Утверждена
приказом директора
муниципального бюджетного
учреждения «Центр физической
культуры и спорта города
Ростова-на-Дону»
от 15.08.2016 г. № 69

ПОЛИТИКА

в отношении обработки и защиты персональных данных муниципального бюджетного учреждения «Центр физической культуры и спорта города Ростова-на-Дону»

г. Ростов-на-Дону
2016 г.

1. Общие положения

1.1. Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту ПДн), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация, определяемая нормативно-правовыми актами Российской Федерации, Перечнем персональных данных (далее - ПДн), обрабатываемых в муниципальном бюджетном учреждении «Центр физической культуры и спорта города Ростова-на-Дону» (далее – МБУ «ЦФКС», Учреждение) определяемых локальными актами Учреждения.

1.2. Настоящая Политика об обработке персональных данных (далее – Политика):

– разработана в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее - Закон о ПДн) в целях обеспечения соответствия законодательству Российской Федерации обработки персональных данных (далее - ПДн) в МБУ «ЦФКС»;

– является основополагающим внутренним документом МБУ «ЦФКС», определяющим ключевые направления его деятельности в области обработки и защиты ПДн;

– раскрывает основные категории персональных данных, обрабатываемых МБУ «ЦФКС», цели, способы и принципы обработки ПДн, права и обязанности учреждения при обработке персональных данных, права субъектов персональных данных, а также перечень мер, применяемых в целях обеспечения безопасности персональных данных при их обработке;

– предназначена для работников МБУ «ЦФКС», осуществляющих обработку персональных данных в целях непосредственной реализации ими закрепленных в Политике принципов, а также является информационным ресурсом для субъектов персональных данных, позволяющим определить концептуальные основы деятельности Учреждения при обработке персональных данных.

2. Источники нормативного правового регулирования вопросов обработки персональных данных

2.1. Обработка персональных данных осуществляется в связи с выполнением законодательно возложенных на МБУ «ЦФКС» полномочий, определяемых:

– Федеральным законом от 04.12.2007 № 329-ФЗ «О физической культуре и спорте в Российской Федерации»;

– Федеральным законом от 06.10.2003 № 131-ФЗ «Об общих принципах организации местного самоуправления в Российской Федерации» ст.16 п.13;

– Федеральным законом от 24.07.1998 № 124-ФЗ «Об основных гарантиях прав ребенка в Российской Федерации»;

– Федеральным законом от 27.07.2013 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг;

– Указом Президента от 24.03.14 № 172 "О Всероссийском физкультурно-спортивном комплексе "Готов к труду и обороне" (ГТО)";

– Постановлением Правительства РФ от 11.06.2014 № 540 "Об утверждении Положения о Всероссийском физкультурно-спортивном комплексе "Готов к труду и обороне" (ГТО)";

– постановлением Администрации города Ростова-на-Дону от 08.07.2016 № 920 «Об утверждении Административного регламента № АР-071-08-Т муниципальной услуги «Проведение занятий физкультурно-спортивной направленности по месту проживания граждан», оказываемой муниципальным бюджетным учреждением «Центр физической культуры и спорта города Ростова-на-Дону».

– иными нормативными актами Российской Федерации, Правительства Ростовской области и Администрации города Ростова-на-Дону.

Кроме того, обработка ПДн в Учреждении осуществляется в ходе трудовых и иных непосредственно связанных с ними отношений, в которых Учреждение выступает в качестве работодателя.

2.2. Обработка ПДн в МБУ «ЦФКС» осуществляется в целях исполнения полномочий Учреждения и организации предоставления государственных, муниципальных и иных услуг, и производится на основании нормативных правовых актов Российской Федерации, Правительства Ростовской области и Администрации города Ростова-на-Дону, соглашений с федеральными органами исполнительной власти Российской Федерации, органами государственных внебюджетных фондов, органами местного самоуправления города Ростова-на-Дону и подведомственными им организациями, иными организациями в соответствии с законодательством Российской Федерации.

2.3. В связи с трудовыми и иными непосредственно связанными с ними отношениями, в которых МБУ «ЦФКС» выступает в качестве работодателя, обрабатываются ПДн лиц, претендующих на трудоустройство в Учреждение, работников (далее - Работники) и бывших Работников.

2.4. В связи с реализацией своих прав и обязанностей как юридического лица, МБУ «ЦФКС» обрабатываются ПДн физических лиц, являющихся контрагентами (возможными контрагентами) по гражданско-правовым договорам, ПДн руководителей, членов коллегиальных исполнительных органов и представителей юридических лиц, ПДн иных физических лиц, представленные участниками закупки, а также граждан, письменно обращающихся в Учреждение по вопросам его деятельности.

2.5. Обработка ПДн осуществляется на основании федеральных законов и иных нормативных правовых актов Российской Федерации, а в необходимых случаях - при наличии письменного согласия субъекта ПДн.

2.6. МБУ «ЦФКС» предоставляет обрабатываемые им ПДн государственным органам и организациям, имеющим, в соответствии с федеральным законом, право на получение соответствующих ПДн.

