008 г. № 512 "Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных", постановлением Правительства Российской Федерации от 17 ноября 2007 г. № 781 "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных", постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации".

1.2. Положение определяет порядок и условия обработки персональных данных в ТОГКУ «МФЦ» с использованием средств автоматизации и без использования таких средств.

1.3. Обработка персональных данных в ТОГКУ «МФЦ» осуществляется в целях исполнения полномочий учреждения по ведению кадровой работы, в обучении и должностном росте, обеспечения личной безопасности работников и членов его семьи, финансового обеспечения его трудовой деятельности, учета результатов исполнения им должностных обязанностей.

2. Порядок обработки персональных данных работников ТОГКУ «МФЦ»и иных лиц.

2.1. Обработка персональных данных работников МФЦ и иных лиц (под иными лицами подразумеваются субъекты персональных данных) осуществляется с согласия субъектов персональных данных, которое действует со дня поступления на работу и на время работы для работников МФЦ, или со дня подачи обращения заявителем до достижения цели обработки персональных данных для иных лиц.

2.2. Работники кадровой службы учреждения, аппарат управления, начальники отделов ТОГКУ «МФЦ» обеспечивают защиту персональных данных, содержащихся в личных делах и субъектов персональных данных, и в информационных системах, от неправомерного их использования или утраты.

2.3. Обработка персональных данных субъектов персональных данных осуществляется как с использованием средств автоматизации, так и без использования таких средств.

2.4. При обработке персональных данных субъектов персональных данных в целях реализации возложенных на учреждение (далее - оператор) полномочий уполномоченные должностные лица обязаны соблюдать следующие требования:

- объем и характер обрабатываемых персональных данных, способы обработки персональных данных должны соответствовать целям обработки персональных данных;

- защита персональных данных субъектов персональных данных от неправомерного их использования или уничтожения обеспечивается в порядке, установленном нормативными правовыми актами Российской Федерации;
- передача персональных данных субъектов персональных данных третьей стороне не допускается без их письменного согласия, за исключением случаев, установленных федеральными законами. В случае если лицо, обратившееся с запросом, не обладает соответствующими полномочиями на получение персональных данных субъекта персональных данных, либо отсутствует письменное согласие субъекта персональных данных на передачу его персональных данных, оператор вправе отказать в предоставлении персональных данных. В этом случае лицу, обратившемуся с запросом, направляется письменный мотивированный отказ в предоставлении запрашиваемой информации;
- обеспечение конфиденциальности персональных данных субъектов персональных данных, за исключением случаев обезличивания персональных данных и в отношении общедоступных персональных данных;
- хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки. Указанные сведения подлежат уничтожению по достижении цели обработки или в случае утраты необходимости в их достижении, если иное не установлено законодательством Российской Федерации. Факт уничтожения персональных данных оформляется соответствующим актом;
- опубликование и распространение персональных данных субъектов персональных данных допускается в случаях, установленных законодательством Российской Федерации.

2.5. Обработка биометрических и специальных категорий персональных данных субъектов персональных данных осуществляется с их письменного согласия, за исключением случаев, предусмотренных законодательством Российской Федерации в области персональных данных. Использование и хранение биометрических и специальных категорий персональных данных вне информационных систем персональных данных может осуществляться только на таких материальных носителях информации и с применением такой технологии ее хранения, которые обеспечивают защиту этих данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения.

2.6. При переводе или назначении работника в другое учреждение (орган) его личное дело передается в это учреждение (орган) по новому месту работы по письменному запросу соответствующего учреждения.

3. Порядок обработки персональных данных субъектов персональных данных, осуществляемой без использования средств автоматизации

3.1. При обработке персональных данных без использования средств автоматизации уполномоченными должностными лицами не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо несовместимы.

3.2. При разработке и использовании типовых форм документов, необходимых для реализации возложенных на ТОГКУ «МФЦ» полномочий, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовая форма), должны соблюдаться следующие условия:

- типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, адрес ТОГКУ «МФЦ» фамилию, имя, отчество и адрес субъекта персональных данных, чьи персональные данные вносятся в указанную типовую форму, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки;
- типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации, при необходимости получения согласия на обработку персональных данных;

- типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, чьи персональные данные содержатся в типовой форме, при ознакомлении со своими персональными данными не имел возможности доступа к персональным данным иных лиц, содержащимся в указанной типовой форме;
- типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

3.3. Уничтожение или обезличивание 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).

3.4. Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем изготовления нового материального носителя с уточненными персональными данными.

4. Порядок обработки персональных данных субъектов персональных данных в информационных системах

4.1. Обработка персональных данных в ТОГКУ «МФЦ»осуществляется:

4.1.1. в электронной базе данных заявителей МФЦ, включающей:

- фамилию, имя, отчество субъекта персональных данных;
- дату рождения субъекта персональных данных;
- адрес места жительства субъекта персональных данных;
- данные документа удостоверяющего личность;
- должность субъекта персональных данных;
- телефон субъекта персональных данных;
- ИНН субъекта персональных данных;
- СНИЛС
- сведения о правоустанавливающих и правоудостоверяющих документах.

4.1.2. в электронной базе данных «Реестр работников МФЦ», включающей:

- фамилию, имя, отчество субъекта персональных данных;
- дату рождения субъекта персональных данных;
- должность субъекта персональных данных;
- номер правового акта и дату приема на работу (увольнения) субъекта персональных данных;
- сведения о трудовом стаже субъекта персональных данных;
- сведения об образовании субъекта персональных данных;
- сведения о повышении квалификации субъекта персональных данных;
- сведения об ученой степени субъекта персональных данных;
- сведения об аттестации субъекта персональных данных;
- сведения о государственных наградах субъекта персональных данных;
- сведения о воинском учете субъекта персональных данных;
- вид служебного контракта субъекта персональных данных;
- данные о включении в кадровый резерв субъекта персональных данных;
- основания исключения из резерва субъекта персональных данных;

4.1.3. в электронной базе данных "Резерв кадров", включающей:

- фамилию, имя, отчество субъекта персональных данных;
- сведения о документе, удостоверяющем личность субъекта персональных данных;
- дату и место рождения субъекта персональных данных;
- адрес места жительства субъекта персональных данных;
- почтовый адрес субъекта персональных данных;
- должность субъекта персональных данных;

- номер правового акта и дату приема на работу (увольнения) субъекта персональных данных;
- сведения о трудовом стаже субъекта персональных данных;
- телефон субъекта персональных данных;
- факс субъекта персональных данных;
- адрес электронной почты субъекта персональных данных;
- анкетные и биографические данные субъекта персональных данных;
- сведения об образовании субъекта персональных данных;
- семейное положение субъекта персональных данных;

4.1.4. в информационной системе бухгалтерского учета и отчетности "1С: Предприятие. Зарплата и кадры", включающей:

- фамилию, имя, отчество субъекта персональных данных;
- сведения о документе, удостоверяющем личность субъекта персональных данных;
- дату рождения субъекта персональных данных;
- адрес места жительства субъекта персональных данных;
- табельный номер субъекта персональных данных;
- должность субъекта персональных данных;
- сведения о суммах перечисленных в Пенсионный фонд России страховых взносов субъекта персональных данных;
- сведения о суммах выплаченных страховых взносов субъекту персональных данных;
- сведения о сумме заработной платы субъекта персональных данных;
- сведения о сумме льгот субъекта персональных данных;
- сведения о сумме доходов субъекта персональных данных;
- сведения о суммах, удержанных с субъекта персональных данных;
- дату и номер страхового свидетельства государственного пенсионного страхования субъекта персональных данных;
- ИНН субъекта персональных данных;
- сведения о количестве детей субъекта персональных данных до 18 лет;
- сведения о количестве детей субъекта персональных данных до 23 лет, обучающихся по очной форме обучения;

4.2. Персональные данные могут быть предоставлены для ознакомления:

Работникам ТОГКУ «МФЦ», допущенным к обработке персональных данных с использованием средств автоматизации в части, касающейся исполнения их должностных обязанностей;

уполномоченным работникам органов исполнительной власти в порядке, установленном законодательством Российской Федерации.

4.3. Безопасность персональных данных, обрабатываемых с использованием средств автоматизации, достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным.

4.4. Уполномоченными должностными лицами, при обработке персональных данных в информационных системах персональных данных, должна быть обеспечена их безопасность с помощью системы защиты, включающей организационные меры и средства защиты информации, в том числе шифровальные (криптографические) средства.

4.5. Обмен персональными данными при их обработке в информационных системах осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и путем применения программных и технических средств.

4.6. Самостоятельное подключение средств вычислительной техники, применяемых для хранения, обработки или передачи персональных данных к информационно-телекоммуникационным сетям, позволяющим осуществлять передачу информации через государственную границу Российской Федерации, в том числе к информационно-телекоммуникационной сети Интернет, не допускается.

4.7. Обслуживание информационных систем персональных данных допускается сторонними организациями при наличии договора и согласия о конфиденциальности.

4.8. Доступ пользователей (операторов информационной системы) к персональным данным в информационной системе персональных данных ТОГКУ «МФЦ» (далее — ИСПДн) должен требовать обязательного прохождения процедуры идентификации и аутентификации.

4.9. Лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

4.10. Должностными лицами ТОГКУ «МФЦ», ответственными за обеспечение безопасности персональных данных при их обработке в информационных системах, должно быть обеспечено:

- своевременное обнаружение фактов несанкционированного доступа к персональным данным и немедленное доведение этой информации до руководства учреждения;
- недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;
- незамедлительное восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- проведение контроля за обеспечением уровня защищенности персональных данных;
- соблюдение условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;
- ведение учета применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;
- незамедлительное приостановление предоставления персональных данных пользователям информационной системы при обнаружении нарушений порядка предоставления персональных данных до выявления причин нарушений и устранения этих причин;
- расследование и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации (СЗИ), которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений.

5. Обязанности субъектов персональных данных и оператора

Для того, чтобы обеспечить достоверность персональных данных, субъекты персональных данных обязаны предоставлять оператору сведения о себе. В случае изменений сведений, составляющих персональные данные (фамилия, имя, отчество, адрес, паспортные данные, сведения об образовании, состоянии здоровья (при выявлении противопоказаний для исполнения обязанностей, обусловленных служебным контрактом) и т.д.), субъект персональных данных обязан своевременно сообщить об этом оператору.

Оператор обязан:

- обеспечить хранение первичной учетной документации по учету труда и его оплаты;
- вести учет передачи персональных данных третьим лицам;
- обеспечить сохранность документов по личному составу и передачу их на государственное хранение в случае реорганизации или ликвидации ТОГКУ «МФЦ»

6. Должностные обязанности лиц, ответственных за организацию, разработку, обеспечение и выполнение мероприятий по защите персональных данных в ТОГКУ «МФЦ»

6.1. Должностными лицами, ответственными за организацию, разработку, обеспечение и выполнение мероприятий по защите персональных данных в ТОГКУ «МФЦ», являются:

- руководители структурных подразделений;
- администратор защиты (безопасности) ИСПДн;
- пользователи ИСПДн.

6.2. Руководитель подразделения отвечает за организацию работ по обеспечению безопасности персональных данных, обрабатываемых в подразделении.

Руководитель подразделения обязан:

- организовывать разработку мероприятий, связанных с обработкой персональных данных;
- организовывать разработку предложений по размещению (расположению) технических средств, входящих в состав ИСПДн, подлежащих аттестации по требованиям безопасности информации;
- разрабатывать и представлять на утверждение ТОГКУ «МФЦ» предложения о назначении ответственных за обработку и защиту (обеспечение безопасности) персональных данных;
- контролировать порядок эксплуатации СВТ и СЗИ;
- организовывать разработку разрешительной системы доступа к информационным ресурсам, программным и техническим средствам ИСПДн, подлежащей аттестации по требованиям безопасности информации;
- организовывать работу по классификации ИСПДн;
- организовывать разработку организационно-методических документов (инструкций, памяток и т.п.) по защите персональных данных;
- участвовать в проведении аттестационных испытаний ИСПДн;
- организовывать периодический контроль работоспособности средств защиты персональных данных;
- контролировать выполнение правил разграничения доступа к техническим средствам и персональным данным на объекте информатизации;
- контролировать установленный порядок обращения со съемными машинными и бумажными носителями информации.

6.4. Администратор защиты (безопасности) ИСПДн (далее - администратор безопасности) назначается из числа работников подразделений, в функции которых входит защита информации ограниченного доступа, по представлению руководителя подразделения. Администратор безопасности непосредственно подчиняется руководителю подразделения.

Администратор безопасности отвечает за соблюдение требований по обеспечению безопасности информации, порядка обращения с машинными носителями информации и правильность применения средств защиты персональных данных.

При этом администратор безопасности в своей работе руководствуется документами, регламентирующими защиту персональных данных от утечки по техническим каналам и НСД, утвержденной инструкцией администратору безопасности ИСПДн и эксплуатационной документацией на установленные на объекте информатизации системы защиты от несанкционированного доступа к информации и от утечки информации по техническим каналам.

На администратора безопасности возлагается непосредственный контроль за обеспечением безопасности выполняемых работ по обработке персональных данных и требований инструкции.

Администратор безопасности обязан:

- разрабатывать предложения по составу общесистемных программных средств, обеспечивающих функционирование ИСПДн, подлежащей аттестации по требованиям безопасности информации;
- разрабатывать предложения по разграничению доступа к информационным ресурсам, программным и техническим средствам ИСПДн, подлежащей аттестации по требованиям безопасности информации;
- определять класс защищенности ИСПДн, подлежащей аттестации по требованиям безопасности информации;
- участвовать и контролировать проведение аттестационных испытаний ИСПДн;
- знать способы, методы и средства защиты персональных данных от НСД;
- знать перечень задач по обработке персональных данных и пользователей, допущенных к их решению;
- вести технический паспорт объекта информатизации;

- осуществлять допуск пользователей к техническим средствам ИСПДн и информации в соответствии с разрешительной системой доступа;
- ежеквартально проводить занятия с пользователями ИСПДн, доводить основные положения нормативных, правовых и руководящих документов по вопросам защиты (обеспечению безопасности) персональных данных;
- контролировать ведение журнала приема-передачи СВТ и учета времени обработки информации на аттестованной по требованиям безопасности ИСПДн;
- еженедельно проверять системный журнал регистрации событий на предмет попыток НСД к информации;
- контролировать своевременность представления списков пользователей**,** допускаемых к обработке персональных данных, с целью закрепления за ними паролей, а также прав пользования ресурсами ИСПДн;
- обеспечивать (осуществлять) смену и ввод пароля для разграничения доступа к информационным ресурсам пользователей, вести учет, хранение, закрепление и выдачу паролей доступа к техническим средствам и информационным ресурсам ИСПДн;
- периодически тестировать все функции системы разграничения доступа к информации;
- осуществлять визуальный контроль целостности компонентов СВТ, а также целостность элементов контроля НСД к внутренним узлам и блокам СВТ;
- осуществлять проверку на наличие компьютерных "вирусов";
- своевременно обновлять базы антивирусных программ;
- контролировать правильность применения и работоспособность средств защиты информации от НСД;
- докладывать руководителю подразделения, ответственного за эксплуатацию ИСПДн, о нарушениях или невыполнении пользователями требований по защите (обеспечению безопасности) персональных данных и правил обращения со съемными машинными носителями информации;
- регулярно создавать резервные копии системных файлов и обрабатываемых данных, подлежащих хранению, на специально учтенных съемных машинных носителях информации.

6.5. Пользователь ИСПДн отвечает за техническое состояние СВТ, обрабатывающих персональные данные, установленный порядок использования программного обеспечения, а также применение технических и программных СЗИ.

При этом пользователь ИСПДн в своей работе руководствуется документами, регламентирующими защиту персональных данных от утечки по техническим каналам и НСД, утвержденной инструкцией пользователю ИСПДн и эксплуатационной документацией на установленные на объекте информатизации системы защиты от НСД к информации и от утечки информации по техническим каналам.

Пользователь ИСПДн обязан:

- знать требования документов по защите (обеспечению безопасности) персональных данных;
- вести журнал приема-передачи СВТ и учета времени обработки информации на аттестованной по требованиям безопасности ИСПДн;
- использовать для работы только учтенные съемные машинные носители информации;
- соблюдать утвержденную разрешительную систему доступа к техническим средствам и информации;
- докладывать администратору безопасности ИСПДн и информировать руководителя подразделения, ответственного за эксплуатацию объекта информатизации, о выявленных изменениях в конфигурации технических средств и программного обеспечения ИСПДн;
- немедленно докладывать администратору безопасности и информировать руководителя подразделения, ответственного за эксплуатацию объекта информатизации, о фактах и попытках НСД к обрабатываемой (хранящейся) в АС информации, нарушениях, выявленных системой антивирусной защиты.

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

В случае выявления нарушений порядка обработки персональных данных в ИСПДн ТОГКУ «МФЦ» уполномоченными должностными лицами принимаются меры по установлению причин нарушений и их устранению. Лица, виновные в нарушениях норм, регулирующих получение, обработку и защиту персональных данных работников МФЦ и иных лиц, в соответствии со статьей 24 Федерального закона "О персональных данных" несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

ПРИЛОЖЕНИЕ № 2
УТВЕРЖДЕНО
приказом ТОГКУ «МФЦ»
от _____ № _____

Правила
обработки персональных данных в ТОГКУ «МФЦ»

1. Общие положения

Настоящие Правила обработки персональных данных в ТОГКУ «МФЦ» (далее - Правила) устанавливают процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных (ПДн), а также определяющие для каждой цели обработки ПДн содержание обрабатываемых ПДн, категории субъектов, ПДн которых обрабатываются, сроки их обработки и хранения; порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований.

Правила разработаны в соответствии с Федеральным законом от 27 июля 2006 г. № 152 - ФЗ "О персональных данных" (далее - Федеральный закон), Трудовым кодексом Российской Федерации, постановлением Правительства Российской Федерации от 21 марта 2012 г. № 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами" и другими нормативными правовыми актами.

