Утверждена приказом МАУ ГОЩ «МФЦ городского округа Щёлково»

№ 01-04/47 от 21.05.2021

**ПОЛИТИКА**

**Муниципального автономного учреждения городского округа Щёлково «Многофункциональный центр предоставления государственных и муниципальных услуг городского округа Щёлково»**

**в отношении обработки и защиты персональных данных**

1. Общие положения
   1. Настоящая Политика Муниципального автономного учреждения городского округа Щёлково «Многофункциональный центр предоставления государственных и муниципальных услуг городского округа Щёлково» (далее соответственно - МФЦ, Политика) разработана в соответствии со ст. 18.1 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее - 152-ФЗ, Закон о ПДн) и является основополагающим внутренним регулятивным документом МФЦ, определяющим ключевые направления его деятельности в области обработки и защиты персональных данных (далее - ПДн).
   2. Политика разработана в целях реализации требований законодательства в области обработки и защиты ПДн и направлена на обеспечение защиты прав и свобод человека и гражданина при обработке его ПДн в МФЦ, в том числе защиты прав на неприкосновенность частной жизни, личной и семейной тайн.
   3. Основные понятия, используемые в Политике:
      1. Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).
      2. Оператор персональных данных (оператор) - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.
      3. Обработка персональных данных - любое действие (операция) или совокупность действий (операций) с персональными данными, совершаемых с использованием средств автоматизации или без их использования. Обработка персональных данных может включать в себя в том числе: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.
      4. Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники.
      5. Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц.
      6. Предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.
      7. Блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).
      8. Уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.
      9. Обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.
      10. Информационная система персональных данных (далее - ИСПДн) - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.
      11. Трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.
   4. Действие Политики распространяется на все персональные данные субъектов, обрабатываемые в информационных системах персональных данных МФЦ с применением средств автоматизации и без применения таких средств.
   5. К настоящей Политике должен иметь доступ любой субъект персональных данных.
2. Основания, цели обработки и состав персональных данных,  
   обрабатываемых в МФЦ
   1. Обработка ПДн в МФЦ осуществляется в связи с выполнением законодательно возложенных на МФЦ функций, определяемых:
      1. Федеральным законом от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг»;
      2. Постановлением Правительства Российской Федерации от 22 декабря 2012 г. № 1376 «Об утверждении Правил организации деятельности
      3. Постановлением Правительства Российской Федерации от 27 сентября 2011 г. № 797 «О взаимодействии между многофункциональными центрами предоставления государственных (муниципальных) услуг и федеральными органами исполнительной власти, органами государственных внебюджетных фондов, органами государственной власти субъектов Российской Федерации, органами местного самоуправления»;
      4. Распоряжением Мингосуправления МО от 21.07.2016 N 10-57/РВ "О региональном стандарте организации деятельности многофункциональных центров предоставления государственных и муниципальных услуг в Московской области"
      5. Иными нормативно-правовыми актами Российской Федерации и Московской области;
      6. Заключенными МФЦ соглашениями о взаимодействии с ведомствами и органами исполнительной власти;
      7. Локальными нормативными актами МФЦ.

2.2. В МФЦ обрабатываются персональные данные при наличии хотя бы одного из следующих условий:

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

- обработка персональных данных необходима для достижения целей, предусмотренных законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;

- обработка персональных данных необходима для исполнения полномочий МФЦ, предусмотренных Федеральным законом от 27 июля 2010 года N 210-ФЗ "Об организации предоставления государственных и муниципальных услуг", включая регистрацию субъекта персональных данных на едином портале государственных и муниципальных услуг и региональном портале государственных и муниципальных услуг Московской области;

- обработка персональных данных 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 персональных данных 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;

- осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с законодательством Российской Федерации.