2.7. При обработке ПДн обеспечиваются их точность, достаточность, а при необходимости - и актуальность по отношению к целям обработки.

3. Принципы обеспечения безопасности персональных данных

3.1. Основной задачей обеспечения безопасности ПДн при их обработке в МБУ «ЦФКС» 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 процесс е обработки.

3.2. Для обеспечения безопасности ПДн МБУ «ЦФКС» 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 МБУ «ЦФКС»;

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 осуществляется на основании результатов анализа практики обработки ПДн в МБУ «ЦФКС» с 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 и исключительно в объеме, необходимом для выполнения их должностных обязанностей;

9) гибкость: обеспечение выполнения функций защиты ПДн при изменении характеристик функционирования информационных систем, используемых в МБУ «ЦФКС», а также объема и состава обрабатываемых ПДн;

10) открытость алгоритмов и механизмов защиты: структура, технологии и алгоритмы функционирования системы защиты ПДн (далее - СЗПДн) не дают возможности преодоления имеющихся в МБУ «ЦФКС» систем защиты возможными нарушителями безопасности ПДн;

11) научная обоснованность и техническая реализуемость: уровень 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 МБУ «ЦФКС» 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 МБУ «ЦФКС» 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.

4. Доступ к обрабатываемым персональным данным

4.1. Доступ к обрабатываемым в МБУ «ЦФКС» ПДн имеют лица, уполномоченные приказом Учреждения.

4.2. Доступ Работников к обрабатываемым ПДн осуществляется в соответствии с их должностными обязанностями и требованиями внутренних регулятивных документов МБУ «ЦФКС». Работники под роспись знакомятся с документами МБУ «ЦФКС», устанавливающими порядок обработки ПДн, включая документы, устанавливающие права и обязанности конкретных Работников.

4.3. Порядок доступа субъекта ПДн к его ПДн, обрабатываемым МБУ «ЦФКС», определяется в соответствии с законодательством и определяется внутренними регулятивными документами МБУ «ЦФКС».

5. Реализуемые требования к защите персональных данных

5.1. МБУ «ЦФКС» 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.

5.2. 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 МБУ «ЦФКС» исходя из требований:

- Закона о ПДн;
- главы 14 Трудового кодекса Российской Федерации;

– Постановления Правительства Российской Федерации от 1.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– Постановления Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

– приказа ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности ПДн при их обработке в информационных системах ПДн»;

– иных нормативных правовых актов Российской Федерации, Правительства Ростовской области и Администрации города Ростова-на-Дону об обработке и защите ПДн.

5.3. В предусмотренных законодательством случаях обработка ПДн осуществляется МБУ «ЦФКС» с согласия субъектов ПДн. МБУ «ЦФКС» производится устранение выявленных нарушений законодательства об обработке и защите ПДн.

5.4. 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.

5.5. МБУ «ЦФКС» 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.

5.6. При обработке ПДн с использованием средств автоматизации МБУ «ЦФКС», в частности, применяются следующие меры:

1) назначается ответственный 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 МБУ «ЦФКС»;

4) проводится оценка вреда, который может быть причинен субъектам ПДн в случае нарушения Закона о ПДн, определяется соотношение указанного вреда и принимаемых МБУ «ЦФКС» мер, направленных на обеспечение исполнения обязанностей, предусмотренных Законом о ПДн.

5.7. Обеспечение безопасности ПДн в МБУ «ЦФКС» 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.

В МБУ «ЦФКС», в том числе, осуществляются:

– оценка эффективности принимаемых и реализованных мер по обеспечению безопасности ПДн;

– учет машинных носителей ПДн, обеспечение их сохранности;

– обнаружение фактов несанкционированного доступа к ПДн и обеспечению принятие соответствующих мер;

– восстановление ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

– установление правил доступа к обрабатываемым ПДн, а также обеспечение регистрации и учета действий, совершаемых с ПДн;

– 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;

– контроль за принимаемыми мерами по безопасности ПДн, уровня защищенности.

5.8. Обеспечение защиты ПДн в МБУ «ЦФКС» 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.

5.9. В состав мер по обеспечению безопасности ПДн, реализуемых в рамках СЗПДн с учетом актуальных угроз безопасности ПДн и применяемых информационных технологий, входят:

– идентификация и аутентификация субъектов доступа и объектов доступа;

– управление доступом субъектов доступа к объектам доступа;

– ограничение программной среды;

– защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные (далее - машинные носители персональных данных);

– регистрация событий безопасности;

– антивирусная защита;

– обнаружение (предотвращение) вторжений;

– контроль (анализ) защищенности персональных данных;

– обеспечение целостности информационной системы и персональных данных; обеспечение доступности персональных данных;

– защита среды виртуализации; защита технических средств;

– защита информационной системы, ее средств, систем связи и передачи данных;

– выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных (далее - инциденты), и реагирование на них;

– управление конфигурацией информационной системы и системы зашиты персональных данных.