При организации обработки и защиты ПДн необходимо руководствоваться следующими документами:

Федеральным законом от 27 июля 2006 г. № 149 - ФЗ "Об информации, информационных технологиях и о защите информации";

Федеральным законом от 27 июля 2006 г. № 152 - ФЗ "О персональных данных";

Требованиями к защите персональных данных при их обработке в информационных системах персональных данных (утверждены постановлением Правительства Российской Федерации от 01 ноября 2012 г. № 1119);

Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации (утверждено постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687);

Положением по аттестации объектов информатизации по требованиям безопасности информации (утверждено председателем Государственной технической комиссии при Президенте Российской Федерации 25 ноября 1994 г.);

Специальными требованиями и рекомендациями по технической защите конфиденциальной информации (утверждены приказом председателя Гостехкомиссии России от 30 августа 2002 г. № 282);

нормативными и методическими документами по технической защите информации Гостехкомиссии России, ФСТЭК России и ФСБ России.

2. Категории субъектов персональных данных

В ТОГКУ «МФЦ» осуществляется обработка ПДн следующих категорий лиц (далее - субъект персональных данных):

- заявителей в рамках получения ими государственных и муниципальных услуг;
- работников ТОГКУ «МФЦ» в рамках трудовых отношений;
- посетителей, обращающихся по личным вопросам к руководству МФЦ

3. Принципы обработки персональных данных

Обработка ПДн в ТОГКУ «МФЦ» должна осуществляться на основе следующих принципов:

- обработки ПДн на законной и справедливой основе;
- ограничения обработки ПДн при достижении конкретных, заранее определенных и законных целей;
- недопущения объединения баз данных, содержащих ПДн, обработка которых осуществляется в целях, несовместимых между собой;
- обработки ПДн субъектов персональных данных, которые отвечают целям их обработки;
- соответствия содержания и объема обрабатываемых ПДн заявленным целям обработки;
- исключения избыточности обрабатываемых ПДн по отношению к заявленным целям их обработки;
- обеспечения точности, достаточности и актуальности ПДн по отношению к целям обработки ПДн;
- обеспечения принятия необходимых мер оператором при удалении или уточнении неполных или неточных данных;
- осуществления хранения ПДн оператором в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен федеральным законом или договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных;
- уничтожения либо обезличивания ПДн по достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом;
- обеспечения защиты прав и свобод человека и гражданина при обработке его ПДн, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну;
- обязанности лица, осуществляющего обработку ПДн по поручению оператора, соблюдать принципы и правила обработки ПДн;
- соблюдения принципов и правил обработки ПДн при поручении такой обработки другому лицу;
- соблюдения конфиденциальности ПДн;
- обработки ПДн (в том числе при обработке общедоступных ПДн, специальных категорий ПДн, биометрических ПДн, при принятии решений на основании исключительно автоматизированной обработки ПДн, при трансграничной передаче ПДн) с письменного согласия субъектов персональных данных либо на ином законном основании;
- соблюдения законности при осуществлении трансграничной передачи ПДн;
- соблюдения обязанностей, возлагаемых на учреждение действующим законодательством и иными нормативными актами по обработке ПДн;
- принятия мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных законодательством в области ПДн;
- принятия необходимых правовых, организационных и технических мер или обеспечение их принятия для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн;
- недопустимости ограничения прав и свобод человека и гражданина по мотивам, связанным с использованием различных способов обработки ПДн или обозначения принадлежности ПДн, содержащихся в государственных информационных системах персональных данных (ИСПДн), конкретному субъекту персональных данных;
- недопустимости использования оскорбляющих чувства граждан или унижающих человеческое достоинство способов обозначения принадлежности ПДн, содержащихся в государственных ИСПДн, конкретному субъекту персональных данных;
- личной ответственности должностных лиц, осуществляющих обработку ПДн;
- документального оформления всех принятых решений по обработке и обеспечению безопасности ПДн.

4. Цели обработки персональных данных

ТОГКУ «МФЦ», являясь оператором ПДн, должна определять цели обработки ПДн.

Цели обработки ПДн должны быть четко определены и соответствовать:

заявленным в Уставе учреждения, регламенте и положениях о структурных подразделениях МФЦ основным полномочиям и правам;

задачам и функциям структурных подразделений (должностных лиц) ТОГКУ «МФЦ», указанным в положениях о таких структурных подразделениях (должностных регламентах).

Цели обработки ПДн определяют:

- содержание и объем обрабатываемых ПДн;
- категории субъектов, персональные данные которых обрабатываются;
- сроки их обработки и хранения;
- порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований.

Цели обработки ПДн должны быть:

- конкретны;
- заранее определены;
- законны;
- заявлены.

Обработка ПДн в ТОГКУ «МФЦ» осуществляется для следующих целей:

- исполнения полномочий по ведению кадровой работы, содействия работникам МФЦ в обучении и должностном росте, обеспечения его личной безопасности и членов его семьи, финансового обеспечения его трудовой деятельности, учета результатов исполнения им должностных обязанностей;
- учета документов кандидатов на замещение вакантных должностей в ТОГКУ «МФЦ»
- формирования и подготовки кадрового резерва;
- систематизации данных о гражданах, обращающихся по различным вопросам к руководству МФЦ;
- обеспечения полномочий по вопросам предоставления государственных и муниципальных услуг

Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

5. Способы и правила обработки персональных данных в ИСПДн в зависимости от применения средств автоматизации

Способы обработки ПДн в ИСПДн:

1. обработка ПДн без использования средств автоматизации;
2. обработка ПДн с использованием средств автоматизации.

5.1. Правила обработки персональных данных без использования средств автоматизации

Для обработки различных категорий ПДн, осуществляемой без использования средств автоматизации, для каждой категории ПДн должен использоваться отдельный материальный носитель.

При фиксации ПДн на материальных носителях не допускается фиксация на одном материальном носителе ПДн, цели обработки которых заведомо не совместимы.

При несовместимости целей обработки ПДн, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку ПДн отдельно от других зафиксированных на том же носителе ПДн, должны быть приняты меры по обеспечению раздельной обработки ПДн, в частности, при необходимости использования или распространения определенных ПДн отдельно от находящихся на том же материальном носителе других ПДн, осуществляется копирование ПДн, подлежащих распространению или использованию, способом, исключающим одновременное копирование ПДн, не подлежащих распространению и использованию, и используется (распространяется) копия ПДн.

При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них ПДн, должны соблюдаться следующие условия:

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

сведения о цели обработки ПДн, осуществляемой без использования средств автоматизации;

имя (наименование) и адрес оператора;

фамилию, имя, отчество и адрес субъекта персональных данных, источник получения ПДн;

сроки обработки ПДн;

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

общее описание используемых оператором способов обработки ПДн;

типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку ПДн, осуществляемую без использования средств автоматизации, при необходимости получения письменного согласия на обработку ПДн;

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 ПДн, цели обработки которых заведомо не совместимы.

Уточнение ПДн 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.

5.2. Правила обработки персональных данных средствами автоматизации

Обработка ПДн средствами автоматизации в ТОГКУ «МФЦ» допускается в следующих случаях:

обработка ПДн осуществляется с согласия субъекта персональных данных на обработку его персональных данных;

обработка ПДн необходима для достижения целей, предусмотренных законом, для осуществления и выполнения возложенных законодательством Российской Федерации на ТОГКУ «МФЦ» функций, полномочий и обязанностей;

обработка ПДн необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;

обработка ПДн необходима для осуществления прав и законных интересов МФЦ или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

обработка ПДн осуществляется в статистических или иных исследовательских целях при условии обязательного обезличивания ПДн;

осуществляется обработка ПДн, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе (персональные данные, сделанные общедоступными субъектом персональных данных);

осуществляется обработка ПДн, подлежащих опубликованию или обязательному раскрытию в соответствии с Федеральным законом.

Обработка ПДн средствами автоматизации должна осуществляться на основании правил, инструкций, руководств, регламентов и иных документов, определяющих технологический процесс обработки информации, содержащей такие данные, определенных для выполнения конкретных операций с заранее определенными целями, с учетом требований настоящих Правил.

6. Обработка персональных данных с согласия субъекта персональных данных

В случае если обработка ПДн субъекта персональных данных в ИСПДн осуществляется на основании согласия и не имеется оснований для обработки таких ПДн без получения согласия, должны выполняться указанные в настоящем пункте правила.

Субъект персональных данных принимает решение о предоставлении его ПДн и дает согласие на их обработку свободно, своей волей и в своем интересе.

Согласие на обработку ПДн должно быть:

- конкретным;
- информированным;
- сознательным.

Согласие на обработку ПДн ТОГКУ «МФЦ» может быть дано субъектом персональных данных или его представителем только в письменной форме. Равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с Федеральным законом электронной подписью.

Получение согласия субъекта персональных данных в форме электронного документа на обработку его ПДн в целях предоставления государственных услуг, а также услуг, которые являются необходимыми и обязательными для предоставления государственных услуг, осуществляется в порядке, установленном Правительством Российской Федерации.

В случае получения согласия на обработку ПДн от представителя субъекта персональных данных полномочия данного представителя на дачу согласия от имени субъекта персональных данных проверяются оператором.

В случае недееспособности субъекта персональных данных согласие на обработку его ПДн дает законный представитель субъекта персональных данных.

В случае смерти субъекта персональных данных согласие на обработку его ПДн дают наследники субъекта персональных данных, если такое согласие не было дано субъектом персональных данных при его жизни.

В случае получения согласия от законного представителя субъекта персональных данных или наследников субъекта персональных данных они обязаны представить документы, подтверждающие их полномочия.

Допускается включение согласия в типовые формы (бланки) материальных носителей ПДн и в договор с субъектом персональных данных.

Письменные согласия субъектом персональных данных должны храниться в ТОГКУ «МФЦ».

Согласие на обработку ПДн может быть отозвано субъектом персональных данных путем направления запроса в учреждение.

7. Обработка персональных данных без согласия субъекта персональных данных

Обработка ПДн заявителей без получения согласия на такую обработку от субъекта персональных данных может осуществляться для предоставления государственных или муниципальных услуг по запросу заявителей, согласно п.4 ст.7 гл. 2 Федерального закона от 27.07.2010 № 210 ФЗ «Об организации предоставления государственных и муниципальных услуг».

8. Правила обработки персональных данных в ИСПДн в зависимости от категории обрабатываемых персональных данных

В ТОГКУ «МФЦ» устанавливаются следующие особые правила обработки ПДн в зависимости от категории обрабатываемых ПДн:

обработка специальных категорий ПДн;

обработка общедоступных ПДн.

8.1. Правила обработки специальных категорий персональных данных

К специальным категориям ПДн относятся сведения, касающиеся:

- расовой принадлежности;
- национальной принадлежности;
- политических взглядов;
- религиозных убеждений;
- философских убеждений;
- состояния здоровья;
- интимной жизни;
- судимости.

В ТОГКУ «МФЦ» разрешается обработка сведений специальных категорий ПДн в минимально необходимом объеме при обязательном соблюдении любого из следующих условий:

субъект персональных данных дал согласие в письменной форме на обработку своих ПДн;

обработка ПДн осуществляется в соответствии с законодательством о государственной социальной помощи, трудовым законодательством, законодательством Российской Федерации о пенсиях по государственному пенсионному обеспечению, о трудовых пенсиях;

обработка ПДн необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия субъекта персональных данных невозможно;

обработка ПДн необходима для установления или осуществления прав субъекта персональных данных или третьих лиц;

обработка ПДн осуществляется в соответствии с законодательством об обязательных видах страхования, страховым законодательством;

обработка ПДн о судимости осуществляется в пределах полномочий, предоставленных ТОГКУ «МФЦ» в соответствии с законодательством Российской Федерации.

Обработка специальных категорий ПДн в остальных случаях в ТОГКУ «МФЦ» не допускается.

Обработка специальных категорий ПДн должна быть незамедлительно прекращена, если устранены причины, вследствие которых осуществлялась обработка, если иное не установлено Федеральным законом.

.

8.2. Правила обработки общедоступных персональных данных

Общедоступные персональные данные физических лиц, полученные из сторонних общедоступных источников ПДн, в ТОГКУ «МФЦ» обрабатываются в исключительных случаях в сроки, не превышающие необходимые для их использования. При этом совместно с такими данными должны собираться реквизиты их источника и подтверждение согласия субъекта персональных данных на включение такой информации в общедоступные источники ПДн, так как в случае обработки общедоступных ПДн обязанность доказывания того, что обрабатываемые персональные данные являются общедоступными, возлагается на МФЦ. По достижении целей обработки общедоступных ПДн они подлежат немедленному уничтожению.

С целью информационного обеспечения и осуществления взаимодействия как внутри ТОГКУ «МФЦ», так и со сторонними физическими и юридическими лицами в учреждении могут создаваться общедоступные источники ПДн. Создание общедоступного источника ПДн осуществляется по решению директора ТОГКУ «МФЦ». В решении о создании общедоступного источника ПДн должны быть указаны:

цель создания общедоступного источника ПДн;

ссылка на нормативный акт, устанавливающий необходимость создания общедоступного источника ПДн (при наличии);

перечень ПДн, которые вносятся в общедоступный источник ПДн;

порядок включения ПДн в общедоступный источник ПДн;

порядок уведомления пользователей общедоступного источника ПДн об исключении из него ПДн либо внесении в него изменений;

порядок получения письменного согласия субъекта персональных данных на включение ПДн в общедоступный источник ПДн;

ссылка на нормативный акт, устанавливающий порядок исключения ПДн из общедоступного источника ПДн.

В общедоступный источник ПДн с письменного согласия субъекта персональных данных могут включаться: должность, фамилия, имя, отчество, абонентский номер рабочего телефона, место получения образования, достигнутые результаты и другая информация.

Включение в общедоступные источники персональных данных ПДн субъекта персональных данных допускается только на основании его письменного согласия.

Исключение ПДн из указанного общедоступного источника осуществляется при утрате необходимости в обработке таких данных, либо на основании заявления субъекта персональных данных в соответствии с действующим законодательством Российской Федерации.

9. Правила обработки персональных данных в ИСПДн в зависимости от цели обработки персональных данных

В ТОГКУ «МФЦ» устанавливаются следующие особые правила обработки ПДн в зависимости от цели обработки ПДн:

правила обработки ПДн субъекта с целью его однократного обращения;

правила работы с обезличенными данными.

9.1. Правила обработки персональных данных с целью однократного обращения субъекта персональных данных к руководству МФЦ

При ведении журналов (реестров, карточек обращения), содержащих персональные данные, необходимые для однократной регистрации субъекта персональных данных при обращении в ТОГКУ «МФЦ», должны соблюдаться следующие условия:

необходимость ведения такого журнала (реестра, карточки) должна быть предусмотрена правовым актом учреждения, содержащим сведения о цели обработки ПДн, осуществляемой без использования средств автоматизации, способы фиксации и состав информации, запрашиваемой у субъектов персональных данных, перечень лиц, ответственных за ведение и сохранность журнала (реестра, карточки), сроки обработки ПДн,;

копирование содержащейся в таких журналах (реестрах, карточках) информации не допускается;

персональные данные каждого субъекта персональных данных могут заноситься в такой журнал (книгу, карточку) не более одного раза в каждом случае приема субъекта персональных данных.

9.2. Правила работы с обезличенными данными

Обезличиванием ПДн называются действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность ПДн конкретному субъекту персональных данных.

Порядок обезличивания в ТОГКУ «МФЦ» установлен Правилами работы с обезличенными персональными данными.

10. Правовое основание обработки персональных данных

Правовое основание обработки ПДн включает в себя:

определение законности целей обработки ПДн;

оценку вреда, который может быть причинен субъекту персональных данных в случае нарушения требований по обработке и обеспечению безопасности ПДн;

определение заданных характеристик безопасности ПДн;

определение сроков обработки, в том числе хранения ПДн, осуществление контроля за соблюдением сроков обработки ПДн и фактов достижения целей обработки ПДн.

10.1. Определение законности целей обработки персональных данных

Заявляемые цели обработки ПДн должны быть законны, причем, кроме самого факта обработки ПДн, должны рассматриваться и соответственно иметь правовое основание особые правила обработки определенных наборов ПДн (таких как специальные категории ПДн, биометрические персональные данные и др.), особые способы обработки ПДн (обработка без

использования средств автоматизации, исключительно автоматизированная обработка ПДн и др.), а так- же особые цели обработки ПДн .

При определении правовых оснований обработки ПДн должны определяться реквизиты федеральных законов, а также иных подзаконных актов и документов органов государственной власти, которые требуют обработки ПДн или иных документов, являющихся такими основаниями.

Обработка ПДн без документально определенного и оформленного правового основания обработки ПДн не допускается.

10.2. Оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных

Оценкой вреда, который может быть причинен субъекту персональных данных в случае нарушения требований по обработке и обеспечению безопасности ПДн, является определение юридических или иным образом затрагивающих права и законные интересы последствий в отношении субъекта персональных данных, которые могут возникнуть в случае нарушения требований по обработке и обеспечению безопасности ПДн.

К юридическим последствиям относятся случаи возникновения, изменения или прекращения личных либо имущественных прав граждан или иным образом затрагивающих его права, свободы и законные интересы.

При обработке ПДн должны определяться и документально оформляться все возможные юридические или иным образом затрагивающие права и законные интересы последствия в отношении субъекта персональных данных, которые могут возникнуть в случае нарушения требований по обработке и обеспечению безопасности его ПДн.

Определение таких юридических последствий необходимо для недопущения нарушения и обеспечения защиты прав и свобод человека и гражданина при обработке его ПДн, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну, а также определения соотношения вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности ПДн и принимаемых мер.

Обработка ПДн без оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности ПДн, не допускается.

10.3. Заданные характеристики безопасности персональных данных

Всеми лицами, получающими доступ к персональным данным, должна обеспечиваться конфиденциальность таких данных.

Конфиденциальность ПДн это обязательное для соблюдения оператором или иным получившим доступ к ПДн лицом требование не раскрывать третьим лицам и не распространять ПДн без согласия субъекта персональных данных, если иное не предусмотрено Федеральным законом.

Вне зависимости от необходимости обеспечения конфиденциальности ПДн, при обработке ПДн должно определяться наличие требований по обеспечению иных характеристик безопасности ПДн, отличных от нее.

К таким характеристикам относятся:

- требование по обеспечению защищенности от уничтожения ПДн;
- требование по обеспечению защищенности от изменения ПДн;
- требование по обеспечению защищенности от блокирования ПДн;
- требование по обеспечению защищенности от иных несанкционированных действий.

Обеспечение указанных характеристик безопасности ПДн устанавливается федеральными законами и иными нормативными правовыми актами.

При определении правовым ТОГКУ «МФЦ» необходимости обеспечения характеристик безопасности ПДн, отличных от конфиденциальности, основным критерием должна служить оценка вреда, который может быть причинен субъекту персональных данных, с чьим ПДн произошло нарушение таких характеристик безопасности.