* 1. Категории субъектов персональных данных, персональные данные которых обрабатываются в МФЦ:
     1. работники и бывшие работники МФЦ и их близкие родственники;
     2. кандидаты на замещение вакантных должностей в МФЦ и их близкие родственники;
     3. студенты, учащиеся образовательных учреждений, проходящие производственную практику в МФЦ и их близкие родственники;
     4. клиенты МФЦ, представители/работники клиентов и контрагентов по гражданско-правовым договорам, в том числе потенциальных, ПДн руководителей, членов коллегиальных исполнительных органов и представителей юридических лиц;
     5. физические лица, ПДн которых используются для осуществления пропускного режима в занимаемых МФЦ помещениях;
     6. лица, письменно обращающиеся в МФЦ по вопросам его деятельности;
     7. заявители, обращающиеся за получением государственных и муниципальных услуг в соответствии с Федеральным законом от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг»;
  2. МФЦ может предоставлять обрабатываемые им ПДн организациям, имеющим право на получение соответствующих ПДн, в строгом соответствии с требованиями действующего законодательства Российской Федерации.
  3. Трансграничная передача персональных данных на территорию иностранных государств МФЦ не осуществляется.

1. **Принципы обеспечения безопасности персональных данных**

3.1. Основной задачей обеспечения безопасности ПДн при их обработке в МФЦ является предотвращение несанкционированного доступа к ним третьих лиц, предупреждение преднамеренных программно­-технических и иных воздействий с целью хищения ПДн, разрушения (уничтожения) или искажения их в процессе обработки.

* 1. Для обеспечения безопасности ПДн МФЦ руководствуется следующими принципами:
     1. Законность: защита ПДн основывается на положениях нормативных правовых актов и методических документов уполномоченных государственных органов в области обработки и защиты ПДн;
     2. Системность: обработка ПДн осуществляется с учетом всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности ПДн;
     3. Комплексность: защита ПДн строится с использованием функциональных возможностей информационных технологий, реализованных в информационных системах, используемых в МФЦ;
     4. Непрерывность: защита ПДн обеспечивается на всех этапах их обработки и во всех режимах функционирования систем обработки ПДн, в том числе при проведении ремонтных и регламентных работ;
     5. Своевременность: меры, обеспечивающие надлежащий уровень безопасности ПДн, принимаются до начала их обработки;
     6. Преемственность и непрерывность совершенствования: модернизация и наращивание мер и средств защиты ПДн осуществляются на основании результатов анализа практики обработки ПДн в МФЦс учетом выявления новых способов и средств реализации угроз безопасности ПДн, отечественного и зарубежного опыта в сфере защиты информации;
     7. Персональная ответственность: ответственность за обеспечение безопасности ПДн возлагается на Работников в пределах их обязанностей, связанных с обработкой и защитой ПДн;
     8. Минимизация прав доступа: доступ к ПДн предоставляется Работникам только в объеме, необходимом для выполнения их должностных обязанностей;
     9. Гибкость: обеспечение выполнения функций защиты ПДн при изменении характеристик функционирования информационных систем, используемых в МФЦ, а также объема и состава обрабатываемых ПДн;
     10. Открытость алгоритмов и механизмов защиты: структура, технологии и алгоритмы функционирования систем защиты ПДн (далее - СЗПДн) не дают возможности преодоления имеющихся в МФЦ систем защиты возможными нарушителями безопасности ПДн;
     11. Научная обоснованность и техническая реализуемость: комплекс мер по защите ПДн определяется современным уровнем развития информационных технологий и средств защиты информации;
     12. Специализация и профессионализм: реализация мер по обеспечению безопасности ПДн и эксплуатация СЗПДн осуществляются Работниками, имеющими необходимые для этого квалификацию и опыт;
     13. Эффективность процедур отбора кадров и выбора контрагентов: кадровая политика МФЦ предусматривает тщательный подбор персонала и мотивацию Работников, позволяющую исключить или минимизировать возможность нарушения ими безопасности ПДн; минимизация вероятности возникновения угрозы безопасности ПДн, источники которых связаны с человеческим фактором, обеспечивается получением наиболее полной информации о контрагентах МФЦ до заключения договоров;
     14. Наблюдаемость и прозрачность: меры по обеспечению безопасности ПДн должны быть спланированы так, чтобы результаты их применения были явно наблюдаемы (прозрачны) и могли быть оценены лицами, осуществляющими контроль;
     15. Непрерывность контроля и оценки: устанавливаются процедуры постоянного контроля использования систем обработки и защиты ПДн, а результаты контроля регулярно анализируются

