

Приложение 1

к приказу ОГБУ «МФЦ»

от _____ № _____

Положение
по обработке и защите персональных данных
при их обработке в информационных системах
персональных данных в ОГБУ «МФЦ»

г. Биробиджан, 2016

Оглавление

1. Общие положения	3
2. Цели и задачи обработки ПДн	4
3. Персональные данные, обрабатываемые в ИСПДн	5
4. Доступ к ПДн	5
5. Основные требования по защите ПДн	6
6. Согласие на обработку ПДн	8
7. Права субъекта в отношении ПДн, обрабатываемых оператором	8
8. Права и обязанности оператора ИСПДн	9
9. Порядок обработки и защиты ПДн	12
10. Правила осуществления внутреннего контроля соответствия обработки ПДн	16
11. Работа с обезличенными данными в случае обезличивания ПДн	17
12. Особенности управления ПДн сотрудников Оператора	17
13. Ответственность за нарушение настоящего положения	17

1. Общие положения

1.1. Настоящее Положение разработано в соответствии с Федеральным законом от 27.07.2006 N 152-ФЗ «О персональных данных» («Персональные данные» далее по тексту - ПДн) и нормативно-методическими документами исполнительных органов государственной власти по вопросам безопасности ПДн при их обработке в информационных системах ПДн (далее — ИСПДн).

1.2. В настоящем Положении используются следующие термины:

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

обработка ПДн - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с ПДн, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн;

автоматизированная обработка ПДн - обработка ПДн с помощью средств вычислительной техники;

распространение ПДн - действия, направленные на раскрытие ПДн неопределенному кругу лиц;

предоставление ПДн - действия, направленные на раскрытие ПДн определенному лицу или определенному кругу лиц;

блокирование ПДн - временное прекращение обработки ПДн (за исключением случаев, если обработка необходима для уточнения ПДн);

уничтожение ПДн - действия, в результате которых становится невозможным восстановить содержание ПДн в ИСПДн и /или в результате которых уничтожаются материальные носители ПДн;

обезличивание ПДн - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность ПДн конкретному субъекту ПДн;

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

трансграничная передача ПДн - передача ПДн на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

- 1.3. Настоящее Положение определяет порядок и условия обработки ПДн в ОГБУ «Многофункциональный центр предоставления государственных и муниципальных услуг в Еврейской автономной области» (далее по тексту - Оператор), включая порядок передачи ПДн третьим лицам, особенности автоматизированной и неавтоматизированной обработки ПДн, порядок доступа к ПДн, систему защиты ПДн, порядок организации внутреннего контроля и ответственность за нарушения при обработке ПДн, иные вопросы.
- 1.4. Действие настоящего Положения распространяется на все процессы по сбору, систематизации, накоплению, хранению, уточнению, использованию, распространению (в том числе передаче), обезличиванию, блокированию, уничтожению ПДн, осуществляемых с использованием средств автоматизации и без их использования.
- 1.5. Настоящее Положение вступает в силу с момента его утверждения Директором Оператора и действует бессрочно, до замены его новым Положением.
- 1.6. Все изменения в Положение вносятся приказом.
- 1.7. Все работники Оператора должны быть ознакомлены с настоящим Положением под роспись.

2. Цели и задачи обработки ПДн

- 2.1. Обработка ПДн должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка ПДн, несовместимая с целями сбора ПДн.
- 2.2. Не допускается объединение баз данных, содержащих ПДн, обработка которых осуществляется в целях, несовместимых между собой.
- 2.3. Обработке подлежат только ПДн, которые отвечают целям их обработки.
- 2.4. Содержание и объем, обрабатываемых ПДн должны соответствовать заявленным целям обработки. Обрабатываемые ПДн не должны быть избыточными по отношению к заявленным целям их обработки.
- 2.5. Обработка ПДн сотрудников Оператора может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности сотрудников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества Оператора.
- 2.6. Основными целями обработки ПДн является:
 - 1) Реализация полномочий в области предоставления государственных и муниципальных услуг населению в соответствии с действующими соглашениями.

