УТВЕРЖДАЮ

Директор МАУ «МФЦ»
Зимовниковского района
Ростовской области

Н.А.Белякова

«08» Декабря 2019 г.

ПОЛОЖЕНИЕ
об обработке персональных данных в МАУ «МФЦ» Зимовниковского района Ростовской области

1. Общие положения

1.1. Положение об обработке персональных данных в МАУ «МФЦ» Зимовниковского района Ростовской области (далее - Положение) разработано в соответствии с, частью 2 статьи 4 Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных" (далее - Федеральный закон "О персональных данных"), Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Постановлением Правительства Российской Федерации от 15 сентября 2008 г. N 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

1.2. Целью данного Положения является защита персональных данных от несанкционированного доступа, неправомерного их использования или утраты.

1.3. Персональные данные относятся к категории конфиденциальной информации. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении срока хранения, определенного действующим законодательством и нормативно-правовыми актами МАУ «МФЦ» Зимовниковского района Ростовской области (далее – Учреждение), если иное не определено законом.

1.4. Сбор персональных данных в Учреждении осуществляется с целью их последующей обработки в ИСПДн.

1.5. Настоящее Положение утверждается и вводится в действие приказом руководителя и является обязательным для исполнения всеми работниками, имеющими доступ к персональным данным.

2. Понятие и состав персональных данных

2.1. Персональные данные - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Оператор персональных данных — государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Субъект персональных данных - это физическое лицо, владелец персональных данных.

2.2. В состав персональных данных Учреждения входят:

- первичные учетные данные субъекта ПДн (ФИО);
- дополнительные сведения о субъекте ПДн:
  - паспортные данные,
  - данные о регистрации (по месту жительства, по месту пребывания),
  - дата и место рождения,
  - семейное положение,
  - номер телефона,
  - адрес электронной почты,
  - данные об изменениях должностного положения,
  - финансовые данные,
  - ИНН,
  - СНИЛС,
  - полис ОМС,
  - категории льготности (в том числе данные о группах инвалидности),
  - данные о количестве и датах предоставления услуг,

  социальный статус.

3. Обработка персональных данных в Учреждении

3.1. Под обработкой персональных данных понимается получение, хранение, комбинирование, передача или любое другое использование персональных данных.

3.2. В целях обеспечения прав и свобод человека и гражданина операторы при обработке персональных данных обязаны соблюдать следующие общие требования:

– обработка персональных данных может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия в трудоустройстве, обучении, продвижении по службе, оказании государственных услуг, обеспечения личной безопасности, контроля количества и качества выполняемой работы и обеспечения сохранности имущества;

– при определении объема и содержания обрабатываемых персональных данных, оператор должен руководствоваться Конституцией Российской Федерации и иными федеральными законами;

– получение персональных данных осуществляется от субъекта ПДн или из диссертационного совета;

– если персональные данные возможно получить только у третьей стороны, то лицо должно быть уведомлено об этом заранее и от него должно быть получено письменное согласие. Оператор должен сообщить лицу о целях, предполагаемых источниках и способах получения персональных данных, а так же о характере подлежащих получению персональных данных и последствиях отказа лица дать письменное согласие на их получение. Согласие субъекта персональных данных не требуется в случае, если обработка персональных данных ведется для осуществления и выполнения, возложенных законодательством Российской Федерации на Учреждение функций, полномочий и обязанностей, не предусматривающих получение согласия субъекта на обработку персональных данных;

– оператор не имеет права получать и обрабатывать персональные данные лиц о политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений данные о частной жизни (информация о жизнедеятельности в сфере семейных бытовых, личных отношений) могут быть получены и обработаны оператором только с письменного согласия лица;

– оператор не имеет право получать и обрабатывать персональные данные лица о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом.

3.3. Использование персональных данных возможно только в соответствии с целями, определившими их получение. Персональные данные не могут быть использованы в целях причинения имущественного и морального вреда гражданам, затруднения реализации прав и свобод граждан Российской Федерации. Ограничение прав граждан Российской Федерации на основе использования информации об их социальном происхождении, о расовой, национальной, языковой, религиозной и партийной принадлежности запрещено и карается в соответствии с законодательством.

3.4. Передача персональных данных возможна только с согласия лица или в случаях, прямо предусмотренных законодательством. При передаче персональных данных оператор должен соблюдать следующие требования:

– не сообщать персональные данные третьей стороне без письменного согласия лица, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью, а также в случаях, установленных федеральным законом;

– не сообщать персональные данные в коммерческих целях без письменного согласия лица;

– предупредить лиц, получающих персональные данные, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные, обязаны соблюдать режим конфиденциальности. Данное положение не распространяется на обмен персональными данными в порядке, установленном федеральными законами;

– разрешать доступ к персональным данным только специально уполномоченным лицам, определенным приказом по организации, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы для выполнения конкретных функций;

– передача персональных данных от держателя или его представителей внешнему потребителю может допускаться в минимальных объемах и только в целях выполнения задач, соответствующих объективной причине сбора этих данных;

– при передаче персональных данных потребителям (в том числе и в коммерческих целях) за пределы организации оператор не должен сообщать эти данные третьей стороне без письменного согласия лица, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью или в случаях, установленных федеральным законом.