1. Доступ к обрабатываемым персональным данным
   1. Доступ к обрабатываемым в МФЦ ПДн имеют лица, в чьи должностные обязанности входит обработка соответствующих ПДн.
   2. Доступ Работников к обрабатываемым ПДн осуществляется в соответствии с их должностными обязанностями и требованиями внутренних регулятивных документов МФЦ.
   3. Допущенные к обработке ПДн Работники под роспись знакомятся с локальными нормативными актами МФЦ, устанавливающими порядок обработки ПДн, включая документы, устанавливающие права и обязанности конкретных Работников.
   4. Порядок доступа субъекта ПДн к его ПДн, обрабатываемым МФЦ, определяется в соответствии с законодательством и внутренними регулятивными документами МФЦ.
   5. Для приема посетителей выделяются зоны ожидания, исключающие несанкционированный доступ к обрабатываемым персональным данным.
2. Реализуемые требования к защите персональных данных
   1. МФЦ принимает правовые, организационные и технические меры (или обеспечивает их принятие), необходимые и достаточные для обеспечения исполнения обязанностей, предусмотренных Законом о ПДн и принятыми в соответствии с ним нормативными правовыми актами, 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.
   2. Состав указанных в пункте 5.1 Политики мер, включая их содержание и выбор средств защиты ПДн, определяется, а внутренние регулятивные документы об обработке и защите ПДн утверждаются (издаются) МФЦ исходя из требований:
      1. Федерального закона от 27 июня 2006 г. N 152-ФЗ "О персональных данных";
      2. Трудового кодекса Российской Федерации;
      3. Постановления Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
      4. Приказа ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности ПДн при их обработке в информационных системах ПДн»;
      5. Приказа ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;
      6. Иных нормативных правовых актов Российской Федерации и Московской области об обработке и защите ПДн;
      7. Настоящей Политикой;
      8. Локальными нормативными актами МФЦ, разработанными в развитие настоящей Политики;
      9. Соглашениями о взаимодействии, заключаемыми МФЦ с ведомствами и органами исполнительной власти;
      10. согласиями на обработку персональных данных.
   3. Хранение ПДн осуществляется в форме, позволяющей определить субъекта ПДн, не дольше чем этого требуют цели обработки ПДн, если срок хранения не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн. При хранении ПДн возможно использование информационных баз данных, находящихся исключительно на территории Российской Федерации.
   4. МФЦ осуществляется ознакомление Работников, непосредственно осуществляющих обработку ПДн, с положениями законодательства о ПДн, в том числе требованиями к защите ПДн, Политикой и иными внутренними регулятивными документами по вопросам обработки ПДн, и (или) обучение указанных работников по вопросам обработки и защиты ПДн.
   5. При обработке ПДн с использованием средств автоматизации МФЦ, в частности, применяются следующие меры:
      1. Назначаются ответственные за организацию обработки ПДн;
      2. Утверждаются (издаются) внутренние регулятивные документы по вопросам обработки и защиты ПДн, в том числе устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства, устранение последствий таких нарушений;
      3. Осуществляется внутренний контроль и (или) аудит соответствия обработки ПДн Закону о ПДн и принятым в соответствии с ним нормативным правовым актам, требованиям к защите ПДн, Политике и внутренним регулятивным документам МФЦ;
      4. Проводится оценка вреда, который может быть причинен субъектам ПДн в случае нарушения Закона о ПДн, определяется соотношение указанного вреда и принимаемых МФЦ мер, направленных на обеспечение исполнения обязанностей, предусмотренных Законом о ПДн.
   6. Обеспечение безопасности ПДн в МФЦ при их обработке в ИСПДн достигается, в частности, путем:
      1. Определения угроз безопасности ПДн. Тип актуальных угроз безопасности ПДн и необходимый уровень защищенности ПДн определяются в соответствии с требованиями законодательства и с учетом проведения оценки возможного вреда;
      2. Определения в установленном порядке состава и содержания мер по обеспечению безопасности ПДн, выбора средств защиты информации. При невозможности технической реализации отдельных выбранных мер по обеспечению безопасности ПДн, а также с учетом экономической целесообразности могут разрабатываться компенсирующие меры, направленные на нейтрализацию актуальных угроз безопасности ПДн. В этом случае в ходе разработки СЗПДн проводится обоснование применения компенсирующих мер для обеспечения безопасности ПДн;