- 2) Организации делопроизводства по вопросам обращения граждан.
- 3) Оформления трудовых отношений: формирование и хранение документации по личному составу сотрудников Оператора; автоматизированное ведение их учета;
- 4) Формирования и хранения документации по договорным отношениям для выполнения Оператором всех требований трудового и налогового законодательства.
- 5) Ведения воинского учета и бронирования сотрудников.

2.7. ИСПДн обеспечивает решение следующих задач:

- 1) Защита персональных данных;
- 2) Контроль использования персональных данных
- 3) Упрощение процедуры обработки персональных данных, сокращение времени на их обработку;
- 4) Обеспечение возможности обмена персональными данными с использованием информационных систем связи;

3. Персональные данные, обрабатываемые в ИСПДн

3.1. В ИСПДн обрабатываются ПДн следующих субъектов ПДн:

- 1) Сотрудники Оператора;
- 2) Кандидаты для приема на работу;
- 3) Физические лица, получатели услуг Учреждения, законные представители получателей услуг Учреждения, ПДн которых обрабатываются Оператором.
- 4) Физические лица, получатели мер социальной поддержки, законные представители получателей мер социальной поддержки, ПДн которых обрабатываются Оператором.
- 5) Физические лица, получатели консультаций, ПДн которых обрабатываются у Оператора.

3.2. Данный перечень может пересматриваться по мере необходимости.

3.3. Полные списки обрабатываемых ПДн формируются в перечне ПДн, подлежащих защите в ИСПДн Оператора, утверждаемом Руководителем Учреждения.

4. Доступ к ПДн

4.1. Сотрудники Оператора, которые в силу выполняемых служебных обязанностей постоянно работают с ПДн, получают допуск к необходимым категориям ПДн на срок выполнения ими соответствующих должностных обязанностей на основании перечня

должностей Учреждения, допущенных к работе с ПДн, который утверждается Руководителем Оператора. Перечень составлен на основе Концепции информационной безопасности и Политики информационной безопасности.

- 4.2. Оператором установлен разрешительный порядок доступа к ПДн. Сотрудникам Оператора предоставляется доступ к работе с ПДн исключительно в пределах и объеме, необходимых для выполнения ими своих должностных обязанностей на основании решения Руководителя.
- 4.3. Временный или разовый допуск к работе с ПДн в связи со служебной необходимостью может быть получен сотрудником Оператора по согласованию Руководителя.
- 4.4. Доступ к ПДн третьих лиц, не являющихся сотрудниками Оператора без согласия субъекта ПДн, запрещен, за исключением доступа сотрудников органов исполнительной власти, осуществляемого в рамках мероприятий по контролю и надзору за исполнением законодательства, реализации функций и полномочий соответствующих органов государственной власти. Предоставление информации по запросу или требованию органа государственной власти осуществляется с ведома Руководителя Оператора.
- 4.5. В случае если сотруднику сторонней организации необходим доступ к ПДн Оператора, то необходимо, чтобы в договоре со сторонней организацией были прописаны условия конфиденциальности ПДн и обязанность сторонней организации и ее сотрудников по соблюдению требований текущего законодательства в области защиты ПДн. Кроме того, в случае доступа к ПДн лиц, не являющихся сотрудниками Оператора, должно быть получено согласие субъектов ПДн на предоставление их ПДн третьим лицам. Указанное согласие не требуется, если ПДн предоставляются в целях исполнения гражданско-правового договора, заключенного Оператором с субъектом ПД.
- 4.6. Доступ сотрудника Оператора к ПДн прекращается с даты, прекращения трудовых отношений, либо даты изменения должностных обязанностей сотрудника и/или исключения сотрудника из списка лиц, имеющих право доступа к ПДн. В случае увольнения все носители, содержащие ПДн, которые в соответствии с должностными обязанностями находились в распоряжении работника во время работы, должны быть переданы соответствующему должностному лицу.