Обработка ПДн без документально определенного и оформленного решения по определению характеристик безопасности ПДн не допускается.

10.4. Определение сроков обработки, в том числе хранения персональных данных, осуществление контроля за соблюдением сроков обработки персональных данных и фактов достижения целей обработки персональных данных

На основании определенных целей обработки ПДн, способов обработки и образующихся в процессе такой обработки различных видов документов устанавливаются сроки такой обработки ПДн, в том числе хранения.

Определение сроков хранения осуществляется в соответствии с требованиями законодательства об архивном деле Российской Федерации, в том числе в соответствии с перечнями типовых архивных документов с указанием сроков их хранения.

При использовании документов, содержащих ПДн, в различных целях, определение сроков обработки, в том числе хранения, таких документов устанавливается по максимальному сроку, предусмотренному Федеральным законом. При этом в случае наличия ПДн в таких документах, обработка которых более не требуется, производятся действия по уничтожению таких данных.

Включение в состав Архивного фонда Российской Федерации документов, содержащих персональные данные, осуществляется на основании экспертизы ценности документов и оформляется договором между ТОГКУ «МФЦ» и государственным архивом. При этом объем передаваемых документов и условия передачи определяются условиями такого договора и действующими требованиями законодательства об архивном деле Российской Федерации.

На документы, включенные в состав Архивного фонда Российской Федерации, действие настоящих Правил не распространяется.

Обработка ПДн без документально определенных и оформленных сроков обработки, в том числе хранения ПДн, не допускается.

С целью выполнения требования по уничтожению либо обезличиванию ПДн по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено Федеральным законом, в ТОГКУ «МФЦ» создается комиссия, определяющая факт достижения целей обработки ПДн и достижение предельных сроков хранения документов, содержащих персональные данные.

11. Действия (операции) с персональными данными

Обработкой ПДн называется любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств ПДн, включая:

- сбор ПДн;
- запись ПДн;
- систематизацию ПДн;
- накопление ПДн;
- хранение ПДн;
- уточнение (обновление) ПДн;
- уточнение (изменение) ПДн;
- извлечение ПДн;
- использование ПДн;
- передачу (распространение) ПДн;
- передачу (предоставление) ПДн;
- передачу (доступ) ПДн;
- обезличивание ПДн;
- блокирование ПДн;
- удаление ПДн;
- уничтожение ПДн.

Обработка ПДн без определенных и документально оформленных действий (операций), совершаемых с персональными данными, не допускается.

12. Осуществление сбора персональных данных

12.1. Способы сбора персональных данных и источники их получения

В ТОГКУ «МФЦ» применяются следующие способы получения ПДн субъектов персональных данных:

заполнение субъектом персональных данных соответствующих форм (в том числе для заключения договора);

получение ПДн от третьих лиц;

получение данных на основании запроса третьим лицам;

сбор данных из общедоступных источников.

Получение ПДн ТОГКУ «МФЦ» допускается только:

непосредственно от субъекта персональных данных;

из общедоступных источников;

от третьих лиц.

Получение ПДн из иных источников не допускается.

В связи с необходимостью постоянного контроля за наличием ПДн в общедоступных источниках ПДн, получение и использование таких данных является не рекомендуемым и должно осуществляться только в исключительных случаях в сроки, не превышающие необходимых для принятия соответствующего решения.

12.2. Правила сбора персональных данных

Если предоставление ПДн является обязательным в соответствии с Федеральным законом, ТОГКУ «МФЦ» обязано разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные.

Если основания на обработку ПДн без согласия отсутствуют, то необходимо получение согласия субъекта персональных данных на обработку его ПДн. Обработка ПДн без получения такого согласия категорически запрещается.

Если персональные данные получены не от субъекта персональных данных, ТОГКУ «МФЦ» до начала обработки таких ПДн обязано предоставить субъекту персональных данных:

наименование либо фамилию, имя, отчество и адрес оператора или его представителя;

сведения о цели обработки ПДн и ее правовое основание;

сведения о предполагаемых пользователях ПДн;

сведения об установленных правах субъекта персональных данных;

сведения об источниках получения ПДн.

ТОГКУ «МФЦ» освобождается от обязанности предоставлять субъекту персональных данных сведения в случаях, если:

субъект персональных данных уведомлен об осуществлении обработки его ПДн соответствующим оператором;

персональные данные получены на основании Федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных;

персональные данные сделаны общедоступными субъектом персональных данных или получены из общедоступного источника;

МФЦ осуществляет обработку ПДн для статистических или иных исследовательских целей, если при этом не нарушаются права и законные интересы субъекта персональных данных;

предоставление субъекту ПДн сведений нарушает права и законные интересы третьих лиц.

13. Осуществление систематизации, накопления, уточнения и использования персональных данных

Систематизация, накопление, уточнение, использование ПДн могут осуществляться любыми законными способами в соответствии с правилами, инструкциями, руководствами, регламентами и иными документами, определяющими технологический процесс обработки информации.

В ТОГКУ «МФЦ» могут быть установлены особенности учета ПДн в ИСПДн, в том числе использование различных способов обозначения принадлежности ПДн, содержащихся в соответствующей информационной системе ПДн, конкретному субъекту персональных данных.

Права и свободы человека и гражданина не могут быть ограничены по мотивам, связанным с использованием различных способов обработки ПДн или обозначения принадлежности ПДн, содержащихся в ИСПДн, конкретному субъекту персональных данных.

Не допускается использование оскорбляющих чувства граждан или унижающих человеческое достоинство способов обозначения принадлежности ПДн, содержащихся в ИСПДн, конкретному субъекту персональных данных.

Уточнение ПДн должно производиться только на основании законно полученной в установленном порядке информации.

Решение об уточнении ПДн субъекта персональных данных принимается лицом, ответственным за организацию обработки ПДн в учреждении.

Использование ПДн должно осуществляться исключительно в заявленных целях. Использование ПДн в заранее не определенных и не оформленных установленным образом целях категорически не допускается.

14. Осуществление записи и извлечения персональных данных

Запись ПДн в ИСПДн ТОГКУ «МФЦ» может осуществляться с любых носителей информации или из других ИСПДн.

Извлечение ПДн из ИСПДн может осуществляться с целью:

вывода ПДн на бумажный или иной носитель информации, не предназначенный для его обработки средствами вычислительной техники;

вывода ПДн на носители информации, предназначенные для их обработки средствами вычислительной техники.

15. Осуществление передачи персональных данных

Передача ПДн в ТОГКУ «МФЦ» должна осуществляться с соблюдением настоящих Правил и действующего законодательства Российской Федерации.

В учреждении приняты следующие способы передачи ПДн субъектов персональных данных:

передача ПДн на электронных и бумажных носителях информации нарочным;

передача ПДн на электронных и бумажных носителях посредством почтовой связи;

передача ПДн по каналам электрической связи.

Перед осуществлением передачи ПДн проверяется основание на осуществление такой передачи и наличие согласия на передачу ПДн в согласии субъекта персональных данных на обработку ПДн или наличие иных законных оснований.

Передача ПДн должна осуществляться на основании:

договора (соглашения) с третьей стороной, которой осуществляется передача ПДн;

запроса, полученного от третьей стороны, которой осуществляется передача ПДн;

исполнения возложенных законодательством Российской Федерации на ТОГКУ «МФЦ» функций, полномочий и обязанностей.

Передача ПДн без согласия субъекта персональных данных или иных законных оснований категорически запрещается.

16. Осуществление хранения персональных данных

Хранение ПДн в ТОГКУ «МФЦ» допускается только в форме документов - зафиксированной на материальном носителе информации (содержащей персональные данные) с реквизитами, позволяющими ее идентифицировать и определить субъекта персональных данных. При этом предусматриваются следующие виды документов:

изобразительный документ - документ, содержащий информацию, выраженную посредством изображения какого-либо объекта;

фотодокумент - изобразительный документ, созданный фотографическим способом;

текстовый документ - документ, содержащий речевую информацию, зафиксированную любым типом письма или любой системой звукозаписи;

письменный документ - текстовой документ, информация которого зафиксирована любым типом письма;

рукописный документ - письменный документ, при создании которого знаки письма наносят от руки;

машинописный документ - письменный документ, при создании которого знаки письма наносят техническими средствами;

документ на машинном носителе - документ, созданный с использованием носителей и способов записи, обеспечивающих обработку его информации электронно-вычислительной машиной.

Хранение ПДн в ТОГКУ «МФЦ» осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен Федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных.

Хранение ПДн в ИСПДн и вне таких систем в МФЦ осуществляется только на таких материальных носителях информации и с применением такой технологии ее хранения, которые обеспечивают защиту этих данных от неправомерного или случайного:

- доступа к ним;
- их уничтожения;
- изменения;
- блокирования;
- копирования;
- предоставления;
- распространения.

17. Осуществление блокирования персональных данных

Блокированием ПДн называется временное прекращение обработки ПДн (за исключением случаев, если обработка необходима для уточнения ПДн).

Блокирование ПДн конкретного субъекта персональных данных должно осуществляться во всех ИСПДн ТОГКУ «МФЦ», включая архивы баз данных, содержащих такие персональные данные.

Блокирование ПДн в МФЦ осуществляется:

в случае выявления неправомерной обработки ПДн при обращении субъекта персональных данных или его представителя либо по запросу субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных с момента такого обращения или получения указанного запроса на период проверки;

в случае отсутствия возможности уничтожения ПДн в установленные сроки до их уничтожения.

После устранения выявленной неправомерной обработки ПДн ТОГКУ «МФЦ» осуществляет снятие блокирования ПДн.

Решение о блокировании и снятии блокирования ПДн субъекта персональных данных принимается ответственным за организацию обработки ПДн в учреждении.

18. Осуществление обезличивания персональных данных

Обезличивание ПДн в ТОГКУ «МФЦ» при обработке ПДн с использованием средств автоматизации осуществляется на основании нормативных правовых актов, правил, инструкций, руководств, регламентов и иных документов для достижения заранее определенных и заявленных целей.

Допускается обезличивание ПДн при обработке ПДн без использования средств автоматизации производить способом, исключающим дальнейшую обработку этих ПДн с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

19. Осуществление удаления и уничтожения персональных данных

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

Уничтожение ПДн в ТОГКУ «МФЦ» производится только в следующих случаях:

обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено Федеральным законом;

персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки;

в случае выявления неправомерной обработки ПДн, если обеспечить правомерность обработки ПДн невозможно;

в случае достижения цели обработки ПДн;

в случае отзыва субъектом персональных данных согласия на обработку его ПДн и в случае, если сохранение ПДн более не требуется для целей обработки ПДн.

По факту уничтожения ПДн обязательно проверяется необходимость уведомления об этом и в случае наличия такого требования осуществляется уведомление указанных в таком требовании лиц.

При уничтожении ПДн необходимо:

убедиться в необходимости уничтожения ПДн;

убедиться в том, что уничтожаются те персональные данные, которые предназначены для уничтожения;

уничтожить персональные данные подходящим способом в соответствии с настоящими Правилами или способом, указанным в соответствующем требовании или распорядительном документе;

проверить необходимость уведомления об уничтожении ПДн;

при необходимости уведомить об уничтожении ПДн требуемых лиц.

При уничтожении ПДн применяются следующие способы:

измельчение в бумагорезательной (бумагоуничтожительной) машине - для документов, исполненных на бумаге;

тщательное вымарывание (с проверкой тщательности вымарывания) - для сохранения возможности обработки иных данных, зафиксированных на материальном носителе, содержавшем персональные данные;

физическое уничтожение частей носителей информации - разрушение или сильная деформация - для носителей информации на жестком магнитном диске (уничтожению подлежат внутренние диски и микросхемы); CD (DVD)-дисках, USB- и Flash-носителях (уничтожению подлежат модули и микросхемы долговременной памяти);

стирание с помощью сертифицированных средств уничтожения информации - для записей в базах данных и отдельных документов на машинном носителе.

При уничтожении ПДн необходимо учитывать их наличие в архивных базах данных и производить уничтожение во всех копиях базы данных, если иное не установлено действующим законодательством Российской Федерации.

При необходимости уничтожения части ПДн допускается уничтожать материальный носитель одним из указанных в настоящем Положении способов, с предварительным копированием сведений, не подлежащих уничтожению, способом, исключающим одновременное копирование ПДн, подлежащих уничтожению.

Уничтожение ПДн производится лицами, обрабатывающими персональные данные в соответствующей ИСПДн, в которой производится уничтожение ПДн, только в присутствии лица, ответственного за организацию обработки ПДн в ТОГКУ «МФЦ».

По факту уничтожения ПДн составляется акт об уничтожении ПДн, который подписывается лицами, производившими уничтожение, заверяется лицом, ответственным за организацию обработки ПДн в учреждении, присутствовавшим при уничтожении, и утверждается директором МФЦ.

Хранение актов об уничтожении ПДн осуществляется в течение срока исковой давности, если иное не установлено нормативными правовыми актами Российской Федерации.

20. Права и обязанности субъекта персональных данных и ТОГКУ «МФЦ» при обработке персональных данных

20.1. Права субъекта персональных данных

Субъект персональных данных, чьи персональные данные обрабатываются в ТОГКУ «МФЦ», имеет право:

на получение сведений о подтверждении факта обработки ПДн учреждением;

на получение сведений о правовых основаниях и цели обработки ПДн;

на получение сведений о цели и применяемых ТОГКУ «МФЦ» способах обработки ПДн;

на получение сведений о наименовании и месте нахождения МФЦ, сведений о лицах, которые имеют доступ к персональным данным ;

на получение сведений о обрабатываемых ПДн, относящихся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен Федеральным законом;

на получение сведений о сроках обработки ПДн, в том числе сроках их хранения;

на получение сведений о порядке осуществления субъектом персональных данных своих прав, предусмотренных законодательством в области ПДн;

на получение информации об осуществленной или о предполагаемой трансграничной передаче данных;

на получение сведений о наименовании и адресе лица, осуществляющего обработку ПДн по поручению ТОГКУ «МФЦ», если обработка поручена или будет поручена такому лицу;

на получение иных сведений, предусмотренных законодательством в области ПДн и другими федеральными законами;

требовать от ТОГКУ «МФЦ» уточнения его ПДн, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки;

принимать предусмотренные законом меры по защите своих прав;

требовать от МФЦ предоставления ему ПДн в доступной форме;

повторного обращения и запроса в целях получения сведений и ознакомления с его персональными данными;

требовать разъяснения порядка принятия решения на основании исключительно автоматизированной обработки его ПДн;

заявить возражение против принятия решения на основании исключительно автоматизированной обработки ПДн решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы;

требовать разъяснения порядка принятия и возможные юридические последствия принятия решения на основании исключительно автоматизированной обработки ПДн решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы, а также разъяснения порядка защиты субъектом персональных данных своих прав и законных интересов;

обжаловать действия или бездействие ТОГКУ «МФЦ» в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке, если субъект персональных данных считает, что ТОГКУ «МФЦ» осуществляет обработку его ПДн с нарушением требований Федерального закона или иным образом нарушает его права и свободы;

на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке;

требовать предоставления безвозмездно субъекту персональных данных или его представителю возможности ознакомления с персональными данными, относящимися к этому субъекту персональных данных;

принимать решение о предоставлении его ПДн и давать согласие на их обработку свободно, своей волей и в своем интересе;

отзывать согласие на обработку ПДн.

Кроме указанных прав в вопросах обработки его ПДн субъект персональных данных обладает другими правами, предоставляемыми ему действующим законодательством Российской Федерации.

20.2. Обязанности субъекта персональных данных

Субъект персональных данных, чьи персональные данные обрабатываются в ТОГКУ «МФЦ», обязан:

предоставлять свои персональные данные в случаях, когда федеральными законами предусматриваются случаи обязательного предоставления субъектом персональных данных своих ПДн;

с целью соблюдения его законных прав и интересов подавать только достоверные персональные данные.

Кроме указанных обязанностей в вопросах обработки его ПДн на субъекта персональных данных налагаются иные обязанности, предусмотренные действующим законодательством Российской Федерации.

20.3. Права ТОГКУ «МФЦ» при обработке персональных данных субъектов персональных данных

ТОГКУ «МФЦ» при обработке ПДн субъектов персональных данных имеет право:

- обрабатывать персональные данные в соответствии с действующим законодательством Российской Федерации;
- поручить обработку ПДн другому лицу с согласия субъекта персональных данных, если иное не предусмотрено Федеральным законом, на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, либо путем принятия государственным или муниципальным органом соответствующего акта;
- мотивированно отказать субъекту персональных данных в выполнении повторного запроса в целях получения сведений, касающихся обработки его ПДн, при нарушении субъектом персональных данных своих обязанностей по подаче такого запроса;
- ограничить право субъекта персональных данных на доступ к его персональным данным в соответствии с федеральными законами, в том числе, если обработка ПДн осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;
- ограничить право субъекта персональных данных на доступ к его персональным данным в соответствии с федеральными законами, в том числе, если доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц;
- отказать субъекту персональных данных в выполнении запроса в целях получения сведений, касающихся обработки его ПДн, в случае, если субъект персональных данных уведомлен об осуществлении обработки его ПДн соответствующим оператором;
- отказать субъекту персональных данных в выполнении запроса в целях получения сведений, касающихся обработки его ПДн, в случае, если персональные данные получены на основании Федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных;
- отказать субъекту персональных данных в выполнении запроса в целях получения сведений, касающихся обработки его ПДн, в случае, если персональные данные сделаны общедоступными субъектом персональных данных или получены из общедоступного источника;
- отказать субъекту персональных данных в выполнении запроса в целях получения сведений, касающихся обработки его ПДн, в случае, если оператор осуществляет обработку ПДн для статистических или иных исследовательских целей, если при этом не нарушаются права и законные интересы субъекта персональных данных;
- отказать субъекту ПДн в выполнении запроса в целях получения сведений, касающихся обработки его ПДн, в случае, если предоставление субъекту персональных данных таких сведений нарушает права и законные интересы третьих лиц;
- самостоятельно определять состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных действующим законодательством в области ПДн, если иное не предусмотрено федеральными законами;
- осуществлять или обеспечивать блокирование или уничтожение ПДн, если обеспечить правомерность обработки ПДн невозможно;
- осуществлять или обеспечивать уничтожение ПДн в случае достижения цели обработки ПДн;
- в случае достижения цели обработки ПДн продолжить обработку ПДн, если обработка ПДн осуществляется без согласия субъекта персональных данных на основании пункта 4 статьи 21 Федерального закона;

- в случае отзыва субъектом ПДн согласия на обработку его ПДн продолжить обработку ПДн, если обработка ПДн осуществляется без согласия субъекта персональных данных на основании пункта 5 статьи 21 Федерального закона;
- в случае отсутствия возможности уничтожения ПДн осуществить блокирование таких ПДн и обеспечить уничтожение ПДн в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами;
- осуществлять без уведомления уполномоченного органа по защите прав субъектов персональных данных обработку ПДн, указанных в пункте 2 статьи 22 Федерального закона.
- Кроме указанных прав в вопросах обработки ПДн субъектов персональных данных ТОГКУ «МФЦ» обладает другими правами, предоставляемыми ему действующим законодательством Российской Федерации.