3.5. Все меры конфиденциальности при сборе, обработке и хранении персональных данных распространяются как на бумажные, так и на электронные (автоматизированные) носители информации.

3.6. Не допускается отвечать на вопросы, связанные с передачей персональной информации по телефону или факсу.

3.7. Хранение персональных данных должно происходить в порядке, исключающем их утрату или их неправомерное использование.

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

4.1. 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.

4.2. При разработке и использовании типовых форм документов, необходимых для реализации возложенных на Учреждение 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 Учреждения, 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, 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.

4.3. 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.

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

5. Доступ к персональным данным

5.1. Право внутреннего доступа (доступ внутри организации) к персональным данным, имеют:

– сотрудники организации при выполнении ими своих служебных обязанностей;

– само лицо, носитель данных.

5.2. Право внешнего доступа к персональным данным имеют:

– надзорно-контрольные органы имеют доступ к информации только в сфере своей компетенции.

6. Защита персональных данных

Под угрозой или опасностью утраты персональных данных понимается единичное или комплексное, реальное или потенциальное, активное или пассивное проявление злоумышленных возможностей внешних или внутренних источников угрозы создавать неблагоприятные события, оказывать дестабилизирующее воздействие на защищаемую информацию.

6.1. Риск угрозы любым информационным ресурсам создают стихийные бедствия, экстремальные ситуации, террористические действия, аварии технических средств и линий связи, другие объективные обстоятельства, а также заинтересованные и незаинтересованные в возникновении угрозы лица.

6.2. Защита персональных данных представляет собой жестко регламентированный технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и, в конечном счете, обеспечивающий достаточно надежную безопасность информации в процессе управленческой и производственной деятельности компании.

6.3. Защита персональных данных от неправомерного их использования или утраты должна быть обеспечена оператором за счет его средств в порядке, установленном федеральным законом.

6.4. «Внутренняя защита». Основным виновником несанкционированного доступа к персональным данным является, как правило, персонал, работающий с документами и базами данных. Регламентация доступа персонала к конфиденциальным сведениям, документам и базам данных входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий между руководителями и специалистами организации. Для обеспечения внутренней защиты персональных данных необходимо соблюдать ряд мер:

– ограничение и регламентация состава работников, функциональные обязанности которых требуют конфиденциальных знаний;

– строгое избирательное и обоснованное распределение документов и информации между работниками;

– рациональное размещение рабочих мест работников, при котором исключалось бы бесконтрольное использование защищаемой информации;

– знание работником требований нормативно – методических документов по защите информации и сохранении тайны;

– наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;

– определение и регламентация состава работников, имеющих право доступа (входа) в помещение, в котором находится вычислительная техника;

– организация порядка уничтожения информации;

– своевременное выявление нарушения требований разрешительной системы доступа работниками подразделения;

– воспитательная и разъяснительная работа с сотрудниками подразделения по предупреждению утраты ценных сведений при работе с конфиденциальными документами;

6.5. «Внешняя защита». Как результат мер, принимаемых по защите конфиденциальной информации, создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лица, пытающегося совершить несанкционированный доступ и овладение информацией. Целью и результатом несанкционированного доступа к информационным ресурсам может быть не только овладение ценными сведениями и их использование, но и их видоизменение, уничтожение, внесение вируса, подмена, фальсификация содержания реквизитов документа и др. Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности Учреждения, посетители, работники других организационных структур. Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов в отделах, занимающихся обработкой персональных данных. Для обеспечения внешней защиты персональных данных необходимо соблюдать ряд мер:

– порядок приема, учета и контроля деятельности посетителей;

– пропускной режим организации;

– учет и порядок выдачи удостоверений;

– технические средства охраны, сигнализации;

– порядок охраны территории, зданий, помещений, транспортных средств;

– требования к защите информации при интервьюировании и собеседованиях.

6.6. Все лица, связанные с получением, обработкой и защитой персональных данных, обязаны подписать обязательство о неразглашении персональных данных.

6.7. По возможности персональные данные обезличиваются.

6.8. Кроме мер защиты персональных данных, установленных законодательством, оператор может вырабатывать совместные меры защиты персональных данных.

7. Права и обязанности

7.1. Закрепление прав лица, регламентирующих защиту его персональных данных, обеспечивает сохранность полной и точной информации о нем.

7.2. В целях защиты персональных данных, хранящихся у оператора, лицо имеет право:

– требовать исключения или исправления неверных или неполных персональных данных;

– на свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные;

– персональные данные оценочного характера дополнить заявлением, выражающим его собственную точку зрения;

– определять своих представителей для защиты своих персональных данных;

– на сохранение и защиту своей личной и семейной тайны.