5. Основные требования по защите ПДн

5.1. При обработке ПДн в информационной системе должно быть обеспечено:

- 1) проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и/или передачу их лицам, не имеющим права доступа к такой информации;

- 2) формирование и проведение единой политики в области обеспечения информационной безопасности;
 - 3) своевременное обнаружение фактов несанкционированного доступа к ПДн;
 - 4) недопущение воздействия на технические средства автоматизированной обработки ПДн, в результате которого может быть нарушено их функционирование;
 - 5) возможность восстановления ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
 - 6) постоянный контроль над обеспечением уровня защищенности ПДн.
- 5.2. Оператор обязан принимать необходимые правовые, организационные, технические и другие меры для обеспечения безопасности ПДн.
- 5.3. Для разработки требований по обеспечению безопасности и внедрения системы обеспечения безопасности ПДн Оператором должна быть разработана «Модель угроз безопасности ПДн при их обработке в ИСПДн» на основе нормативно-методического документа ФСТЭК России «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных».
- 5.4. Оператором в соответствии Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и Приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» должна быть осуществлена классификация ИСПДн Оператора и определены уровни защищенности ПДн, обрабатываемых Оператором.
- 5.6. Оператором на основании Акта классификации ИСПДн и в соответствии с нормативно-методическим документом ФСТЭК России «Состав мер защиты информации и их базовые наборы для соответствующего класса защищенности информационной системы» должна быть разработан и внедрен комплекс мер по защите и обеспечению безопасности ПДн («План мероприятий по обеспечению безопасности ПДн»).
- 5.7. Оператором используются технические средства и программное оборудование для обработки и защиты ПДн. Также ведется журнал учета средств защиты ПДн.
- 5.8. Оператором ведется журнал учета и хранения съемных носителей информации.
- 5.9. Вышеуказанные технические средства ИСПДн размещаются в офисах и помещениях Оператора.
- 5.10. Все лица, допущенные к работе с ПДн, а также связанные с эксплуатацией и техническим сопровождением ИСПДн должны быть под роспись ознакомлены с

требованиями настоящего Положения, а также должны подписать «Обязательство о неразглашении конфиденциальной информации (служебной тайны, персональных данных), не содержащих сведений, составляющих государственную тайну».

5.11. Оператором организован процесс обучения использования средств защиты ПДн, эксплуатируемых Оператором. Обучение по данному направлению рекомендовано лицам, имеющим постоянный доступ к ПДн, и лицам, эксплуатирующим технические и программные средства ИСПДн и средств защиты ИСПДн. В обязательном порядке обучение должны проходить лица, ответственные за эксплуатацию средств защиты информации ИСПДн.

5.12. Сотрудники обязаны незамедлительно сообщать соответствующему должностному лицу Оператора об утрате или недостатке носителей информации, составляющей ПДн, а также о причинах и условиях возможной утечки ПДн. В случае попытки посторонних лиц получить от сотрудника ПДн, обрабатываемых Оператором незамедлительно известить об этом соответствующее должностное лицо Оператора.

6. Согласие на обработку ПДн

6.1. Перед началом любого рода обработки ПДн субъекта, необходимо получение письменного согласия на обработку ПДн, если иное не предусмотрено законодательством Российской Федерации.

6.2. Субъект ПДн принимает решение о предоставлении своих ПДн и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку ПДн должно быть конкретным, информированным и сознательным. Согласие на обработку ПДн может быть дано субъектом ПДн или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено законодательством РФ. В случае получения согласия на обработку ПДн от представителя субъекта ПДн полномочия данного представителя на дачу согласия от имени субъекта ПДн проверяются Оператором.

6.3. Получение письменного согласия на обработку ПДн осуществляется сотрудником Оператора, при получении ПДн от субъекта ПДн, путем оформления письменного согласия по форме, установленной у Оператора ИСПДн.