20.4. Обязанности ТОГКУ «МФЦ» при обработке персональных данных субъектов персональных данных

ТОГКУ «МФЦ» при обработке ПДн субъектов персональных данных обязано:

- строго соблюдать принципы и правила обработки ПДн;
- в случае если обработка ПДн осуществляется по поручению оператора, строго соблюдать и выполнять требования поручения оператора;
- не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено Федеральным законом;
- по требованию субъекта персональных данных либо по решению суда или иных уполномоченных государственных органов исключить из общедоступных источников ПДн сведения о субъекте персональных данных;
- обеспечить конкретность и информированность согласия на обработку ПДн;
- получать согласие на обработку ПДн;
- в случае получения согласия на обработку ПДн от представителя субъекта персональных данных проверять полномочия данного представителя на дачу согласия от имени субъекта персональных данных;
- предоставить доказательство получения согласия субъекта персональных данных на обработку его ПДн или доказательство наличия оснований обработки ПДн без получения согласия;
- строго соблюдать требования к содержанию согласия в письменной форме субъекта персональных данных на обработку его ПДн;
- незамедлительно прекратить обработку специальных категорий ПДн, если устранены причины, вследствие которых осуществлялась обработка, если иное не установлено Федеральным законом;
- убедиться в том, что иностранным государством, на территорию которого осуществляется передача ПДн, обеспечивается адекватная защита прав субъектов персональных данных до начала осуществления трансграничной передачи ПДн;
- предоставить субъекту персональных данных сведения по запросу субъекта персональных данных в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких ПДн;
- мотивировать и представить доказательства обоснованности отказа в выполнении повторного запроса субъекта персональных данных;
- разъяснить субъекту персональных данных порядок принятия решения на основании исключительно автоматизированной обработки его ПДн и возможные юридические последствия такого решения, предоставить возможность заявить возражение против такого решения, а также разъяснить порядок защиты субъектом персональных данных своих прав и законных интересов;
- рассмотреть возражение против принятия решения на основании исключительно автоматизированной обработки его ПДн и уведомить субъекта персональных данных о результатах рассмотрения такого возражения;
- предоставить субъекту персональных данных по его просьбе информацию, касающуюся обработки его ПДн;

- разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные, если предоставление ПДн является обязательным в соответствии с Федеральным законом;
- до начала обработки ПДн, полученных не от субъекта персональных данных, предоставить субъекту персональных данных информацию о своем наименовании и адресе, цели обработки ПДн и ее правовом основании, предполагаемых пользователей ПДн, установленные права субъекта персональных данных, источник получения ПДн;
- принимать меры, необходимые и достаточные для обеспечения выполнения своих обязанностей в области ПДн, если иное не предусмотрено федеральными законами;
- опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки ПДн, к сведениям о реализуемых требованиях к защите ПДн;
- по запросу уполномоченного органа по защите прав субъектов персональных данных представить документы и локальные акты, определяющие политику в отношении обработки ПДн, и сведения о реализуемых требованиях к защите ПДн;
- принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн;
- сообщить субъекту персональных данных или его представителю информацию о наличии ПДн, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя либо при получении запроса субъекта персональных данных или его представителя;
- в случае отказа в предоставлении информации о наличии ПДн о соответствующем субъекте персональных данных или ПДн субъекту персональных данных или его представителю при их обращении либо при получении запроса субъекта персональных данных или его представителя дать в письменной форме мотивированный ответ;
- предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных;
- внести в персональные данные необходимые изменения или уничтожить такие персональные данные в случае предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными;
- строго соблюдать сроки по уведомлениям, блокированию и уничтожению ПДн;
- уведомить субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы;
- сообщить в уполномоченный орган по защите прав субъектов персональных данных по запросу этого органа необходимую информацию;
- в случае выявления неправомерной обработки ПДн при обращении субъекта персональных данных или его представителя либо по запросу субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных оператор обязан осуществить блокирование неправомерно обрабатываемых ПДн, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка ПДн осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки;
- в случае выявления неточных ПДн при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных оператор обязан осуществить блокирование ПДн, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка ПДн осуществляется другим лицом, действующим по поручению оператора) с момента такого

обращения или получения указанного запроса на период проверки, если блокирование ПДн не нарушает права и законные интересы субъекта персональных данных или третьих лиц;

- уточнить персональные данные либо обеспечить их уточнение (если обработка ПДн осуществляется другим лицом, действующим по поручению оператора) и снять блокирование ПДн в случае подтверждения факта неточности ПДн на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов;
- прекратить неправомерную обработку ПДн или обеспечить прекращение неправомерной обработки ПДн лицом, действующим по поручению оператора в случае выявления неправомерной обработки ПДн, осуществляемой оператором или лицом, действующим по поручению оператора;
- уничтожить персональные данные или обеспечить их уничтожение в случае, если обеспечить правомерность обработки ПДн невозможно;
- уведомить субъекта персональных данных или его представителя, а в случае если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган об устранении допущенных нарушений или об уничтожении ПДн;
- прекратить обработку ПДн или обеспечить ее прекращение (если обработка ПДн осуществляется другим лицом, действующим по поручению оператора) и уничтожить персональные данные или обеспечить их уничтожение (если обработка ПДн осуществляется другим лицом, действующим по поручению оператора):
- в случае достижения цели обработки ПДн, если обработка ПДн осуществляется без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом;
- в случае отзыва субъектом персональных данных согласия на обработку его ПДн, если обработка ПДн осуществляется без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом;
- уведомить уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку ПДн;
- уведомить уполномоченный орган по защите прав субъектов персональных данных в случае изменения сведений, указанных в уведомлении о своем намерении осуществлять обработку ПДн;
- назначить лицо, ответственное за организацию обработки ПДн;
- предоставлять лицу, ответственному за организацию обработки ПДн, необходимые сведения;
- неукоснительно соблюдать все требования настоящих Правил;
- ознакомить работников ТОГКУ «МФЦ», непосредственно осуществляющих обработку ПДн, с положениями законодательства Российской Федерации о ПДн, в том числе требованиями к защите ПДн, документами, определяющими политику в отношении обработки ПДн, локальными актами по вопросам обработки ПДн, и обучить таких служащих.

Кроме указанных обязанностей в вопросах обработки ПДн субъектов персональных данных на ТОГКУ «МФЦ» налагаются иные обязанности, предусмотренные действующим законодательством Российской Федерации.

21. Процедуры, направленные на предотвращение и выявление нарушений законодательства в отношении обработки персональных данных и устранение таких последствий

К процедурам, направленным на предотвращение и выявление нарушений законодательства в отношении обработки ПДн и устранение таких последствий, относятся:

реализация мер, направленных на обеспечение выполнения оператором своих обязанностей;

выполнение предусмотренных законодательством о ПДн обязанностей, возложенных на администрацию области;

обеспечение личной ответственности служащих администрации области, осуществляющих обработку либо доступ к персональным данным;

организация рассмотрения запросов субъектов персональных данных или их представителей и ответов на такие запросы;

организация внутреннего контроля соответствия обработки ПДн требованиям к защите ПДн, установленным действующим законодательством в области ПДн и локальными актами ТОГКУ «МФЦ»;

сокращение объема обрабатываемых данных;

сокращение числа должностей работников ТОГКУ «МФЦ», имеющих доступ к персональным данным;

стандартизация операций осуществляемых с персональными данными;

определение порядка доступа работников ТОГКУ «МФЦ»в помещения, в которых ведется обработка ПДн;

проведение необходимых мероприятий по обеспечению безопасности ПДн и носителей их содержащих;

проведение периодических проверок условий обработки ПДн;

повышение осведомленности работников ТОГКУ «МФЦ», занимающих должности, предусматривающие обработку ПДн либо имеющие доступ к ПДн, путем их ознакомления с положениями законодательства Российской Федерации о ПДн (в том числе с требованиями к защите ПДн), и организация обучения указанных работников;

блокирование, внесение изменений и уничтожение ПДн в предусмотренных действующим законодательством в области ПДн случаях;

оповещение субъектов персональных данных в предусмотренных действующим законодательством в области ПДн случаях;

разъяснение прав субъекту персональных данных в вопросах обработки и обеспечения безопасности их ПДн;

оказание содействия правоохранительным органам в случаях нарушений законодательства в отношении обработки персональных;

публикация на официальном сайте ТОГКУ «МФЦ» документов, определяющих политику в отношении обработки ПДн.

Указанный перечень процедур, направленных на предотвращение и выявление нарушений законодательства в отношении обработки ПДн и устранение таких последствий, является открытым и может дополняться мероприятиями в конкретных случаях.

22. Требования к работникам ТОГКУ «МФЦ», осуществляющим доступ к персональным данным или их обработку

ТОГКУ «МФЦ» осуществляет ознакомление работников, непосредственно осуществляющих обработку ПДн или доступ к ним, с положениями законодательства Российской Федерации о ПДн (в том числе с требованиями к защите ПДн), локальными актами учреждения по вопросам обработки ПДн, включая настоящие Правила:

при оформлении служебного контракта;

после каждого перерыва в исполнении своих обязанностей на срок более 45 рабочих дней;

при первоначальном допуске к обработке ПДн в ИСПДн;

при назначении на новую должность, связанную с обработкой ПДн или доступом к ним;

после внесения изменений в действующее законодательство Российской Федерации о ПДн, локальные акты МФЦ по вопросам обработки ПДн, включая настоящие Правила.

Работники ТОГКУ «МФЦ», непосредственно осуществляющие обработку ПДн или доступ к ним обязаны:

неукоснительно следовать принципам обработки ПДн;

знать и строго соблюдать положения действующего законодательства Российской Федерации в области ПДн;

знать и строго соблюдать положения локальных ТОГКУ «МФЦ» области в области обработки и обеспечения безопасности ПДн;

знать и строго соблюдать инструкции, руководства и иные эксплуатационные документы на применяемые средства автоматизации, в том числе программное обеспечение, и средства защиты информации;

соблюдать конфиденциальность ПДн, то есть не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено Федеральным законом;

не допускать нарушений требований и правил обработки и обеспечения безопасности ПДн;

обо всех подозрениях и ставших известными случаях нарушений требований и правил обработки и обеспечения безопасности ПДн сообщать лицу, ответственному за обработку ПДн ТОГКУ «МФЦ».

Работники ТОГКУ «МФЦ» несут личную ответственность за соблюдение указанных обязанностей в предусмотренном действующим законодательством Российской Федерации объеме.

23. Конфиденциальность персональных данных

Запрет раскрытия ПДн третьим лицам и распространения ПДн без согласия субъекта персональных данных, если иное не предусмотрено Федеральным законом, ТОГКУ «МФЦ» и иными лицами, получившим доступ к ПДн, называется конфиденциальностью ПДн.

23.1. Режим ограниченного доступа к персональным данным

С целью реализации требований действующего законодательства Российской Федерации в области ПДн по обеспечению конфиденциальности ПДн в ТОГКУ «МФЦ» вводится режим ограниченного доступа к ПДн.

Создание режима ограниченного доступа к ПДн включает в себя:

разработку и последующее уточнение настоящих Правил в части, касающейся обеспечения конфиденциальности ПДн и обеспечения безопасности ПДн;

разработку и корректировку Перечня помещений, предназначенных для обработки ПДн;

разработку и корректировку Перечня должностей работников ТОГКУ «МФЦ», замещение которых предусматривает осуществление обработки ПДн либо осуществление доступа к ПДн;

разработку и корректировку Перечня должностей работников ТОГКУ «МФЦ», ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных;

разработку и корректировку Перечня информационных ресурсов, содержащих ПДн (мест расположения баз данных или иных документов и массивов, содержащих ПДн);

оборудование помещений, предназначенных для обработки ПДн на предмет соответствия требованиям к инженерно-технической укрепленности по защите объектов от преступных посягательств;

проведение мероприятий по обследованию помещений, предназначенных для обработки ПДн, с составлением актов соответствия или проведением, при необходимости, доработок помещений по инженерно-технической укрепленности по защите объектов от преступных посягательств;

внесение изменений в должностные инструкции (дополнения в служебные договора) работников ТОГКУ «МФЦ», предусматривающие регулирование отношений по использованию информации ограниченного доступа;

получение расписок в ознакомлении работников ТОГКУ «МФЦ», доступ которых к информации ограниченного доступа, обладателем которой является ТОГКУ «МФЦ», необходим для выполнения ими своих трудовых обязанностей, с перечнем информации ограниченного доступа, установленным режимом ограничения доступа к информации и мерами ответственности за его нарушение;

передачу (возврат) работниками ТОГКУ «МФЦ» при прекращении или расторжении служебного контракта имеющихся в пользовании такого служащего материальных носителей информации, содержащей ПДн;

проведение занятий и иных мероприятий по повышению уровня знаний (квалификации) работников ТОГКУ «МФЦ», допущенных к обработке ПДн, по вопросам обработки и обеспечения безопасности ПДн;

разработку и ведение Журнала учета машинных носителей информации;

разработку и ведение Журнала учета сейфов, металлических шкафов, спецхранилищ и ключей от них;

создание и ведение списков лиц, имеющих доступ в помещения, в которых обрабатываются ПДн;

разработку инструкций для работников ТОГКУ «МФЦ» по вопросам обеспечения безопасности ПДн.

23.2. Порядок использования материальных (внешних) носителей информации

Все материальные (внешние) носители информации (далее - носители), используемые для обработки ПДН, должны быть зарегистрированы в установленном порядке. При необходимости они могут маркироваться пометкой "Для служебного пользования" ("ДСП"), либо любой другой, например: "Персональные данные" ("ПДн"), “Содержит персональные данные”.

Учет (регистрация) носителей осуществляются структурным подразделением ТОГКУ «МФЦ», которому поручен учет несекретной документации.

Автоматизированная обработка информации с использованием данных носителей должна осуществляться на аттестованных по требованиям безопасности автоматизированных рабочих местах или в защищенной ИСПДн.

Носители передаются в структурные подразделения ТОГКУ «МФЦ» (исполнителям) под расписку, пересылаются сторонним организациям фельдъегерской связью, заказными или ценными почтовыми отправлениями.

Размножение (тиражирование) носителей осуществляется только с письменного разрешения исполнителя. Учет размноженных носителей осуществляется поэкземплярно.

Носители хранятся в надежно запираемых и опечатываемых шкафах (ящиках, хранилищах).

При необходимости направления носителя(ей) в несколько адресов составляется указатель рассылки, в котором поадресно проставляются номера экземпляров отправляемых носителей. Указатель рассылки подписывается исполнителем и его руководителем.

Уничтожение носителей, утративших свое практическое значение и не имеющих исторической ценности, производится по акту. В учетных формах об этом делается отметка со ссылкой на соответствующий акт.

Передача носителей от одного служащего другому осуществляется с разрешения соответствующего руководителя.

При смене работника, ответственного за учет, составляется акт приема-сдачи, который утверждается директором ТОГКУ «МФЦ» (заместителем диреткора).

Проверка наличия носителей проводится не реже одного раза в год комиссией, назначаемой распоряжением директора ТОГКУ «МФЦ». В состав такой комиссии обязательно включаются лица, ответственные за учет и хранение этих носителей. Результаты проверки оформляются актом.

По фактам утраты носителей назначается комиссия для расследования обстоятельств утраты. Результаты расследования докладываются руководителю, назначившему комиссию.

На утраченные носители составляется акт, на основании которого делаются соответствующие отметки в учетных формах.

24. Обеспечение безопасности персональных данных при их обработке

В соответствии с требованиями действующего законодательства в области ПДн при обработке ПДн ТОГКУ «МФЦ» обязано принимать необходимые правовые, организационные и технические меры для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения ПДн, а также от иных неправомерных действий.

Безопасность ПДн достигается путем исключения несанкционированного, в том числе случайного, доступа к ПДн, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение ПДн, а также иных несанкционированных действий.

Для обеспечения безопасности ПДн при их обработке в информационных системах осуществляется защита речевой информации и информации, обрабатываемой техническими средствами, а также информации, представленной в виде информативных электрических сигналов, физических полей, носителей на бумажной, магнитной, магнитно-оптической и иной основе.

Работы по обеспечению безопасности ПДн при их обработке в информационных системах в ТОГКУ «МФЦ» являются неотъемлемой частью работ по созданию информационных систем.

24.1. Принципы обеспечения безопасности персональных данных при их обработке

Обеспечение безопасности ПДн в ТОГКУ «МФЦ» должно осуществляться на основе следующих принципов:

соблюдение конфиденциальности ПДн и иных характеристик их безопасности;

реализация права на доступ к персональным данным лиц, доступ которых к таким данным разрешается в рамках действующего законодательства Российской Федерации и локальными нормативными актами учреждения;

обеспечение защиты информации, содержащей персональные данные, от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

проведение мероприятий, направленных на предотвращение несанкционированной передачи их лицам, не имеющим права доступа к такой информации;

своевременное обнаружение фактов несанкционированного доступа к персональным данным;

недопущение воздействия на технические средства автоматизированной обработки ПДн, в результате которого может быть нарушено их функционирование;

возможность незамедлительного восстановления ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

постоянный контроль за обеспечением уровня защищенности ПДн;

применение средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия требованиям безопасности ПДн.

Категорически запрещается нарушать указанные принципы по обеспечению безопасности ПДн.

24.2. Требования по уровню обеспечения безопасности

С целью установления методов и способов защиты информации, необходимых для обеспечения безопасности ПДн, определяется уровень защищенности ПДн в зависимости от объема обрабатываемых ими ПДн и угроз безопасности жизненно важным интересам личности, общества и государства.