8. Ответственность за разглашение конфиденциальной информации, связанной с персональными данными

8.1. Персональная ответственность – одно из главных требований к организации функционирования системы защиты персональной информации и обязательное условие обеспечения эффективности этой системы.

8.2. Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.

8.3. Руководитель, разрешающий доступ сотрудника к конфиденциальному документу, несет персональную ответственность за данное разрешение.

8.4. Каждый сотрудник организации, получающий для работы конфиденциальный документ, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

8.5. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

8.6. За неисполнение или ненадлежащее исполнение работником по его вине возложенных на него обязанностей по соблюдению установленного порядка работы со сведениями конфиденциального характера работодатель вправе применять предусмотренные Трудовым Кодексом дисциплинарные взыскания.

8.7. Должностные лица, в обязанность которых входит ведение персональных данных, обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом. Неправомерный отказ в предоставлении собранных в установленном порядке документов, либо несвоевременное предоставление таких документов или иной информации в случаях, предусмотренных законом, либо предоставление неполной или заведомо ложной информации – влечет наложение на должностных лиц административного штрафа в размере, определяемом Кодексом об административных правонарушениях.

8.8. В соответствии с Гражданским Кодексом лица, незаконными методами получившие информацию, составляющую служебную тайну, обязаны возместить причиненные убытки, причем такая же обязанность возлагается и на работников.

8.9. Уголовная ответственность за нарушение неприкосновенности частной жизни (в том числе незаконное собирание или распространение сведений о частной жизни лица, составляющего его личную или семейную тайну, без его согласия), неправомерный доступ к охраняемой законом компьютерной информации, неправомерный отказ в предоставлении собранных в установленном порядке документов и сведений (если эти деяния причинили вред правам и законным интересам граждан), совершенные лицом с использованием своего служебного положения наказывается штрафом, либо лишением права занимать определенные должности или заниматься определенной деятельностью, либо арестом в соответствии с УК РФ.

8.10. Неправомерность деятельности органов государственной власти и организаций по сбору и использованию персональных данных может быть установлена в судебном порядке.

Лист ознакомления

работников МАУ «МФЦ Зимовниковского района» с положением МАУ МФЦ Зимовниковского района от 03.12.2019г. «об обработке персональных данных в МАУ «МФЦ» Зимовниковского района Ростовской области»

Наименование должности	ФИО	Подпись	Дата
Директор	Белякова Наталья Андреевна		03.12.2019
Главный бухгалтер	Мальева Ольга Николаевна		03.12.19
Начальник информационно-аналитического отдела, системный администратор	Косман Антон Борисович		03.12.2019
Ведущий специалист информационно-аналитического отдела	Горбачева Анна Сергеевна		03 12 2019
Ведущий специалист информационно-аналитического отдела	Косман Ирина Валерьевна		03.12.2019
Начальник отдела консультирования, приема-выдачи документов	Винокурова Елена Владимировна		03.12.2019
Ведущий специалист отдела консультирования, приема-выдачи документов	Дьяченко Светлана Викторовна		03.12.2019
Ведущий специалист отдела консультирования, приема-выдачи документов	Денисова Лилия Васильевна		03.12.2019
Ведущий специалист отдела консультирования, приема-выдачи документов	Гайворонская Марина Георгиевна		3.12.2019
Ведущий специалист отдела консультирования, приема-выдачи документов	Грицай Екатерина Олеговна		03.12.2019
Ведущий специалист отдела консультирования, приема-выдачи документов	Просвирова Наталья Владимировна		03.12.2019
Ведущий специалист отдела консультирования, приема-выдачи документов	Керимов Руслан Фикрет оглы		03.12.2019
Ведущий специалист отдела консультирования, приема-выдачи документов	Тицкая Виктория Сергеевна		03.12.2019
Ведущий специалист отдела консультирования, приема-выдачи документов	Утянская Анастасия Павловна		03.12.19

Наименование должности	ФИО	Подпись	Дата
Ведущий специалист-консультант	Литвинов Андрей Николаевич		03.12.2019
Специалист ТОСП	Власенко Людмила Ивановна		03.12.2019
Специалист ТОСП	Землянская Татьяна Михайловна		03.12.2019
Специалист ТОСП	Кабан Галина Григорьевна		03.12.19
Специалист ТОСП	Моисеенко Алла Александровна		03.12.2019
Специалист ТОСП	Раева Наталья Юрьевна		03.12.2019
Специалист ТОСП	Фурсова Наталья Пантелеевна		03.12.2019
Вед. спец. отдела конс-я, приёма - выдачи документов	Меньшикова Маргарита Николаевна		15.07.2020
Специалист ТОСП	Самаева Светлана Назимовна		08.10.2020