7. Права субъекта в отношении ПДн, обрабатываемых оператором

7.1. Субъект ПДн имеет право:

1) На получение информации от Оператора, касающейся обработки его ПДн. Сведения должны быть предоставлены субъекту ПДн Оператором в доступной форме, и в них не должны содержаться ПДн, относящиеся к другим субъектам ПДн, за исключением случаев, если имеются законные основания для раскрытия таких ПДн. Перечень сведений и порядок получения сведений предусмотрен действующим законодательством РФ;

2) Требовать от Оператора 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, а также принимать предусмотренные законодательством РФ меры по защите своих прав; *(ч. 1 ст. 14 закона от 27.07.2006 N 152-ФЗ «О персональных данных»)*

3) На условие письменного согласия при принятии на основании исключительно автоматизированной обработки ПДн решений Оператора, порождающих юридические последствия в отношении субъекта ПДн или иным образом затрагивающих его права и законные интересы; *(ч.2. ст.16 закона от 27.07.2006 N 152-ФЗ «О персональных данных»)*

4) Заявлять возражения на решения Оператора на основании исключительно автоматизированной обработки его ПДн и возможные юридические последствия такого решения; *(ч.3 ст.16 закона от 27.07.2006 N 152-ФЗ «О персональных данных»)*

5) Обжаловать действия или бездействие Оператора в уполномоченный орган по защите прав субъектов ПДн или в судебном порядке. *(ст. 17 закона от 27.07.2006 N 152-ФЗ «О персональных данных»)*

8. Права и обязанности оператора ИСПДн

8.1. Оператор ИСПДн вправе:

1) Поручить обработку ПДн другому лицу с согласия субъекта ПДн, 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. *(ч.3 ст.6 закона от 27.07.2006 N 152-ФЗ «О персональных данных»)*

2) В случае отзыва субъектом ПДн согласия на обработку ПДн, продолжить обработку ПДн без согласия субъекта ПДн при наличии оснований, указанных в законодательстве РФ. *(ч.2 ст.9 закона от 27.07.2006 N 152-ФЗ «О персональных данных»)*

3) Отказать субъекту ПДн в выполнении повторного запроса сведений, не соответствующего условиям, предусмотренным законодательством РФ. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на операторе. *(ч.6 ст.14 закона от 27.07.2006 N 152-ФЗ «О персональных данных»)*

4) Самостоятельно определять состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей Оператора ИСПДн, предусмотренных законодательством РФ. *(ч.1 ст.18.1 закона от 27.07.2006 N 152-ФЗ «О персональных данных»)*

8.2. Оператор ИСПДн обязан:

- 1) Принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей Оператора ИСПДн, предусмотренных законодательством РФ.
- 2) Назначить лицо, ответственное за организацию обработки ПДн.
- 3) До начала обработки ПДн обязан уведомить уполномоченный орган по защите прав субъектов ПДн о своем намерении осуществлять обработку ПДн, за исключением случаев, предусмотренных законодательством РФ.
- 4) При получении доступа к ПДн не раскрывать третьим лицам и не распространять ПДн без согласия субъекта ПДн, если иное не предусмотрено законодательством РФ.
- 5) Представить доказательство получения согласия субъекта ПДн на обработку его ПДн или доказательство наличия законных оснований, обработки ПДн без согласия субъекта ПДн.
- 6) До начала осуществления трансграничной передачи ПДн убедиться в том, что иностранным государством, на территорию которого осуществляется передача ПДн, обеспечивается адекватная защита прав субъектов ПДн.
- 7) При сборе ПДн, предоставить субъекту ПДн по его просьбе информацию, предусмотренную законодательством РФ.
- 8) Если ПДн получены не от субъекта ПДн, Оператор, за исключением случаев, предусмотренных законодательством РФ, до начала обработки таких ПДн предоставить субъекту ПДн следующую информацию:
 - наименование и адрес оператора или его представителя;
 - цель обработки ПДн и ее правовое основание;
 - предполагаемые пользователи ПДн;
 - установленные настоящим Федеральным законом права субъекта ПДн;
 - источник получения ПДн.
- 9) Опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки ПДн, к сведениям о реализуемых требованиях к защите ПДн. Для осуществления сбора ПДн с использованием информационно-телекоммуникационных сетей, опубликовать в соответствующей информационно-телекоммуникационной сети документ, определяющий его политику в отношении обработки ПДн, и сведения о реализуемых требованиях к защите ПДн, а также обеспечить возможность доступа к указанному документу с использованием средств соответствующей информационно-телекоммуникационной сети.