Определение уровня защищенности ПДн включает в себя следующие этапы:

сбор и анализ исходных данных по ИСПДн;

присвоение ИСПДн соответствующего уровня защищенности ПДн и его документальное оформление.

При определении уровня защищенности ПДн учитываются следующие исходные данные:

категория обрабатываемых в ИСПДн ПДн;

объем обрабатываемых ПДн (количество субъектов персональных данных, ПДн которых обрабатываются ИСПДн);

заданные характеристики безопасности ПДн, обрабатываемых в ИСПДн;

структура ИСПДн;

наличие подключений ИСПДн к сетям связи общего пользования и (или) сетям международного информационного обмена;

режим обработки ПДн;

режим разграничения прав доступа пользователей ИСПДн;

местонахождение технических средств ИСПДн.

В случае выделения в составе ИСПДн подсистем, каждая из которых является информационной системой, ИСПДн в целом присваивается уровень защищенности ПДн, соответствующий наиболее высокому уровню защищенности ПДн входящих в нее подсистем.

Определение уровня защищенности ПДн проводится на этапе ее создания или в ходе эксплуатации (для ранее введенных в эксплуатацию и (или) модернизируемых ИСПДн).

Результаты определения уровня защищенности ПДн оформляются соответствующим актом установки уровня защищенности ПДн.

24.3. Состав мероприятий по обеспечению безопасности персональных данных

Мероприятия по обеспечению безопасности ПДн должны носить комплексный характер и включать в себя правовые, организационные и технические меры, описанные в настоящих Правилах.

Порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются настоящими Правилами.

24.4. Состав мероприятий по обеспечению безопасности персональных данных при их обработке, осуществляемой без использования средств автоматизации

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

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

При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность ПДн и исключающие несанкционированный к ним доступ.

Ответственным за организацию и контроль за обеспечением безопасности ПДн в администрации области при обработке ПДн, осуществляемой без использования средств автоматизации, является структурное подразделение администрации области, ответственное за организацию обработки ПДн.

24.5. Состав мероприятий по обеспечению безопасности персональных данных при их обработке, осуществляемой с использованием средств автоматизации

Мероприятия по обеспечению безопасности ПДн при их обработке в информационных системах ПДн в ТОГКУ «МФЦ» включают в себя:

определение угроз безопасности ПДн при их обработке, формирование на их основе модели угроз;

разработку на основе модели угроз системы защиты ПДн, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты ПДн, предусмотренных для соответствующего класса информационных систем;

проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;

установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;

обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей ПДн;

учет лиц, допущенных к работе с персональными данными в информационной системе;

контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

разбирательство и составление заключений по фактам несоблюдения условий хранения носителей ПДн, использования средств защиты информации, которые могут привести к нарушению конфиденциальности ПДн или другим нарушениям, приводящим к снижению уровня защищенности ПДн, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

описание системы защиты ПДн.

К методам и способам защиты информации в ИСПДн относятся:

методы и способы защиты информации, обрабатываемой техническими средствами информационной системы, от несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение ПДн, а также иных несанкционированных действий (далее - методы и способы защиты информации от несанкционированного доступа);

методы и способы защиты речевой информации, а также информации, представленной в виде информативных электрических сигналов, физических полей, от несанкционированного доступа к персональным данным, результатом которого может стать копирование, распространение ПДн, а также иных несанкционированных действий (далее - методы и способы защиты информации от утечки по техническим каналам).

Методами и способами защиты информации от несанкционированного доступа являются:

реализация разрешительной системы допуска пользователей (обслуживающего персонала) к информационным ресурсам, информационной системе и связанным с ее использованием работам, документам;

ограничение доступа пользователей в помещения, где размещены технические средства, позволяющие осуществлять обработку ПДн, а также хранятся носители информации;

разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;

регистрация действий пользователей и обслуживающего персонала, контроль несанкционированного доступа и действий пользователей, обслуживающего персонала и посторонних лиц;

учет и хранение съемных носителей информации и их использование, исключающее хищение, подмену и уничтожение;

резервирование технических средств, дублирование массивов и носителей информации;

использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия;

использование защищенных каналов связи;

размещение технических средств, позволяющих осуществлять обработку ПДн, в пределах охраняемой территории;

организация физической защиты помещений и собственно технических средств, позволяющих осуществлять обработку ПДн;

предотвращение внедрения в информационные системы вредоносных программ (программ-вирусов) и программных закладок.

В ИСПДн, имеющих подключение к информационно-телекоммуникационным сетям международного информационного обмена (сетям связи общего пользования) или при функционировании которых предусмотрено использование съемных носителей информации, используются средства антивирусной защиты.

При взаимодействии информационных систем с информационно-телекоммуникационными сетями международного информационного обмена (сетями связи общего пользования) наряду с указанными методами и способами основными методами и способами защиты информации от несанкционированного доступа являются:

межсетевое экранирование с целью управления доступом, фильтрации сетевых пакетов и трансляции сетевых адресов для скрытия структуры информационной системы;

обнаружение вторжений в информационную систему, нарушающих или создающих предпосылки к нарушению установленных требований по обеспечению безопасности ПДн;

анализ защищенности информационных систем, предполагающий применение специализированных программных средств (сканеров безопасности);

защита информации при ее передаче по каналам связи;

использование смарт-карт, электронных замков и других носителей информации для надежной идентификации и аутентификации пользователей;

использование средств антивирусной защиты;

централизованное управление системой защиты ПДн информационной системы.

Защита речевой информации и информации, представленной в виде информативных электрических сигналов и физических полей, осуществляется в случаях, когда при определении угроз безопасности ПДн и формировании модели угроз применительно к информационной системе являются актуальными угрозы утечки акустической речевой информации, угрозы утечки видовой информации и угрозы утечки информации по каналам побочных электромагнитных излучений и наводок.

В ИСПДн с установленным вторым уровнем защищенности ПДн для обработки информации используются средства вычислительной техники, удовлетворяющие требованиям национальных стандартов по электромагнитной совместимости, по безопасности и эргономическим требованиям к средствам отображения информации, по санитарным нормам, предъявляемым к видеодисплейным терминалам средств вычислительной техники.

Величина звукоизоляции определяется оператором исходя из характеристик помещения, его расположения и особенностей обработки ПДн в информационной системе.

Размещение устройств вывода информации средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео и буквенно-цифровой информации, входящих в состав ИСПДн, в помещениях, в которых они

установлены, осуществляется таким образом, чтобы была исключена возможность просмотра посторонними лицами текстовой и графической видовой информации, содержащей ПДн.

Обмен ПДн при их обработке в ИСПДн осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и (или) путем применения технических средств, в том числе средств криптографической защиты информации.

25. Требования к помещениям, в которых производится обработка персональных данных

Размещение оборудования ИСПДн, специального оборудования и охрана помещений, в которых ведется работа с ПДн, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей ПДн и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

Помещения, в которых располагаются технические средства ИСПДн или хранятся носители ПДн, должны соответствовать требованиям пожарной безопасности, установленным действующим законодательством Российской Федерации.

Определение уровня специального оборудования помещения осуществляется специально создаваемой комиссией. По результатам определения класса и обследования помещения на предмет его соответствия такому классу составляются акты.

Кроме указанных мер по специальному оборудованию и охране помещений, в которых устанавливаются криптографические средства защиты информации или осуществляется их хранение, реализуются дополнительные требования, определяемые методическими документами Федеральной службы безопасности России.

27. Мероприятия при возникновении обстоятельств непреодолимой силы (форс-мажор)

В случае появления обстоятельств непреодолимой силы, возникших в результате событий чрезвычайного характера, которые ТОГКУ «МФЦ» не может предвидеть, за возникновение которых она не несет ответственности и не может предотвратить разумными мерами, должностные лица учреждения обязаны принять все возможные меры по недопущению нарушения прав субъекта персональных данных.

К обстоятельствам непреодолимой силы относятся события: землетрясение, наводнение, пожар, забастовки, насильственные или военные действия любого характера, решения органов государственной власти, препятствующие исполнению требований законодательства в области ПДн.

Надлежащим доказательством наличия указанных выше обстоятельств будут служить официальные документы ТОГКУ «МФЦ» и органов государственной власти области и Российской Федерации.

ТОГКУ «МФЦ» в случае возникновения указанных выше обстоятельств и нарушения прав субъектов персональных данных, связанных с такими обстоятельствами, извещает субъекта персональных данных всеми доступными способами.

ПРИЛОЖЕНИЕ № 4
УТВЕРЖДЕНО
приказом ТОГКУ «МФЦ»
от _____№ _____

Правила
рассмотрения запросов субъектов персональных данных или их представителей

1. Общие положения

Настоящие Правила рассмотрения запросов субъектов персональных данных или их представителей (далее - Правила) регулируют отношения, возникающие при выполнении ТОГКУ «МФЦ» (далее - Оператор) обязательств согласно требованиям статей 14, 20 и 21 Федерального закона от 27 июля 2006 г. № 152-ФЗ "О персональных данных" (далее - Федеральный закон № 152-ФЗ).

Положения настоящих Правил распространяются на действия оператора при получении запроса от заявителей, работников и их законных представителей (далее - субъект персональных данных) и Уполномоченного органа по защите прав субъектов персональных данных.

Эти действия направлены на определение порядка учета (регистрации), рассмотрение запросов, а также на подтверждение наличия, ознакомления, уточнения, уничтожения персональных данных (ПДн) или отзыв согласия на обработку ПДн, а также на устранение нарушений законодательства, допущенных при обработке ПДн.

Настоящие Правила разработаны в соответствии Трудовым кодексом Российской Федерации, постановлением Правительства Российской Федерации от 21 марта 2012 г. № 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами" и другими нормативными правовыми актами.

2. Организация и проведение работ Оператором по запросу
персональных данных

Субъект персональных данных имеет право на получение информации, касающейся обработки его ПДн в соответствии с частью 7 статьи 14 Федерального закона № 152-ФЗ.

Право субъекта персональных данных на доступ к его ПДн может быть ограничено в соответствии с частью 8 статьи 14 Федерального закона № 152-ФЗ.

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

Сведения, указанные в части 7 статьи 14 Федерального закона № 152-ФЗ, предоставляются субъекту персональных данных Оператором при получении запроса от субъекта персональных данных.

Сведения, указанные в части 7 статьи 14 Федерального закона № 152-ФЗ, должны быть предоставлены субъекту персональных данных в доступной форме и в них не должны содержаться ПДн, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких ПДн.

Запрос субъекта персональных данных должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с Оператором (номер служебного контракта, дата заключения служебного контракта, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки ПДн Оператором, подпись субъекта персональных данных. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

Рассмотрение запросов является служебной обязанностью должностных лиц Оператора, в чьи обязанности входит обработка ПДн.

Должностные лица Оператора обеспечивают:

объективное, всестороннее и своевременное рассмотрения запроса;

принятие мер, направленных на восстановление или защиту нарушенных прав, свобод и законных интересов субъектов персональных данных;

направление письменных ответов по существу запроса.

Ведение делопроизводства по запросам осуществляется управлением информационных технологий, связи и документооборота администрации области.

Все поступившие запросы регистрируются в день их поступления в журнале учета запросов граждан (субъектов персональных данных) по вопросам обработки ПДн. На запросе проставляется штамп, в котором указывается входящий номер и дата регистрации.

Запрос прочитывается, проверяется на повторность, при необходимости сверяется с находящейся в архиве предыдущей перепиской.

В случае подачи субъектом персональных данных повторного запроса, в целях получения сведений, указанных в части 7 статьи 14 Федерального закона № 152-ФЗ, необходимо руководствоваться частями 4 и 5 статьи 14 Федерального закона № 152-ФЗ. Повторный запрос наряду со сведениями, указанными выше, должен содержать обоснование направления повторного запроса.

Оператор вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным частями 4 и 5 статьи 14 Федерального закона № 152-ФЗ. Такой отказ должен быть мотивированным.

Прошедшие регистрацию запросы в тот же день докладываются директору ТОГКУ «МФЦ», который дает по каждому из них письменное указание исполнителям.

Исполнители при рассмотрении и разрешении запроса обязаны:

- внимательно разобраться в их существе, в случае необходимости истребовать дополнительные материалы или направить работника на места для проверки фактов, изложенных в запросах, принять другие меры для объективного разрешения поставленных заявителями вопросов, выявления и устранения причин и условий, порождающих факты нарушения законодательства о ПДн;
- принимать по ним законные, обоснованные и мотивированные решения и обеспечивать своевременное и качественное их исполнение;
- сообщать в письменной форме заявителям о решениях, принятых по их запросам, со ссылками на законодательство Российской Федерации, а в случае отклонения запроса - разъяснять также порядок обжалования принятого решения.

Оператор обязан сообщить субъекту персональных данных информацию о наличии ПДн, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими ПДн при запросе субъекта персональных данных либо в течение тридцати дней с даты получения запроса субъекта персональных данных.

В случае отказа в предоставлении информации о наличии ПДн о соответствующем субъекте персональных данных или ПДн субъекту персональных данных при получении запроса субъекта персональных данных Оператор обязан руководствоваться частью 2 статьи 20 Федерального закона № 152-ФЗ.

Оператор обязан:

предоставить безвозмездно субъекту персональных данных возможность ознакомления с ПДн, относящимися к этому субъекту персональных данных;

уведомить субъекта персональных данных о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым ПДн этого субъекта были переданы.

Запрос считается исполненным, если рассмотрены все поставленные в нем вопросы, приняты необходимые меры и даны исчерпывающие ответы заявителю.

Ответы на запросы печатаются на бланке установленной формы и регистрируются за теми же номерами, что и запросы.

Должностное лицо, назначенное директором ТОГКУ «МФЦ», осуществляет непосредственный контроль за соблюдением установленного законодательством и настоящими Правилами порядка рассмотрения запросов. На контроль берутся все запросы.

При осуществлении контроля обращается внимание на сроки исполнения запроса и полноту рассмотрения поставленных вопросов, своевременность их исполнения и направления ответов заявителям.

3. Действия Оператора в ответ на запросы по персональным данным

В случае поступления запроса субъекта персональных данных по ПДн необходимо выполнить следующие действия:

при получении запроса субъекта персональных данных на наличие ПДн необходимо в течение 30 дней с даты получения запроса (согласно части 1 статьи 20 Федерального закона № 152-ФЗ) подтвердить обработку ПДн в случае ее осуществления. Если обработка ПДн субъекта не ведется, то в течение 30 дней с даты получения запроса (согласно части 2 статьи 20 Федерального закона № 152-ФЗ) необходимо отправить уведомление об отказе в предоставлении информации о наличии персональных данных;

при получении запроса субъекта персональных данных на ознакомление с ПДн необходимо в течение 30 дней с даты получения запроса (согласно части 1 статьи 20 Федерального закона № 152-ФЗ) предоставить для ознакомления ПДн, в случае осуществления обработки этих ПДн. Если обработка ПДн субъекта не ведется, то в течение 30 дней с даты получения запроса (согласно части 2 статьи 20 Федерального закона №152-ФЗ) необходимо отправить уведомление об отказе в предоставлении информации по ПДн.

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

- подтверждение факта обработки персональных данных Оператором;
- правовые основания и цели обработки персональных данных;
- цели и применяемые оператором способы обработки персональных данных;
- наименование и место нахождения Оператора, сведения о лицах (за исключением работников Оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Оператором или на основании Федерального закона № 152-ФЗ;
- обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен Федеральным законом № 152-ФЗ;
- сроки обработки персональных данных, в том числе сроки их хранения;
- порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом № 152-ФЗ;
- информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Оператора, если обработка поручена или будет поручена такому лицу;
- иные сведения, предусмотренные Федеральным законом № 152-ФЗ или другими федеральными законами.

При получении запроса субъекта персональных данных или его представителя на уточнение ПДн необходимо внести в них необходимые изменения в срок, не превышающий 7 рабочих дней со дня предоставления субъектом ПДн или его представителем сведений, подтверждающих, что ПДн являются неполными, неточными или неактуальными, по предоставлению субъектом ПДн или его

сведений, подтверждающих, что ПДн, которые относятся к соответствующему субъекту и обработку которых осуществляет Оператор, являются неполными, неточными или неактуальными (согласно части 3 статьи 20 Федерального закона № 152-ФЗ) и отправить уведомление о внесенных изменениях. Если обработка ПДн субъекта не ведется или не были предоставлены сведения, подтверждающие, что ПДн, которые относятся к соответствующему субъекту и обработку которых осуществляет Оператор, являются неполными, неточными или неактуальными, то необходимо в течение 30 дней с даты получения запроса отправить уведомление об отказе в осуществлении изменения ПДн.

При получении запроса субъекта персональных данных на уничтожение ПДн необходимо их уничтожить в срок, не превышающий 7 рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие ПДн являются незаконно полученными или не являются необходимыми для заявленной цели обработки (согласно части 3 статьи 20 Федерального закона № 152-ФЗ), и отправить уведомление об уничтожении. Если обработка ПДн субъекта не ведется или не были предоставлены сведения, подтверждающие, что ПДн, которые относятся к соответствующему субъекту и обработку которых осуществляет Оператор, являются незаконно полученными или не являются необходимыми для заявленной цели обработки, а также в силу необходимости обработки ПДн по требованиям иных законодательных актов, то необходимо в течение 30 дней с даты получения запроса отправить уведомление об отказе в уничтожении ПДн.

При получении запроса на отзыв согласия субъекта персональных данных на обработку ПДн необходимо прекратить их обработку и, в случае, если сохранение ПДн более не требуется для целей обработки ПДн, уничтожить ПДн в срок, не превышающий 30 дней с даты поступления указанного отзыва (согласно части 5 статьи 21 Федерального закона № 152-ФЗ), если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если Оператор не вправе осуществлять обработку ПДн без согласия субъекта персональных данных на основаниях, предусмотренных настоящим Федеральным законом или другими федеральными законами (согласно части 5 статьи 21 Федерального закона № 152-ФЗ).

При выявлении недостоверности ПДн при обращении или по запросу субъекта ПДн необходимо их блокировать с момента такого обращения или получения такого запроса на период проверки (согласно части 1 статьи 21 Федерального закона № 152-ФЗ). Если факт недостоверности ПДн подтвержден на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов, необходимо уточнить ПДн в течение 7 рабочих дней со дня представления таких сведений и снять блокирование ПДн (согласно части 2 статьи 21 Федерального закона № 152-ФЗ). Если факт недостоверности ПДн не подтвержден, то необходимо отправить уведомление об отказе в изменении ПДн.