      3. Применения организационных и технических мер по обеспечению безопасности ПДн, необходимых для выполнения требований к защите ПДн, обеспечивающих определенные уровни защищенности ПДн, включая применение средств защиты информации, прошедших процедуру оценки соответствия, когда применение таких средств необходимо для нейтрализации актуальных угроз.
   7. В МФЦ в том числе осуществляются:
      1. Оценка эффективности принимаемых и реализованных мер по обеспечению безопасности ПДн;
      2. Учет машинных носителей ПДн, обеспечение их сохранности;
      3. Обнаружение фактов несанкционированного доступа к ПДн и принятие соответствующих мер;
      4. Восстановление ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
      5. Установление правил доступа к обрабатываемым ПДн, а также обеспечение регистрации и учета действий, совершаемых с ПДн;
      6. Организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;
      7. Контроль за принимаемыми мерами по обеспечению безопасности ПДн, уровнем защищенности.
   8. Обеспечение защиты ПДн в МФЦ при их обработке, осуществляемой без использования средств автоматизации, достигается, в частности, путем:
      1. Обособления ПДн от иной информации;
      2. Недопущения фиксации на одном материальном носителе ПДн, цели обработки которых заведомо не совместимы;
      3. Использования отдельных материальных носителей для обработки каждой категории ПДн;
      4. Принятия мер по обеспечению раздельной обработки ПДн 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.
   9. В состав мер по обеспечению безопасности ПДн, реализуемых в рамках СЗПДн с учетом актуальных угроз безопасности ПДн и применяемых информационных технологий, входят:
      1. Идентификация и аутентификация субъектов доступа и объектов доступа;
      2. Управление доступом субъектов доступа к объектам доступа;
      3. Ограничение программной среды;
      4. Защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные;
      5. Регистрация событий безопасности;
      6. Антивирусная защита;
      7. Обнаружение (предотвращение) вторжений;
      8. Контроль (анализ) защищенности персональных данных;
      9. Обеспечение целостности информационной системы и персональных данных;
      10. Обеспечение доступности персональных данных;
      11. Защита технических средств;
      12. Защита информационной системы, ее средств, систем связи и передачи данных;
      13. Выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) возникновению угроз безопасности персональных данных, и реагирование на них;
      14. Управление конфигурацией информационной системы и системы защиты персональных данных.
   10. При передаче персональных данных субъекта персональных данных работники МФЦ, осуществляющие обработку персональных данных, должны соблюдать следующие требования:
       1. не сообщать персональные данные субъекта персональных данных третьей стороне без письменного согласия субъекта, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта персональных данных, а также в случаях, установленных Федеральным законом о персональных данных;
       2. не сообщать персональные данные субъекта персональных данных в коммерческих целях без его письменного согласия;
       3. предупредить лиц, получающих персональные данные субъекта персональных данных о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что правило соблюдено. Лица, получающие персональные данные субъекта персональных данных, обязаны соблюдать режим конфиденциальности;
       4. разрешать доступ к персональным данным субъекта персональных данных только лицам, определенным соответствующим приказом МФЦ, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы для выполнения конкретных функций;
       5. не запрашивать информацию о состоянии здоровья субъекта персональных данных, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работниками трудовой функции;
       6. передавать персональные данные субъекта персональных данных представителям субъекта персональных данных в порядке, установленном Трудовым кодексом Российской Федерации, и ограничить эту информацию только теми персональными данными субъекта персональных данных, которые необходимы для выполнения указанными представителями их функций.