10) Представить документы и локальные акты, предусмотренные законодательством РФ, и/или иным образом подтвердить принятие мер, необходимых и достаточных для обеспечения выполнения обязанностей Оператора ИСПДН, по запросу уполномоченного органа по защите прав субъектов ПДн.

11) При обработке 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.

12) Сообщить в порядке, предусмотренном законодательством РФ, субъекту ПДн или его представителю информацию безвозмездно о наличии ПДн, относящихся к соответствующему субъекту ПДн, а также предоставить возможность ознакомления с этими ПДн при обращении субъекта ПДн или его представителя либо в течение тридцати дней с даты получения запроса субъекта ПДн или его представителя.

13) В случае отказа в предоставлении информации о наличии ПДн о соответствующем субъекте ПДн или ПДн субъекту ПДн или его представителю при их обращении либо при получении запроса субъекта ПДн или его представителя оператор обязан дать в письменной форме мотивированный ответ, содержащий ссылку на положение законодательства РФ, являющееся основанием для такого отказа, в срок, не превышающий тридцати дней со дня обращения субъекта ПДн или его представителя либо с даты получения запроса субъекта ПДн или его представителя.

14) В срок, не превышающий семи рабочих дней со дня предоставления субъектом ПДн или его представителем сведений, подтверждающих, что ПДн являются неполными, неточными или неактуальными, внести в них необходимые изменения. В срок, не превышающий семи рабочих дней со дня представления субъектом ПДн или его представителем сведений, подтверждающих, что такие ПДн являются незаконно полученными или не являются необходимыми для заявленной цели обработки, оператор обязан уничтожить такие ПДн. Оператор обязан уведомить субъекта ПДн или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым ПДн этого субъекта были переданы.

15) Сообщить в уполномоченный орган по защите прав субъектов ПДн по запросу этого органа необходимую информацию в течение тридцати дней с даты получения такого запроса.

16) В случае выявления неправомерной обработки ПДн, осуществляемой Оператором или лицом, действующим по поручению Оператора, Оператор в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку ПДн или обеспечить прекращение неправомерной обработки ПДн лицом, действующим по поручению Оператора. В случае если

обеспечить правомерность обработки ПДн невозможно, Оператор в срок, не превышающий семи рабочих дней с даты выявления неправомерной обработки ПДн, обязан уничтожить такие ПДн или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении ПДн Оператор обязан уведомить субъекта ПДн или его представителя, а в случае, если обращение субъекта ПДн или его представителя либо запрос уполномоченного органа по защите прав субъектов ПДн были направлены уполномоченным органом по защите прав субъектов ПДн, также указанный орган.

17) В случае достижения цели обработки ПДн прекратить обработку ПДн или обеспечить ее прекращение (если обработка ПДн осуществляется другим лицом, действующим по поручению Оператора) и уничтожить ПДн или обеспечить их уничтожение (если обработка ПДн осуществляется другим лицом, действующим по поручению Оператора) в срок, не превышающий тридцати дней с даты достижения цели обработки ПДн, если Оператор не вправе осуществлять обработку ПДн без согласия субъекта ПДн на основаниях, предусмотренных законодательством РФ.

18) В случае отзыва субъектом ПДн согласия на обработку его ПДн, прекратить их обработку или обеспечить прекращение такой обработки (если обработка ПДн осуществляется другим лицом, действующим по поручению Оператора) и в случае, если сохранение ПДн более не требуется для целей обработки ПДн, уничтожить ПДн или обеспечить их уничтожение (если обработка ПДн осуществляется другим лицом, действующим по поручению Оператора) в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если Оператор не вправе осуществлять обработку ПДн без согласия субъекта ПДн на основаниях, предусмотренных законодательством РФ.