При выявлении неправомерных действий с ПДн Оператору по запросу субъекта ПДн необходимо в срок, не превышающий трех рабочих дней с даты этого выявления, прекратить неправомерную обработку ПДн (согласно части 3 статьи 21 Федерального закона № 152-ФЗ). В случае если обеспечить правомерность обработки ПДн невозможно, Оператор в срок, не превышающий 10 рабочих дней с даты выявления неправомерной обработки ПДн (согласно части 3 статьи 21 Федерального закона № 152-ФЗ), обязан уничтожить такие ПДн. Об устранении допущенных нарушений или об уничтожении ПДн Оператор обязан уведомить субъекта персональных данных, а в случае, если обращение субъекта персональных данных либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

При достижении целей обработки ПДн Оператор обязан незамедлительно прекратить обработку ПДн и уничтожить соответствующие ПДн в течение 30 дней с даты достижения цели обработки ПДн (согласно части 4 статьи 21 Федерального закона № 152-ФЗ), если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если Оператор не вправе осуществлять обработку ПДн без согласия

субъекта персональных данных на основаниях, предусмотренных Федерального закона № 152-ФЗ или другими федеральными законами, и отправить уведомление об уничтожении ПДн.

В случае поступления запроса уполномоченного органа по защите прав субъекта персональных данных по ПДн необходимо выполнить следующие действия:

- при получении запроса необходимо в течение 30 дней (согласно части 4 статьи 20 Федерального закона № 152-ФЗ) предоставить информацию, необходимую для осуществления деятельности указанного органа;
- при выявлении недостоверных ПДн по запросу уполномоченного органа по защите прав субъекта ПДн необходимо их блокировать с момента такого обращения или получения такого запроса на период проверки (согласно части 1 статьи 21 Федерального закона № 152-ФЗ). Если факт недостоверности ПДн подтвержден на основании документов, предоставленных субъектом ПДн, необходимо в течение 7 рабочих дней уточнить ПДн и снять их блокирование (согласно части 2 статьи 21 Федерального закона № 152-ФЗ). Если факт недостоверности ПДн не подтвержден, то необходимо отправить уведомление об отказе изменения и снять блокирование ПДн;
- при выявлении неправомерных действий Оператора с ПДн по запросу уполномоченного органа по защите прав субъекта ПДн необходимо прекратить неправомерную обработку ПДн в срок, не превышающий 3 рабочих дней с момента такого обращения или получения такого запроса на период проверки (согласно части 1 статьи 21 Федерального закона 152-ФЗ). В случае невозможности обеспечения правомерности обработки оператором ПДн в срок, не превышающий 10 рабочих дней с даты выявления неправомерности действий с ПДн, необходимо уничтожить ПДн и отправить уведомление об уничтожении ПДн.

4. Ответственность Оператора

Персональные данные не подлежат разглашению (распространению). Прекращение доступа к такой информации не освобождает работника от взятых им обязательств по неразглашению информации ограниченного доступа.

Организация и проведение работ по ответам на запросы, устранению нарушений, а также уточнению, блокированию и уничтожению ПДн возлагается на ответственного в учреждении за обработку персональных данных. Нарушение установленного порядка рассмотрения запросов влечет в отношении виновных должностных лиц ответственность в соответствии с законодательством Российской Федерации.

Типовые формы документов по запросу субъектов персональных данных или их представителей

Директору ТОГКУ «МФЦ»
_____
(ф.и.о. заявителя)
_____
_____
_____
проживающего по адресу:
_____
_____
_____
_____
_____
(наименование и реквизиты документа,
удостоверяющего личность заявителя)

Заявление

В том случае, если ТОГКУ «МФЦ» обрабатывает мои персональные данные, прошу предоставить мне сведения о Вашей организации. В противном случае прошу Вас уведомить меня об отсутствии обработки моих персональных данных.

Ответ прошу направить в письменной форме по вышеуказанному адресу в срок, предусмотренный Федеральным законом от 27 июля 2006 г. № 152 ФЗ "О персональных данных".

"___" _____ 20 ___г. _____
(подпись)

Директору ТОГКУ «МФЦ»
_____
(ф.и.о. заявителя)
_____
_____
_____
проживающего по адресу:
_____
_____
_____
_____
_____
(наименование и реквизиты документа,
удостоверяющего личность заявителя)

Заявление

В соответствии со статьей 14 Федерального закона от 27 июля 2006 г. № 152 ФЗ "О персональных данных", прошу предоставить мне для ознакомления обрабатываемую Вами информацию, составляющую мои персональные данные, указать:

- осуществляется ли обработка моих персональных данных;
- цели, способы и сроки ее обработки;
- перечень обрабатываемых вами моих персональных данных и источник их получения;
- какие лица имеют доступ или могут получить доступ к моим персональным данным;
- срок хранения моих персональных данных;
- осуществлялась ли трансграничная передача моих персональных данных, если нет, то предполагается ли такая передача;
- сведения о том, какие юридические последствия для меня может повлечь её обработка;
- другое.

Ответ прошу направить в письменной форме по вышеуказанному адресу в предусмотренный Законом срок.

___" _____ 20 ____г. _____
(подпись)

_____
____

расшифровка подписи

Уведомление субъекта ПДн об обработке ПДн

Уважаемый(ая) _____,
(ф.и.о.)

ТОГКУ «МФЦ» производится обработка сведений, составляющих Ваши персональные данные: _____
_____
_____
_____
_____
_____
_____
(указать сведения)

Цели обработки: _____
Способы обработки: _____
Перечень лиц, которые имеют доступ к информации, содержащей Ваши персональные данные или могут получить такой доступ:

Должность	Ф.И.О.	Вид доступа	Примечания	

Другое.

По результатам обработки указанной информации нами планируется принятие следующих решений _____
_____
_____, которые будут доведены до Вашего сведения.

Против принятого решения Вы имеете право заявить свои письменные возражения в _____ срок.

_____ _____
(должность) (подпись) _____

___" _____ 20__г. асшифровка подписи)

Директору ТОГКУ «МФЦ»
_____
(ф.и.о. заявителя)
_____
_____
_____
проживающего по адресу:
_____
_____
_____
_____
_____
(наименование и реквизиты документа,
удостоверяющего личность заявителя)

Заявление

Прошу уточнить обрабатываемые Вами мои персональные данные в соответствии со сведениями: _____
_____,
_____
_____
_____
(указать уточненные персональные данные заявителя)

в связи с тем, что _____

_____
_____
_____
(указать причину уточнения персональных данных)

Ответ прошу направить в письменной форме по вышеуказанному адресу в срок, предусмотренный Федеральным законом от 27 июля 2006 г. № 152 ФЗ "О персональных данных".

_" __ 20 ___г. _____
(подпись)
_____
(расшифровка
подписи)

Уведомление об уточнении ПДн субъекта ПДн

Уважаемый(ая)_____,
(ф.и.о.)

в связи с _____
_____

сообщаем Вам, что Ваши персональные данные уточнены в соответствии со сведениями:
_____
_____

Директор ТОГКУ «МФЦ» _____
(расшифровка, подпись)

ректор ТОГКУ «МФЦ» _____
(должность)

"___" _____ 20__г.

Директору ТОГКУ «МФЦ»
_____
(ф.и.о. заявителя)
_____
_____
_____
проживающего по адресу:
_____
_____
_____
_____
_____
(наименование и реквизиты документа,
удостоверяющего личность заявителя)

Заявление

Прошу заблокировать обрабатываемые Вами мои персональные данные:
_____
_____
_____
_____
_____
_____
(указать блокируемые персональные данные)

на срок:_____, в связи с тем, что_____
_____
_____
_____
(указать срок блокирования) (указать причину блокирования данных)

Ответ прошу направить в письменной форме по вышеуказанному адресу в срок, предусмотренный Федеральным законом от 27 июля 2006 г. № 152 ФЗ "О персональных данных".

__" _____ 20___г. _____ _____
(подпись) (расшифровка подписи)

Уведомление о блокировании ПДн субъекта ПДн

Уважаемый(ая) _____,
(ф.и.о.)
в связи с _____ сообщаем Вам, что Ваши персональные данные _____
_____
_____
_____
_____
_____
(указать персональные данные)

заблокированы на срок _____

Директор ТОГКУ «МФЦ» _____
(расшифровка, подпись)

_____
(должность)

"___" _____ 20 ___г.

Директору ТОГКУ «МФЦ»
_____
(ф.и.о. заявителя)
_____
_____
_____
проживающего по адресу:
_____
_____
_____
_____
_____
(наименование и реквизиты документа,
удостоверяющего личность заявителя)

Заявление

Прошу Вас прекратить обработку и уничтожить мои персональные данные: _____
_____
_____
_____
_____
(указать уничтожаемые персональные данные)
в связи с тем, что _____.
(указать причину уничтожения персональных данных)
_____
_____
_____
_____

Ответ прошу направить в письменной форме по вышеуказанному адресу в срок, предусмотренный Федеральным законом от 27 июля 2006 г. № 152 ФЗ "О персональных данных".

"___" _____ 20 ___г. _____ _____
(подпись) (расшифровка подписи)

Уведомление о прекращении обработки и уничтожении ПДн субъекта ПДн

Уважаемый(ая) _____
(ф.и.о.)
в связи с _____
_____
_____
_____
сообщаем Вам, что обработка Ваших персональных данных прекращена и Ваши персональные данные _____

_____
_____
_____
_____
(указать персональные данные)
уничтожены.

_____
(должность)

"____" _____ 20 ___г.

Директор ТОГКУ «МФЦ» _____
(расшифровка, подпись)

_____
(ф.и.о. заявителя)
_____
_____
_____
проживающего по адресу:
_____
_____
_____
_____
_____

Запрос

Уважаемый(ая) _____,
(ф.и.о.)
в связи с _____
у администрации ТОГКУ «МФЦ» возникла необходимость получения следующей информации, составляющей Ваши персональные данные: _____
_____
_____
_____
_____
_____
_____
_____
(перечислить информацию)

Просим Вас предоставить указанные сведения в течение _____ рабочих дней с момента получения настоящего запроса.

В случае невозможности предоставить указанные сведения просим в указанный срок дать письменное согласие на получение нами необходимой информации из следующих источников _____ следующими способами _____

По результатам обработки указанной информации нами планируется принятие следующих решений, которые будут доведены до Вашего сведения. _____

Против принятого решения Вы имеете право заявить свои письменные возражения в _____ срок.

Ответ прошу направить в письменной форме в наш адрес в срок, предусмотренный Федеральным законом от 27 июля 2006 г. № 152 ФЗ "О персональных данных".

_____ _____ _____
(должность) (подпись) (расшифровка подписи)

"___" _____ 20 ___г.

Уведомление субъекта ПДн об устранении допущенных нарушений

Уважаемый(ая) _____
(ф.и.о.)
в связи с _____
_____
сообщаем Вам, что все допущенные нарушения при обработке Ваших персональных данных устранены.

Нашим учреждением были внесены изменения в Ваши персональные данные:_____
_____
_____
_____
_____
_____
(указать персональные данные)

_____
(должность)

"___" _____ 20__г.

Директор ТОГКУ «МФЦ» _____
(расшифровка, подпись)

ЖУРНАЛ

учета запросов граждан (субъектов персональных данных) в ТОГКУ «МФЦ»
по вопросам обработки персональных данных

Начат: "___" _____ 20 ___ г.

Окончен: "___" _____ 20 ___ г.

На _____ листах

Срок хранения _____ лет

Содержание

№ п/п	Сведения о запрашивающем лице	Краткое содержание запроса	Цель запроса	Отметка о предоставлении информации или отказе в ее предоставлении	Дата передачи /отказа в предоставлении информации	Подпись ответственного лица	Примечание
1	2	3	4	5	6	7	8

Разъяснения субъекту
персональных данных юридических последствий отказа предоставить
свои персональные данные

Уважаемый(-ая), _____
(имя, отчество)

В соответствии с требованиями Федерального закона Российской Федерации от 27 июля 2006 г. №152-ФЗ "О персональных данных" уведомляем Вас, что обязанность предоставления Вами персональных данных установлена_____
_____ Федерального закона
(пункт, статья, часть)
_____,
(реквизиты и наименование федерального закона)
а также следующими нормативными актами_____
_____.
(указываются реквизиты и наименования таких нормативных актов)
_____
_____
_____
_____
_____

В случае отказа Вами предоставить свои персональные данные ТОГКУ «МФЦ» не сможет на законных основаниях осуществлять такую обработку, что приведет к следующим для Вас юридическим последствиям._____
_____.
(перечислить юридические последствия для субъекта персональных данных, то есть случаи возникновения, изменения или прекращения личных либо имущественных прав граждан или случаи иным образом затрагивающее его права, свободы и законные интересы)
_____
_____
_____
_____
_____

В соответствии с действующим законодательством Российской Федерации в области персональных данных Вы имеете право:

на получение сведений о ТОГКУ «МФЦ» как операторе, осуществляющем обработку Ваших персональных данных (в объеме, необходимом для защиты своих прав и законных интересов по вопросам обработки своих персональных данных), о месте нахождения учреждения, о наличии у МФЦ своих персональных данных, а также на ознакомление с такими персональными данными;

подавать запрос на доступ к своим персональным данным;

требовать безвозмездного предоставления возможности ознакомления со своими персональными данными, а также внесения в них необходимых изменений, их уничтожения или блокирования при предоставлении сведений, подтверждающих, что такие персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки;

получать уведомления по вопросам обработки персональных данных в установленных действующим законодательством Российской Федерации случаях и сроки;

требовать от ТОГКУ «МФЦ» разъяснения порядка защиты субъектом персональных данных своих прав и законных интересов;

обжаловать действия или бездействие оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке;

на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

Директор ТОГКУ «МФЦ» _____

(инициалы, подпись)

ПРИЛОЖЕНИЕ № 5
УТВЕРЖДЕНО
Приказом ТОГКУ «МФЦ»
от _____ № ___

Правила
осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в ТОГКУ «МФЦ»

1. Общие положения

Настоящие Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в ТОГКУ «МФЦ» (далее - Правила) относятся к основным организационно-распорядительным документам системы документов информационной безопасности учреждения и разработаны в соответствии с требованиями постановления Правительств Российской Федерации от 21 марта 2012 г. № 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 Правилах определен порядок организации и осуществления внутреннего контроля обработки персональных данных (ПДн) в ТОГКУ «МФЦ» с целью своевременного выявления и предотвращения:

- хищения технических средств и носителей информации;
- утраты информации;
- преднамеренных программно-технических воздействий на информацию и (или) средства вычислительной техники, вызывающих нарушение целостности информации и нарушение работоспособности автоматизированной системы;
- несанкционированного доступа к ПДн с целью уничтожения, искажения, модификации (подделки), копирования и блокирования;
- утечки информации по техническим каналам.

Внутренний контроль состояния защиты информации включает в себя:

- контроль организации защиты информации;
- контроль эффективности защиты информации.

2. Порядок внутреннего контроля за соблюдением требований по обработке и обеспечению безопасности персональных данных

В целях осуществления внутреннего контроля соответствия обработки ПДн установленным требованиям организуется проведение периодических проверок условий обработки ПДн. Проверки осуществляются заместителем директора или работниками ответственными за соблюдение требований по обработке ПДн не реже одного раза в год в соответствии с утвержденным графиком.

При осуществлении внутреннего контроля соответствия обработки ПДн установленным требованиям производится проверка:

- соблюдения принципов обработки ПДн;
- соответствия локальных актов в области ПДн, действующему законодательству Российской Федерации;
- выполнения работниками МФЦ требований и правил обработки ПДн в информационных системах персональных данных (ИСПДн) ТОГКУ «МФЦ»;

- перечней ПДн, используемых для решения задач и функций структурными подразделениями МФЦ и необходимости обработки ПДн в ИСПДн ТОГКУ «МФЦ»;
- актуальности содержащихся в Правилах обработки ПДн в ТОГКУ «МФЦ» в каждой ИСПДн учреждения информации о законности целей обработки ПДн и оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности ПДн;
- правильности осуществления сбора, систематизации, записи, накопления, хранения, уточнения (обновления, изменения), извлечения, использования, передачи (распространения, предоставления, доступа), обезличивания, блокирования, удаления, уничтожения ПДн в каждой ИСПДн;
- актуальности перечня должностей работников ТОГКУ «МФЦ», имеющих доступ к ПДн;
- соблюдения прав субъектов персональных данных, чьи ПДн обрабатываются в ИСПДн ТОГКУ «МФЦ»;
- соблюдения обязанностей ТОГКУ «МФЦ» как оператора ПДн, предусмотренных действующим законодательством в области ПДн;
- порядка взаимодействия с субъектами персональных данных, ПДн данные которых обрабатываются в ИСПДн МФЦ, в том числе соблюдения сроков, предусмотренных действующим законодательством в области ПДн, соблюдения требований по уведомлениям, порядка разъяснения субъектам персональных данных необходимой информации, порядка реагирования на обращения (запросы) субъектов персональных данных, порядка действий при достижении целей обработки ПДн и отзыве согласий субъектами персональных данных;
- наличия необходимых согласий субъектов персональных данных, чьи ПДн обрабатываются в ИСПДн МФЦ;
- актуальности сведений, содержащихся в уведомлении об обработке (о намерении осуществлять обработку) персональных данных;
- актуальности перечня ИСПДн в ТОГКУ «МФЦ»;
- наличия и актуальности сведений, содержащихся в Правилах обработки ПДн ТОГКУ «МФЦ» для каждой ИСПДн МФЦ;
- знания и соблюдения работниками ТОГКУ «МФЦ» положений действующего законодательства Российской Федерации в области ПДн;
- знания и соблюдения работниками ТОГКУ «МФЦ» локальных актов администрации области в области обработки и обеспечения безопасности ПДн;
- знания и соблюдения работниками инструкций, руководств и иных эксплуатационных документов на применяемые средства автоматизации, в том числе программное обеспечение, и средства защиты информации;
- соблюдения работниками МФЦ конфиденциальности ПДн;
- проверка наличия и актуальности локальных актов ТОГКУ «МФЦ» в области обеспечения безопасности ПДн, в том числе в Технических паспортах ИСПДн;

О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, лицо, ответственное за проведение проверки, докладывает директору МФЦ

При проведении внутреннего контроля на ИСПДн (отдельное автоматизированное рабочее место) ТОГКУ «МФЦ» составляется протокол контроля выполнения требований по обеспечению безопасности информации, содержащей сведения ограниченного доступа, при ее автоматизированной обработке на автоматизированном рабочем месте.