   11. Передача МФЦ персональных данных или ее представителей третьим лицам может допускаться только в случаях, установленных Федеральным законом о персональных данных.
   12. МФЦ при обращении или по запросу субъекта персональных данных либо его представителя, а также по запросу Роскомнадзора инициируют блокировку неправомерно обрабатываемых персональных данных этого субъекта с момента обращения или получения запроса на период проверки. В случае выявления неправомерной обработки персональных данных в МФЦ или лицом, действующим по поручению МФЦ, в срок, не превышающий трех рабочих дней с даты этого выявления, в МФЦ прекращают неправомерную обработку персональных данных или обеспечивают прекращение неправомерной обработки. В случае если обеспечить правомерность обработки персональных данных невозможно, в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, такие персональные данные уничтожаются в МФЦ или МФЦ обеспечивает их уничтожение в организациях, осуществляющих обработку этих данных на основании договоров на оказание соответствующих услуг МФЦ.
   13. МФЦ на основании сведений, представленных субъектом персональных данных или его представителем либо Роскомнадзором, или иных необходимых документов уточняет персональные данные в течение семи рабочих дней со дня представления таких сведений.
   14. По достижении цели обработки персональных данных в МФЦ обработка персональных данных прекращается и эти персональные данные уничтожаются, за исключением случаев, предусмотренных законодательством Российской Федерации.
   15. В случае отзыва субъектом персональных данных своего согласия на обработку персональных данных в МФЦ обработка прекращается в срок, не превышающий тридцати дней с даты поступления отзыва.
   16. В МФЦ по запросу субъекта персональных данных или его представителя сообщают информацию о наличии персональных данных, относящихся к субъекту. По запросу субъекта персональных данных или его представителя в МФЦ знакомят субъекта персональных данных или его представителя с этими персональными данными в течение тридцати дней с даты получения запроса.
   17. При сборе, обработке и хранении персональных данных хранение и защита персональных данных как на бумажных, так и на электронных (автоматизированных) носителях информации осуществляется в порядке, исключающем их утрату или их неправомерное использование.
3. **Использование web-ресурсов МФЦ**
   1. МФЦ использует файлы cookies, в том числе обрабатывает сведения о посетителях web-ресурсов, необходимые для правильной работы web-ресурсов МФЦ, а также в целях улучшения качества работы и удобства использования web-ресурсов.
   2. Некоторая часть функционала web-ресурсов МФЦ может быть использована без предоставления персональных данных. Однако для использования специальных возможностей web-ресурсов необходимо предоставить пользовательские данные, включая персональные данные.
   3. Проставляя галочку (чек-бокс) или нажимая кнопку в электронной форме подтверждения, предоставляемой web-ресурсом МФЦ, субъект персональных данных выражает свое согласие на обработку своих персональных данных МФЦ на условиях, предусмотренных настоящей Политикой.
   4. Субъект персональных данных не использует web-ресурсы МФЦ и не предоставляет МФЦ свои персональные данные, если он не согласен с положениями данного раздела настоящей Политики.
   5. Субъект персональных данных вправе отозвать свое разрешение на использование файлов cookies, удалив соответствующие cookies в настройках интернет браузера.

**7. Заключительные положения**

7.1. Настоящая Политика является общедоступным документом МФЦ и распространяет свое действие на отношения по обработке персональных данных, возникшие как до, так и после утверждения настоящей Политики.

7.2. Настоящая Политика подлежит изменению в случае принятия нормативных актов, устанавливающих новые требования по обработке и защите персональных данных или внесения изменений в действующие нормативные правовые акты.

7.3. Персональные данные относятся к конфиденциальной информации. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении срока хранения, если иное не определено федеральным законом.

7.4. Лица, виновные в нарушении правил обработки персональных данных и требований к защите персональных данных работника, установленных действующим законодательством Российской Федерации и настоящей Политикой, несут ответственность, предусмотренную законодательством Российской Федерации.