9. Порядок обработки и защиты ПДн

- 9.1. Обеспечение конфиденциальности ПДн, обрабатываемых Оператором, является обязательным требованием для всех лиц, которым ПДн стали известны.
- 9.2. Сотрудники Оператора, осуществляющие оформление документов, обязаны получать в установленных случаях согласие субъектов ПДн на обработку их ПДн.
- 9.3. В случае нарушения установленного порядка обработки ПДн сотрудники Оператора несут ответственность в соответствии с разделом 11 настоящего Положения.
- 9.4. ПДн субъектов на бумажных носителях, обрабатываемые Оператором, хранятся в отделах (у сотрудников), имеющих допуск к обработке соответствующих ПДн, а также в архиве Учреждения. Право допуска сотрудников к неавтоматизированной ИСПДн определяется приказом Руководителя. Носители ПДн не должны оставаться без присмотра. При покидании рабочего места, сотрудники, осуществляющие обработку ПДн должны, убирать носители в сейф, запираемый шкаф или иным образом

ограничивать несанкционированный доступ к носителям. При утере или порче ПДн осуществляется по возможности их восстановление.

9.5. Места хранения документов, содержащих ПДн:

9.5.1. ПДн клиентов Оператора (договоры, акты, соглашения, анкеты, копии паспортов, иные подобные документы, содержащие ПДн клиентов Оператора, носители информации (флеш-карты, CD-диски, и т.п.) хранятся в специально предусмотренных помещениях Оператора, размещаются на полках и запираются на ключ.

9.5.2. ПДн сотрудников Оператора — документы, носители информации (флеш-карты, CD-диски и т.п.) хранятся в сейфе учреждения и запираются на ключ.

9.6. Выдача документов для ознакомления осуществляется лицам, допущенным к соответствующей информации в целях исполнения должностных обязанностей, на срок, не более одного рабочего дня.

9.7. Иные носители информации (флеш-карты, CD-диски и т.п.) могут храниться в помещениях Оператора, размещаются на полках и запираются на ключ или же в сейфах или запираемых шкафах.

9.8. При работе с программными средствами автоматизированной системы Оператора, реализующей функции просмотра и редактирования ПДн, запрещается демонстрация экранных форм, содержащих такие данные, лицам, не имеющим соответствующего допуска.

9.9. При получении ПДн сотрудником Оператора, который в соответствии с должностными обязанностями получает ПДн от клиента, в обязательном порядке проводится проверка достоверности ПДн. Ввод ПДн, полученных Оператором, в информационную систему осуществляется сотрудниками имеющими доступ к соответствующим ПДн. Сотрудники, осуществляющие ввод информации, несут ответственность за достоверность и полноту введенной информации.

9.10. Особенности обработки ПДн, содержащихся на бумажных носителях, без использования средств автоматизации (при составлении документов не используется ПЭВМ) установлены в соответствии с Постановлением Правительства РФ от 15.09.2008 N 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

9.11. При неавтоматизированной обработке различных категорий ПДн должен использоваться отдельный материальный носитель для каждой категории ПДн.

9.12. При неавтоматизированной обработке ПДн на бумажных носителях:

1) Не допускается фиксация на одном бумажном носителе ПДн, цели обработки которых заведомо не совместимы;

2) ПДн должны обособляться от иной информации, в частности путем фиксации их на отдельных бумажных носителях, в специальных разделах или на полях форм (бланков);

9.13. Хранение ПДн должно осуществляться в форме, позволяющей определить субъекта ПДн, 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 ПДн.

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

9.15. 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 ПДн.

9.16. Уничтожение носителей, содержащих ПДн, осуществляется в следующем порядке:

1) ПДн на бумажных носителях уничтожаются путем использования шредеров (уничтожители документов), установленных в офисе Оператора, а также путем полного сжигания в печах, арендуемых Учреждением для целей уничтожения бумажных носителей.

2) ПДн, размещенные в памяти ПЭВМ уничтожаются путем удаления её из памяти ПЭВМ.

3) ПДн, размещенные на флеш-карте, CD-диске, ином носителе информации уничтожаются путем удаления файла с носителя, при необходимости путем нарушения работоспособности флеш-карты или CD-диска.