ПРИЛОЖЕНИЕ № 6
УТВЕРЖДЕНО
Приказом ТОГКУ «МФЦ»
от _____ № ___

Правила
работы с обезличенными персональными данными в ТОГКУ «МФЦ»

1. Общие положения

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

Настоящие Правила определяют порядок работы с обезличенными данными в ТОГКУ «МФЦ» и действуют постоянно.

2. Условия обезличивания

Обезличивание персональных данных (ПДн) проводится с целью снижения ущерба от разглашения защищаемых ПДн и снижения требований к защите информационной системы персональных данных (ИСПДн) ТОГКУ «МФЦ».

Обезличивание персональных данных также осуществляется по достижению целей обработки ПДн или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено Федеральным законом.

Способы обезличивания при условии дальнейшей обработки ПДн:

- уменьшение перечня обрабатываемых сведений;
- замена части сведений идентификаторами;
- замена численных значений минимальным, средним или максимальным значением (например, иногда нет необходимости обрабатывать сведения о возрасте каждого субъекта, достаточно обрабатывать данные о среднем возрасте по всей выборке или отдельным ее частям);
- обобщение - понижение точности некоторых сведений;
- понижение точности некоторых сведений;
- деление сведений на части и обработка их в разных информационных системах;
- другие способы.

Способом обезличивания в случае достижения целей обработки или в случае утраты необходимости в достижении этих целей является сокращение перечня ПДн.

Для обезличивания ПДн применяются любые способы явно не запрещенные законодательно.

Перечень должностей ТОГКУ «МФЦ», ответственных за проведение мероприятий по обезличиванию обрабатываемых ПДн, утвержден приказом директора ТОГКУ «МФЦ».

Решение о необходимости обезличивания ПДн принимает руководитель МФЦ.

Руководители структурных подразделений ТОГКУ «МФЦ», непосредственно осуществляющих обработку ПДн, готовят предложения по обезличиванию ПДн, обоснование такой необходимости и определяют способ обезличивания.

Работники ТОГКУ «МФЦ» обслуживающие базы данных с ПДн, осуществляют непосредственное обезличивание выбранным способом.

3. Порядок работы с обезличенными персональными данными

Обезличенные ПДн не подлежат разглашению и нарушению конфиденциальности.

Обезличенные ПДн могут обрабатываться с использованием и без использования средств автоматизации.

При обработке обезличенных ПДн с использованием средств автоматизации необходимо соблюдение:

- парольной политики;
- антивирусной политики;
- правил работы со съемными носителями (если они используется);
- правил резервного копирования;
- правил доступа в помещения, где расположены элементы информационных систем.

При обработке обезличенных ПДн без использования средств автоматизации необходимо соблюдение:

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

ПРИЛОЖЕНИЕ № 7
УТВЕРЖДЕНО
приказом ТОГКУ «МФЦ»
от _____№ _____

СОГЛАСИЕ
работников ТОГКУ «МФЦ» на обработку персональных данных

Я, _____,
(Ф.И.О.)

дата рождения _____, зарегистрированный(ая) по адресу: _____
_____, документ, удостоверяющий личность: паспорт, серия_____
номер_____выдан_____
дата выдачи _____, даю согласие Тамбовскому областному государственному казенному учреждению «Многофункциональный центр предоставления государственных и муниципальных услуг» (392017, г. Тамбов, ул. М. Горького, д. 20) на обработку моих персональных данных, содержащихся в моем личном деле и (или) в электронном виде на локальной компьютерной сети (фамилии, имени, отчества, даты рождения, адреса, контактного телефона, реквизитов полиса ОМС, СНИЛС и иной информации, относящейся к моей личности) для совершения любых действий, связанных с выполнением мной трудовых функций.

Также ТОГКУ «МФЦ» вправе обрабатывать мои персональные данные посредством внесения их в электронную базу данных, включения в списки (реестры) и отчетные формы, предусмотренные документами, регламентирующими предоставление отчетных данных (документов).

Настоящим я признаю и подтверждаю, что в случае необходимости предоставления моих персональных данных третьему лицу, передачи ТОГКУ «МФЦ» принадлежащих ему функций и полномочий иному лицу, ТОГКУ «МФЦ» вправе в необходимом объеме раскрывать для совершения вышеуказанных действий информацию обо мне лично (включая мои персональные данные) таким третьим лицам, их представителям и иным уполномоченным ими лицам, а также предоставлять таким лицам соответствующие документы (копии документов), содержащие такую информацию.

Также настоящим признаю и подтверждаю, что настоящее согласие считается данным мною любым третьим лицам, указанным выше и любые такие третьи лица имеют право на обработку моих персональных данных на основании настоящего согласия и передачу информации обо мне и моих персональных данных ТОГКУ «МФЦ».

Настоящее согласие действует с «___»_____ 20__г. и до
(дата начала трудовой деятельности)

прекращения мною трудовых отношений с ТОГКУ «МФЦ».

_____ _____ _____
(дата) (подпись) (расшифровка подписи)

ПРИЛОЖЕНИЕ № 8
УТВЕРЖДЕНО
приказом ТОГКУ «МФЦ»
от _____№ _____

Обязательство о неразглашении
персональных данных субъекта

Я, _____, паспорт серии _____,
(Ф.И.О.)
номер_____, выданный _____
« ___ » _____ 20___ года, понимаю, что получаю доступ к персональным данным
_____
_____
(работников мфц, ТОСП, заявителей, обращающихся в МФЦ за предоставлением услуг. Указать нужное)

Я также понимаю, что во время исполнения своих обязанностей мне приходится заниматься сбором, обработкой и хранением персональных данных.

Я понимаю, что разглашение такого рода информации может нанести ущерб субъектам персональных данных, как прямой, так и косвенный.

В связи с этим даю обязательство при работе (сбор, обработка и хранение) с персональными данными соблюдать все требования, описанные в Положение об обработке персональных данных в ТОГКУ «МФЦ».

Я подтверждаю, что не имею права разглашать сведения (указываются сведения, не подлежащие разглашению):
_____
_____
_____
_____
_____
_____
_____
_____

Я предупрежден(а) о том, что в случае разглашения мной сведений, касающихся персональных данных или их утраты я несу ответственность в соответствии действующим законодательством Российской Федерации.

« ___ » _____ 20__ г. _____
(подпись)

ПРИЛОЖЕНИЕ № 9
УТВЕРЖДЕНО
приказом ТОГКУ «МФЦ»
от _____№ _______

ПЕРЕЧЕНЬ

персональных данных, обрабатываемых в связи с реализацией трудовых отношений

1. Фамилию, имя, отчество субъекта персональных данных;
2. Дату рождения субъекта персональных данных;
3. Должность субъекта персональных данных;
4. Данные документа удостоверяющих личность;
5. Номер правового акта и дату приема на работу (увольнения) субъекта персональных данных;
6. Сведения о трудовом стаже субъекта персональных данных (данные трудовой книжки);
7. Сведения об образовании субъекта персональных данных;
8. Сведения о повышении квалификации субъекта персональных данных;
9. Сведения об ученой степени субъекта персональных данных;
10. Сведения об аттестации субъекта персональных данных;
11. Сведения о воинском учете субъекта персональных данных;
12. Сведения о государственных наградах субъекта персональных данных;
13. Вид служебного контракта субъекта персональных данных;
14. Данные о включении в кадровый резерв субъекта персональных данных;
15. Основания исключения из резерва субъекта персональных данных

ПРИЛОЖЕНИЕ № 10
УТВЕРЖДЕНО
приказом ТОГКУ «МФЦ»
от _____№ _____

ПЕРЕЧЕНЬ

персональных данных, обрабатываемых в связи с предоставлением государственных и муниципальных услуг

1. Фамилию, имя, отчество субъекта персональных данных;
2. Дату рождения субъекта персональных данных;
3. Адрес места жительства субъекта персональных данных;
4. Данные документа удостоверяющего личность;
5. Должность субъекта персональных данных;
6. Телефон субъекта персональных данных;
7. ИНН субъекта персональных данных;
8. СНИЛС
9. Сведения о правоустанавливающих и правоудостоверяющих документах.

ПРИЛОЖЕНИЕ № 11
УТВЕРЖДЕНО
приказом ТОГКУ «МФЦ»
от _____№ _____

ПЕРЕЧЕНЬ

должностей работников ТОГКУ «МФЦ», ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных

1. Директор учреждения
2. Заместители директора
3. Начальник филиала
4. Инженер-электроник
5. Начальник отдела информационно-технологического обеспечения.
6. Начальник отдела предоставления государственных и муниципальных услуг в МФЦ.
7. Начальник отдела предоставления государственных и муниципальных услуг
8. Начальник экспертно-правового отдела.
9. Секретарь руководителя
10. Ведущий инспектор по кадрам
11. Инспектор по кадрам

ПРИЛОЖЕНИЕ № 12
УТВЕРЖДЕНО
приказом ТОГКУ «МФЦ»
от ____№ _____

ПЕРЕЧЕНЬ

должностей работников ТОГКУ «МФЦ», имеющих доступ к персональным данным работников учреждения

1. Директор учреждения
2. Заместители директора
3. Главный бухгалтер, начальник отдела
4. Бухгалтер
5. Секретарь руководителя
6. Инженер по охране труда и энергообеспечению
7. Ведущий инспектор по кадрам
8. Инспектор по кадрам
9. Начальники отделов
10. Заместители начальников отделов
11. Начальник филиала
12. Заместитель начальника филиала
13. Ведущий юрисконсульт
14. Главный юрисконсульт-эксперт
15. Аналитик (отдел предоставления государственных и муниципальных услуг в структурных подразделениях (ТОСП)

ПРИЛОЖЕНИЕ № 13
УТВЕРЖДЕНО
приказом ТОГКУ «МФЦ»
от _____№ _____

ПЕРЕЧЕНЬ

должностей работников ТОГКУ «МФЦ», имеющих доступ к персональным данным заявителей

1. Директор учреждения
2. Заместители директора
3. Секретарь руководителя
4. Ведущий инспектор по кадрам
5. Инспектор по кадрам
6. Начальники отделов (за исключением начальника отдела материально-технического обеспечения и начальника хозяйственного отдела)
7. Заместители начальников отделов
8. Главный юрисконсульт-эксперт
9. Юрисконсульт
10. Главный специалист
11. Специалист
12. Инженер-электроник
13. Инженер программист
14. Старший администратор
15. Администратор
16. Начальник филиала
17. Заместитель начальника филиала
18. Аналитик (отдел предоставления государственных и муниципальных услуг в структурных подразделениях (ТОСП)

ПРИЛОЖЕНИЕ № 14
УТВЕРЖДЕНО
Приказом ТОГКУ
«МФЦ»
от _____ № ___

Порядок
доступа работников ТОГКУ «МФЦ», в помещения учреждения, в которых ведется обработка персональных данных

1. Общие положения

Настоящий Порядок доступа работников ТОГКУ «МФЦ» в помещения МФЦ, в которых ведется обработка персональных данных, (далее – Порядок) разработан в соответствии с Федеральным законом от 27 июля 2006 г. № 152 - ФЗ "О персональных данных" и постановлением Правительства Российской Федерации от 21 марта 2012 г. № 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами" и другими нормативными правовыми актами.

Настоящий Порядок регламентирует условия и порядок осуществления доступа работников ТОГКУ «МФЦ» в помещения МФЦ, в которых ведется обработка персональных данных (далее - помещения) в целях обеспечения безопасности персональных данных (ПДн).

Для обеспечения доступа работников МФЦ в помещения предусматривается комплекс специальных мер, направленных на поддержание и обеспечение установленного порядка деятельности учреждения.

Указанные меры организуются ответственным за организацию обработки ПДн, а осуществляются руководителями структурных подразделений МФЦ, осуществляющих обработку ПДн. Контроль за порядком обеспечения доступа работников ТОГКУ «МФЦ» в помещения осуществляется руководителями структурных подразделений администрации области, осуществляющих обработку ПДн.

Обеспечение безопасности персональных данных от уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн достигается, в том числе, установлением правил доступа в помещения, где ведется обработка ПДн с использованием средств автоматизации или без использования таковых.

Для помещений, в которых обрабатываются ПДн, организуется режим обеспечения безопасности, при котором обеспечивается сохранность носителей ПДн и средств защиты информации, а также исключается возможность неконтролируемого проникновения и пребывания в этих помещениях посторонних лиц.

2. Порядок доступа работников ТОГКУ «МФЦ» в помещения

2.1. Доступ работников МФЦ и работников организаций, предоставляющих услуги в МФЦ в зал МФЦ до открытия учреждения осуществляется по постоянным пропускам или по документам удостоверяющим личность под контролем охранников (в Мичуринском филиала – вахтеров). До окончания рабочего времени охрана помещения залов осуществляется: в Тамбовском МФЦ- охранниками в рамках заключенного контракта по охране помещения, в

филиале - вахтерами. Режим охраны и порядок действия сотрудников охраны регламентирован «Инструкцией по организации охраны и пропускного режима в ТОГКУ «МФЦ», а вазтеров – должностной инструкцией.

Пребывание посторонних лиц в залах допускается только в присутствии вышеуказанных работников на время, ограниченное необходимостью решения вопросов, связанных с исполнением функций по предоставлению государственных и муниципальных услуг или осуществлением полномочий в рамках договоров, заключенных с ТОГКУ «МФЦ». Доступ посторонних лиц на территорию рабочих мест – («окон») со стороны специалистов ведущих прием заявителей запрещен. Во время перерыва (обед, время отдыха т.п) компьютер специалиста выключается и свободные «окна» находятся по усиленным наблюдением охранников (вахтеров).

2.2. Совмещенный кабинет, предназначенный для работы специалистов УФМС и кадровой службы ТОГКУ «МФЦ» имеют право вскрывать (закрывать) ведущий инспектор по кадрам, инспектор по кадрам и специалисты УФМС, согласно списку, утвержденному начальником ООЗП УФМС России по Тамбовской области и приказу директора ТОГКУ «МФЦ» от 11.03.2015 № 1-ахд Первый из указанных специалистов, пришедший на работу, в присутствии охранника вскрывает кабинет с отметкой о вскрытии в журнале вскрытия (закрытия) помещений. Доступ посторонних лиц в кабинет происходит после его вскрытия под контролем работников ТОГКУ «МФЦ» и специалистов УФМС в рамках исполнения ими своих должностных обязанностей. Опечатывание и сдача кабинета под охрану после окончания рабочего времени производится этими же лицами с отметкой в журнале вскрытия (закрытия) помещений.

2.3. Кабинет работников экспертно-правового отдела имеют право вскрывать (закрывать) работники этого отдела. Первый из работников отдела, пришедший на работу, в присутствии охранника вскрывает кабинет с отметкой о вскрытии в журнале вскрытия (закрытия) помещений. Доступ посторонних лиц в кабинет происходит после его вскрытия под контролем работников отдела в рамках исполнения ими своих должностных обязанностей. Опечатывание и сдача кабинета под охрану после окончания рабочего времени производится этими же лицами с отметкой в журнале вскрытия (закрытия) помещений.

2.4. Доступ работников в другие кабинеты и помещения осуществляется в соответствии со списком работников ТОГКУ «МФЦ», имеющих право самостоятельного доступа в помещения, в которых ведется обработка ПДн и допуска к обработке персональных данных (далее - Список).

Список готовится и уточняется, ответственным за организацию обработки ПДн, по представлению руководителей структурных подразделений МФЦ, осуществляющих обработку ПДн, и утверждается директором учреждения.

2.5. Внутренний контроль за соблюдением порядка доступа в помещения ТОГКУ «МФЦ» проводится ответственным за организацию обработки ПДн или комиссией, список которой утверждается распоряжением директора.

ПРИЛОЖЕНИЕ № 16
УТВЕРЖДЕНО
Приказом ТОГКУ «МФЦ»
от _____ № ___

Инструкция пользователя
автоматизированной системы при работе с персональными данными.

Пользователи АИС МФЦ и др. информационных систем, обязаны строго соблюдать установленные правила работы на комплексах средств автоматизации и несут персональную ответственность за неукоснительное выполнение требований и мероприятий по защите информации на своих автоматизированных рабочих местах.

Пользователи обязаны:

- знать и выполнять требования руководства оператора при работе в АИС МФЦ и др. информационных системах;
- знать и соблюдать установленные требования по режиму обработки конфиденциальной информации, учету и хранению машинных носителей информации;
- при работе в АИС МФЦ и др. информационных системах использовать только учтенные установленным порядком машинные носители информации, штатное общесистемное, прикладное и специальное программное обеспечение;
- экран видеомонитора в помещении располагать во время работы так, чтобы исключалась возможность ознакомления посторонними лицами с отображаемой на нём информацией;
- при выходе из помещения в течение рабочего дня выключать или блокировать рабочую станцию;
- соблюдать правила работы со средствами защиты информации и установленный режим разграничения доступа к техническим средствам, программам, данным, файлам с конфиденциальной информацией, в том числе персональными данными при их обработке;
- уметь пользоваться средствами антивирусной защиты и при необходимости проверять ПЭВМ на наличие вредоносных программ – «вирусов» ,осуществлять антивирусный контроль ПЭВМ не реже одного раза в неделю;
- осуществлять проверку файлов на наличие вредоносных программ перед началом обработки информации, хранящейся на съемных машинных носителях информации.
- перед началом работы получить у Администратора свои учётные данные (логин, пароль, идентификатор), надежно запоминать и хранить в тайне;
- докладывать Администратору о фактах компрометации пароля, несанкционированного доступа со стороны других пользователей, случаях утечки и нарушения целостности информации, обрабатываемой в АС, нарушениях целостности компонентов системы защиты информации;
- информировать Администратора о нарушениях установленной технологии обработки защищаемой информации или нарушениях функционирования средств и систем защиты информации.

Пользователям АИС МФЦ и др. информационных систем запрещается:

- осуществлять обработку информации конфиденциального характера на автоматизированном рабочем месте (АРМ) без выполнения мероприятий по защите информации;
- обрабатывать информацию с грифом, выше установленного для АИС МФЦ и др. информационных систем;
- оставлять без контроля АРМ до окончания сеанса работы без его блокировки;

- оставлять во время работы съемные носители с конфиденциальной информацией без присмотра, передавать их посторонним лицам;
- сообщать устно или письменно другим лицам личные имена учётных записей и пароли к ним;
- осуществлять ввод паролей, допуская возможность ознакомления с ними посторонних лиц;
- сообщать (или передавать) посторонним лицам личные атрибуты доступа к ресурсам АИС МФЦ и др. информационных систем;
- хранить пароли на любых носителях (как бумажных, так и электронных);
- самовольно вносить изменения в состав, конструкцию и размещение аппаратного обеспечения АИС МФЦ и др. информационных систем, открывать крышки устройств и блоков технических средств объекта информатизации;
- устанавливать и использовать при работе в АИС МФЦ и в др. информационных системах программное обеспечение, не входящее в перечень средств указанных в документации на АИС МФЦ и др. информационных систем,
- изменять установленный алгоритм функционирования технических и программных средств;
- осуществлять электропитание и заземление основных технических средств и систем от нештатных сетей электропитания и заземления;
- обрабатывать на АРМ информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к информационным ресурсам обработки информации;
- создавать или модифицировать программное обеспечение для АРМ или вносить изменения в существующее программное обеспечение, приводящее к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы АИС МФЦ и др. информационных систем, а равно использование либо распространение таких программ или машинных носителей с такими программами;
- отключать (блокировать), тиражировать, распространять (передавать) и модифицировать используемые в составе АИС МФЦ и др. информационных систем средства защиты информации;
- допускать к результатам решения задач (в том числе промежуточным) лиц, не имеющих к ним прямого отношения;
- пытаться работать от имени других пользователей;
- уничтожать, копировать или производить какие-либо другие действия над документами, программами, файлами, базами данных других пользователей без их разрешения;
- использовать для обработки и хранения защищаемой информации неучтенные установленным порядком машинные носители информации (CD и DVD диски, флеш накопители, съёмные / внешние жёсткие диски, дискеты и т.п.);
- хранить на учтенных носителях информации программы и данные, не относящиеся к рабочей информации;
- хранить носители с конфиденциальной информацией вблизи сильных источников электромагнитных излучений и прямых солнечных лучей;
- работать на средствах АИС МФЦ и др. информационных систем при обнаружении компьютерных вирусов или каких-либо неисправностей;
- осуществлять попытки НСД к конфиденциальной информации, в том числе персональным данным в АИС МФЦ и в др. информационных системах, в частности:
- производить подбор пароля другого пользователя;
- превышать свои полномочия при работе на АРМ;
- проводить работы по исследованию обнаруженных компьютерных вирусов;
- привлекать посторонних лиц для производства ремонта ОТСС без согласования со специалистом по защите информации;
- производить иные действия, ограничения, на исполнение которых предусмотрены требованиями нормативных актов.

Пользователь имеет право:

- доступа к аппаратным и программным средствам АИС МФЦ и др. информационных систем, необходимым для исполнения его должностных обязанностей;
- доступа к информационным ресурсам в соответствии с таблицей разграничения доступа (матрицей доступа) АИС МФЦ и др. информационным системам. Для каждой категории пользователей любой ресурс имеет свои значения атрибутов управления доступом, используемые при определении прав доступа пользователя к ресурсу;
- обращаться к Администратору по вопросам защиты информации;
- обращаться к Администратору с просьбой об оказании технической и методической помощи по обеспечению безопасности обрабатываемой в АИС МФЦ и др. информационных системах информации.

Пользователь несет ответственность:

- за несоблюдение действующей инструкции, приказов и распоряжений в области защиты персональных данных;
- за разглашение защищаемой информации, ставшей ему известной в ходе исполнения своих должностных обязанностей;
- за нарушение правил внутреннего трудового распорядка, трудовой дисциплины, правил техники безопасности, приведшей к утечке персональных данных заявителей;
- за правонарушения, совершенные в процессе осуществления своей деятельности в пределах, определенным действующим административным, уголовным и гражданским законодательством Российской Федерации.
- за причинение материального ущерба в пределах, определенных действующим трудовым и гражданским законодательством Российской Федерации.

ПРИЛОЖЕНИЕ № 17
УТВЕРЖДЕНО
Приказом ТОГКУ «МФЦ»
от 26.06.02015г. № 31

Парольная политика

Тамбовского областного государственного казенного учреждения «Многофункциональный центр предоставления государственных и муниципальных услуг»

Парольная зашита ИС обеспечивается в соответствии с требованиями руководящих документов федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации.

Настоящая политика регламентирует организационно-техническое обеспечение процессов формирования, использования, смены, хранения и прекращения действия паролей (удаления учетных записей пользователей) в ИС , а также процесса контроля действий пользователей и обслуживающего персонала системы при работе с паролями.

Общие положения

Тамбовское областное государственное казенное учреждение «Многофункциональный центр предоставления государственных и муниципальных услуг» производит обработку персональных данных в соответствии с положением об обработке персональных данных в учреждении, утвержденным приказом директора ТОГКУ «МФЦ» от 26.06.2015 № 31 " Об утверждении документов по организации работ по защите персональных данных в ТОГКУ «МФЦ».

Основные понятия и определения

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

Информационная система персональных данных (ИСПДн) - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

Автоматизированная система (АС) - система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций;

Автоматизированная обработка персональных данных -обработка персональных данных с помощью средств вычислительной техники;

Администратор информационной безопасности (администратор) — работник ТОГКУ «МФЦ», назначенный приказом и отвечающий за обеспечение информационной безопасности;

Пользователь - работник ТОГКУ «МФЦ», назначенный приказом и отвечающий за обработку ПДн в ИСПДн.

Методы взлома паролей

К одному из наиболее распространенных методов атаки на любую ИС относится взлом паролей пользователей, которые проходят проверку подлинности для того, чтобы можно было получить доступ к внутренней сети. Соответственно, если злоумышленник получит доступ к учетной записи пользователя, у него будет возможность получить доступ к внутренним документам учреждения и к прочей защищенной информации. Помимо учетных записей пользователей для доступа к внутренней сети, также часто злоумышленники стараются

взламывать аккаунты электронной почты, социальных сетей, блогов и прочего. Поэтому пользователям следует строго соблюдать меры по парольной защите.

1. Логическое угадывание.

Этот метод является самым простым, и начинают обычно именно с логического угадывания пароля. Например, злоумышленник может попробовать угадать пароль пользователей, зная имя, фамилию и его год рождения, а его пароль состоит из «Фамилия + год рождения» или логин, указанный в обратном порядке, то такой пароль будет взломан через несколько минут.

2.Перебор паролей по словарю.

Так как часто в качестве паролей используют одно слово, например название вулкана или другое «простое» слово и, максимум, добавляют к такому паролю одну цифру, злоумышленники могут взломать пароль, используя заранее отобранные пароли, которые загружаются из специальных словарей. В такие словари обычно включаются слова из разных языков, которые могут использовать неопытные или безразличные к своей безопасности пользователи. Подбор пароля, используя данный метод, обычно не занимает много времени и злоумышленник сможет получить доступ к учетной записи пользователя буквально через несколько часов.

Другим методом, связанным с перебором по словарю, называется перебор по таблице хешированных паролей. Этот метод используется тогда, когда злоумышленник смог определить хеши паролей и ему остается лишь найти в базе данных пароль, который будет полностью соответствовать данному хешу.

3. Метод грубой силы.

Метод грубой силы или полный (прямой) перебор отличается от предыдущего метода тем, что при подборе пароля используется не определённый словарь, согласно которому можно подобрать простой пароль, а большое количество любых возможных комбинаций. В этом случае, все зависит лишь от сложности пароля и количества символов. В следующей таблице, можно приблизительно оценить сложность создаваемых паролей, если учесть что в паролях будут только лишь буквы одного регистра с цифрами и скорость перебора составляет 100000 паролей за одну секунду:

Количество знаков	Количество вариантов	Время перебора
1	36	менее секунды
2	1296	менее секунды
3	46 656	менее секунды
4	1 679 616	17 секунд
5	60 466 176	10 минут
6	2 176 782 336	6 часов
7	78 364 164 096	9 дней
8	2,821 109 9? 1012	11 месяцев
9	1,015 599 5?1014	32 года
10	3,656 158 4?1015	1 162 года

11	1,316 217 0?1017	41 823 года
12	4,738 381 3?1018	1 505 615 лет

Соответственно, более-менее стойким паролем можно считать пароль, длина которого будет состоять не менее чем из восьми символов.

4.Использование человеческого фактора.

Несмотря на то, что при использовании человеческого фактора не применяется какая либо технология, этот метод в большинстве случаев считается самым действенным и иногда даже самым быстрым, так как в этом случае злоумышленники получают пароли незаконным методом от самих пользователей, причем, последние об этом могут даже не подозревать. Прежде всего, при использовании этого метода получения пользовательских паролей злоумышленник обычно узнает имена служащих организации, которые он может, как знать изначально, так и найти на том же, скажем, веб-сайте компании, а уже после этого, согласно продуманному заранее сценарию злоумышленник может получить от пользователей практически любые данные.

Методов получения пользовательских паролей, используя человеческий фактор, очень много.

Основные способы следующие:

Фишинг. Является довольно распространенным методом получения от пользователей необходимой информации. Сама атака происходит следующим образом: пользователю на почтовый ящик приходит письмо, в котором пользователю предлагают, перейдя по предоставленной ссылке, в целях обеспечения безопасности сменить на сайте свой пароль. На самом деле, такая ссылка ведет на сайт хакера со страницей, которая очень похожа на страницу официального сайта и при попытке смены своего пароля, пароль будет отправлен злоумышленнику;

Заражение компьютеров средствами троянских коней». «Троянским конем» называется вредоносная программа, которая распространяется злоумышленниками, при помощи которой он может получить доступ данным, в зависимости от того, какую он поставил перед собой задачу. В свою очередь, пользовательские пароли не являются исключениями;

Кви про кво. Данный метод обозначает недоразумение, возникшее в результате того, что одно лицо, вещь или понятие принято за другое. В случае с хищением паролей, этот способ подразумевает звонок злоумышленников. Злоумышленник может представиться техническим специалистом и узнать о уязвимостях, которые могут быть в организации и воспользоваться ими. Или же просто узнать пользовательский пароль по телефону;

Претекстинг. Этот способ самый простой. Используя данный метод хищения пароля, злоумышленником выполняются действия, отработанные по заранее составленному сценарию. Он может начать общаться с пользователем на каком- то веб-сайте, средствами переписки по электронной почте и т.д. По вполне понятным причинам, данный метод может занять значительно больше времени, чем все указанные раньше.

Правила формирования паролей

Минимальные требования к длине, сложности и периоду действия пароля:

Пароль не должен содержать имя учетной записи пользователя или какую- либо его часть или включать в себя легко вычисляемые сочетания символов (имена, фамилии и т.д.), а также общепринятые сокращения (EAT\, 1TE1. и т.п.);

Пароль должен состоять не менее чем из 8 (восьми) символов;

В пароле должны присутствовать символы:

1. прописные буквы английского алфавита от A до Z;
2. строчные буквы английского алфавита от a до z;

3. десятичные цифры (от 0 до 9);

4. неалфавитные символы (например, !, $, #, %)

В целях обеспечения информационной безопасности (далее - администратор) и противодействия попыткам подбора, символы вводимого пароля не должны отображаться на экране в явном виде.

Пароли для пользовательских учетных записей должны соответствовать требованиям:

Формирование и выдачу паролей для работы с АС рекомендуется осуществлять администратором информационной безопасности;

Максимальный срок действия пароля должен быть ограничен и должен меняться не реже 1 раза в шесть месяцев.

Учетная запись пользователя, не сменившего вовремя пароль, должна автоматически блокироваться. Блокировка должна сниматься «вручную» администратором или специалистом службы технической поддержки с одновременной сменой пароля пользователя.

Новый пароль пользователя не должен совпадать как минимум с тремя предыдущими паролями.

Пароль не должен совпадать с именем учетной записи пользователя.

В журнал учета работ АС должно заноситься сообщение о многократно не удавшихся попытках авторизации пользователя.

Пароли пользователей на доступ к различным ресурсам должны быть разными.

Недопустимо хранение пароля в открытом виде на любых видах носителей информации.

Количество попыток ввода паролей не должна превышать трех раз.

Пароли для административных учетных записей должны соответствовать требованиям:

Максимальный срок действия пароля должен быть ограничен шестью месяцами.

Новый пароль администратора не должен совпадать как минимум с предыдущим паролем.

Пароль не должен совпадать с именем учетной записи администратора.

В случае не удавшейся попытки авторизации в журнал учета работ АС должно заноситься соответствующее сообщение. При многократных не удавшихся попытках авторизации должно генерироваться предупреждение системы обнаружения вторжений. Количество попыток ввода паролей не должна превышать трех раз.

Пароли на доступ к различным ресурсам должны различаться, не допускается использование универсальных паролей для административных учетных записей.

Криптографические ключи, используемые для аутентификации, должны быть защищены парольными фразами. Требования к стойкости парольных фраз криптографических ключей идентичны требованиям к паролям административных учетных записей.

Порядок ввода пароля

Непосредственно перед вводом пароля для предотвращения возможности неверного ввода пользователь должен убедиться в правильности языка ввода (раскладки клавиатуры), проверить, не является ли активной клавиша CAPSLOCK (если это необходимо), а также проконтролировать расположение клавиатуры (клавиатура должна располагаться таким образом, что бы исключить возможность увидеть набираемый текст посторонними).

При вводе пароля пользователю запрещается проговаривать вслух вводимые символы.

Хранение паролей

Недопустимо хранение пароля в открытом виде на любых видах носителей информации.

Журнал выдачи паролей пользователю должен храниться в надежно запираемом сейфе администратора.

Порядок выдачи (смены) пароля

Новый пароль должен выдаваться пользователю только после обязательной

регистрации в журнале выдачи паролей (Приложение №1 к Политике) .

В случае выдачи пароля на бумажном носителе (для первоначального запоминания) в журнале выдачи паролей указывается регистрационный номер носителя, при этом на самом носителе указываются только регистрационный номер и пароль (обезличивание пароля).

При возникновении служебной необходимости в срочном доступе к АС временно отсутствующего пользователя разрешается произвести смену пароля пользователя администратором или лицом, курирующим вопросы организации защиты информационных систем ПДн, при этом должен быть составлен акт о смене пароля.

В случае возникновения необходимости в смене пароля в виду компрометации пользователь должен немедленно известить администратора или лицо, курирующее вопросы организации защиты информационных систем ПДн.

Внеплановая смена пароля или удаление учетной записи пользователя в случае прекращения его полномочий (увольнение, перевод в другое структурное подразделение и т.п.) должна производиться непосредственно после окончания последнего сеанса работы данного пользователя.

Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, перевод в другое структурное подразделение и другие обстоятельства) администратора.

Сотрудники Технической поддержки АС в течение суток после смены паролей должны передать на хранение их новые значения вместе с именами соответствующих учетных записей в запечатанном конверте администратору или лицу, курирующему вопросы организации защиты информационных систем ПДн. При получении конверта с новыми паролями старые пароли уничтожается с составлением соответствующего акта.

Учетная запись пользователя, ушедшего в длительный отпуск (более 60 дней), должна блокироваться администратором с момента получения письменного уведомления от кадрового подразделения.

Удаление учетных записей пользователей, уволенных или переведенных в другое структурное подразделение должно производиться администратором немедленно с момента получения письменного уведомления из кадрового подразделения.

Кадровое подразделение должно известить администратора о состоявшемся приказе в течение 24 часов после увольнения, перевода работника в другое структурное подразделение.

Порядок уничтожения пароля

После прекращения действия бумажные носители возвращаются администратору о чем последний расписывается в журнале выдачи паролей и проставляет дату возврата. Учтенные бумажные носители, после установленного срока хранения уничтожаются комиссией по акту. Акт утверждается директором учреждения.

Ответственность при организации парольной защиты

Пользователю запрещается разглашать или передавать свой пароль для ввода другим лицам.

Администратору запрещается разглашать все известные ему имена учетных записей пользователей и их пароли или передавать журнал выдачи паролей другому работнику.

За разглашение парольной информации, работник привлекается к ответственности в соответствии с действующим законодательством Российской Федерации.

Повседневный контроль действий пользователей АС при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на администратора, периодический контроль возлагается на лицо, курирующее вопросы организации защиты информационных систем персональных данных.

Работники ТОГКУ «МФЦ» должны быть ознакомлены с данной политикой под роспись.

Правила парольной защиты

1. Не используйте один и тот же пароль для доступа к учётным записям "User №" и к другим ресурсам (например, доступ в интернет, системам электронной коммерции и т. д.). По возможности не используйте один и тот же пароль для доступа к различным ресурсам внутри учреждения. Например, используйте один пароль для прикладных программ и другой для администрирования ресурсов.

2. Не сообщайте ваш пароль никому, даже вашим коллегам. Все пароли являются конфиденциальной информацией.

3. Не сообщайте никому свой пароль по телефону.

4. Не отправляйте свой пароль по электронной почте.

5. Не говорите о своём пароле рядом с посторонними.

6. Не упоминайте о содержимом пароля (например, "мой день рождения").

7. Не указывайте свой пароль в анкетах или опросниках.

8. Не сообщайте свой пароль членам своей семьи.

9. Не сообщайте свой пароль сослуживцам перед уходом в отпуск.

10. Не записывайте пароль и не храните его на рабочем месте.

11. Не храните пароль в файле на компьютере, включая переносной, без шифрования.

12. Не используйте функцию "Запомнить пароль" в приложениях.

Если кто-либо требует сообщить ваш пароль, сошлитесь на этот документ или попросите позвонить начальнику информационно-технологического отдела.

Если вы считаете, что учётная запись или пароль скомпрометированы, сообщите об этом начальнику информационно-технологического отдела и смените все пароли.

Доведение парольной политики

Доведение парольной политики целесообразно провести в форме инструктажа с последующей сдачей работниками мини-зачета по изложенным темам.

Во время инструктажа необходимо сконцентрироваться на том, что должен сделать сам работник для реализации политики информационной безопасности, а также на том, что ожидает тех работников, которые в этой реализации не пожелают принять участие.

«Парольные» инструктажи нужно периодически повторять, опять-таки с проведением зачетов после них. Достаточная периодичность - раз в полгода.

Приложение №1
к Парольной политике

Типовая форма журнала учета и выдачи (смены) паролей

№ п.п.	Регистрационный номер	Кто получил (Ф.И.О)	Кто выдал (Ф.И.О)	Дата выдачи
1	2	3	4	5

Место хранения, № печати	Кто принял (ФИО, подпись)	Подпись администратора безопасности	Дата сдачи	№ акта об уничтожении
6	7	8	9	10