9.17. Уничтожение носителей контролируется комиссией, назначенной Руководителем Учреждения. Об уничтожении носителя комиссией составляется акт.

9.18. Помещения Оператора, в которых хранятся ПДн, согласно Перечня помещений для хранения ПДн, утвержденного в Учреждения, при отсутствии сотрудников в помещении, должны запираются и опечатываться, окна должны быть закрыты. В нерабочее время так же должна быть включена сигнализация (при наличии).

9.19. Сетевое оборудование, серверы следует располагать в местах, недоступных для посторонних лиц (в специальных помещениях, шкафах, коробах).

- 9.20. Уборка помещений и обслуживание технических средств ИСПДн должна осуществляться под контролем ответственных за данные помещения и технические средства лиц с соблюдением мер, исключающих несанкционированный доступ к ПДн, носителям информации, программным и техническим средствам обработки, передачи и защиты информации ИСПДн.
- 9.21. В обязанности администраторов ИСПДн входит управление учетными записями пользователей ИСПДн, поддержание штатной работы ИСПДн, обеспечение резервного копирования данных, а также установка и конфигурирование аппаратного и программного обеспечения ИСПДн, не связанного с обеспечением безопасности ПДн в ИСПДн. Также, в обязанности администраторов ИСПДн входит обеспечение соответствия порядка обработки и обеспечения безопасности ПДн в ИСПДн требованиям по конфиденциальности, целостности и доступности ПДн, предъявляемых к конкретной ИСПДн, и общим требованиям по безопасности ПДн, установленных федеральным законодательством.
- 9.22. В обязанности администраторов ИСПДн также входит установка, конфигурирование и администрирование аппаратных и программных средств защиты информации ИСПДн, учет и хранение машинных носителей ПДн, периодический аудит журналов безопасности и анализ защищенности ИСПДн, а также участие в служебных расследованиях фактов нарушения установленного порядка обработки и обеспечения безопасности ПДн.
- 9.23. Квалификационные требования и детальный перечень прав и обязанностей администраторов ИСПДн закрепляются в соответствующих должностных инструкциях, с которыми сотрудники, назначаемые на данные роли, должны быть ознакомлены под роспись.
- 9.24. Организация внутреннего контроля процесса обработки ПДн у Оператора осуществляется в целях изучения и оценки фактического состояния защищенности ПДн, своевременного реагирования на нарушения установленного порядка их обработки, а также в целях совершенствования этого порядка и обеспечения его соблюдения.
- 9.25. Мероприятия по осуществлению внутреннего контроля обработки и обеспечения безопасности ПДн направлены на решение следующих задач:
- 1) Обеспечение соблюдения сотрудниками Оператора требований настоящего Положения и нормативно-правовых актов, регулирующих обработку и защиту ПДн.
 - 2) Оценка компетентности персонала, задействованного в обработке ПДн.
 - 3) Обеспечение работоспособности технических средств ИСПДн и средств защиты ПДн, их соответствия требованиям уполномоченных органов исполнительной власти по вопросам безопасности ПДн.

4) Выявление нарушений установленного порядка обработки ПДн и своевременное предотвращение негативных последствий таких нарушений.

5) Принятие корректирующих мер, направленных на устранение выявленных нарушений, как в порядке обработки ПДн, так и в работе технических средств ИСПДн.

6) Разработка рекомендаций по совершенствованию порядка обработки и обеспечения безопасности ПДн по результатам контрольных мероприятий.

7) Осуществление внутреннего контроля за исполнением рекомендаций и указаний по устранению нарушений.

9.26. Результаты контрольных мероприятий оформляются актами и являются основанием для разработки рекомендаций по совершенствованию порядка обработки и обеспечения безопасности ПДн, по модернизации технических средств ИСПДн и средств защиты ПДн, по обучению и повышению компетентности персонала, задействованного в обработке ПДн.

10. Правила осуществления внутреннего контроля соответствия обработки ПДн

10.1. Проверки проводятся в Учреждении на основании ежегодного плана, утвержденного Руководителем Учреждения, или на основании поступившего в Учреждения письменного заявления о нарушениях правил обработки персональных данных (внеплановые проверки).

10.2. В плане по каждой проверке устанавливается объект внутреннего контроля, проверяемый период, срок проведения проверки, ответственные исполнители.

10.3. Проверки проводятся Комиссией, создаваемой приказом Руководителя Учреждения. В проведении проверки не может участвовать работник Учреждения, прямо или косвенно заинтересованный в ее результатах.

10.4. Основанием для проведения внеплановой проверки является поступившее в Учреждения письменное обращение субъекта персональных данных или его представителя о нарушении правил обработки персональных данных.

10.5. Проведение внеплановой проверки организуется в течение 5 рабочих дней с момента поступления обращения. Срок проведения проверки не может превышать 30 дней со дня принятия решения о ее проведении.

10.6. Члены Комиссии, получившие доступ к персональным данным субъектов персональных данных в ходе проведения проверки, обеспечивают конфиденциальность персональных данных субъектов персональных данных, не раскрывают третьим лицам и не распространяют персональные данные без согласия субъекта персональных данных.

10.7. По результатам каждой проверки Комиссией проводится заседание. Решения,

принятые на заседаниях Комиссии, оформляются протоколом. По существу поставленных в обращении (жалобе) вопросов Комиссия в течение 5 рабочих дней со дня окончания проверки дает письменный ответ заявителю.

11. Работа с обезличенными данными в случае обезличивания ПДн

11.1. Обезличивание персональных данных производится с целью устранения возможности определить принадлежность ПДн конкретному субъекту ПДн работниками Учреждения, входящими в «Перечень должностей работников ОГБУ «МФЦ», ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных, в случае обезличивания персональных данных» и в соответствии с законодательством РФ.

11.2. Обезличенные персональные данные конфиденциальны и не подлежат разглашению.

11.3. Обезличенные персональные данные могут обрабатываться с использованием и без использования средств автоматизации.

11.4. При обработке обезличенных персональных данных необходимо соблюдение раздела 9 настоящего Положения.

12. Особенности управления ПДн сотрудников Оператора

12.1. Управление ПДн сотрудников Оператора регламентируется «Положением об обработке персональных данных сотрудников ОГБУ «МФЦ», утвержденного Руководством Оператора.

13. Ответственность за нарушение настоящего положения

13.1. Руководство Оператора несет ответственность за необеспечение конфиденциальности ПДн и несоблюдение прав и свобод субъектов ПДн в отношении их ПДн, в том числе прав на неприкосновенность частной жизни, личную и семейную тайну.

13.2. Сотрудники Оператора несут персональную ответственность за несоблюдение требований по обработке и обеспечению безопасности ПДн, установленных настоящим Положением, в соответствии с законодательством Российской Федерации.

13.3. Сотрудник Оператора может быть привлечен к ответственности в случаях:

- 1) Умышленного или неосторожного раскрытия ПДн;
- 2) Утраты материальных носителей ПДн;
- 3) Нарушения требований настоящего Положения и других нормативных документов Оператора в части вопросов доступа и работы с ПДн.

13.4. В случаях нарушения установленного порядка обработки и обеспечения безопасности ПДн, несанкционированного доступа к ПДн, раскрытия ПДн и нанесения Оператору, его сотрудникам, клиентам и контрагентам материального или иного ущерба виновные лица несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность, в том числе:

- КоАП РФ, Статья 5.39. Отказ в предоставлении информации;
- КоАП РФ, Статья 13.11. Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных);
- КоАП РФ, Статья 13.12. Нарушение правил защиты информации;
- КоАП РФ, Статья 13.13. Незаконная деятельность в области защиты информации;
- КоАП РФ, Статья 13.14. Разглашение информации с ограниченным доступом;
- УК РФ, Статья 137. Нарушение неприкосновенности частной жизни;
- УК РФ, Статья 140. Отказ в предоставлении гражданину информации;
- УК РФ, Статья 272. Неправомерный доступ к компьютерной информации.