Гончарова Н.Н.

Подписано цифровой подписью: Гончарова Н.Н.
Дата: 2023.06.28 10:34:22 +03'00'

УТВЕРЖДЕНО
приказом МБУДО СДЮСШОР № 4
от 17.03.2015г № 12-од
с изменениями утвержденными
приказом МБУ СШОР № 4
от 09.01.2019г № 02-од
с изменениями утвержденными
приказом МБУДО СШ по спортивной гимнастике
от 22.03.2023г № 12-од

ПОЛИТИКА
в отношении обработки и обеспечения безопасности персональных данных МБУДО СШ по спортивной гимнастике

1. Общие положения

1.1. Настоящая Политика в области обработки и защиты персональных данных, (далее – Политика) МБУДО СШ по спортивной гимнастике (далее СШ):

– разработана в целях обеспечения реализации требований законодательства Российской Федерации в области обработки персональных данных;

– раскрывает основные категории персональных данных, обрабатываемых в СШ (далее – Оператор), цели, способы и принципы обработки Оператором персональных данных, права и обязанности Оператора при обработке персональных данных, права субъектов персональных данных, а также перечень мер, применяемых Оператором в целях обеспечения безопасности персональных данных при их обработке;

– является документом, декларирующим концептуальные основы деятельности Оператора при обработке персональных данных.

1.2. Настоящая Политика утверждается приказом руководителя.

1.3. Основные понятия:

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту 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.

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

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.

Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

1.4. В настоящей Политике используются следующие обозначения и сокращения:

АРМ – автоматизированное рабочее место

ИСПДн – информационная система персональных данных

НСД – несанкционированный доступ

ПДн – персональные данные

СЗИ – средства защиты информации

СЗПДн – система (подсистема) защиты персональных данных

1.5. Требования настоящей Политики распространяются на всех работников СШ, а также всех прочих лиц (имеющих санкционированный доступ к информационным системам и ресурсам СШ (исполнители контрактов, аудиторы и т.п.).

2. Обрабатываемые категории персональных данных и источники их поступления.

2.1. Перечень персональных данных, подлежащих защите в СШ, формируется в соответствии с Федеральным законом РФ от 27 июля 2006 г. № 152 - ФЗ «О персональных данных». Сведениями, составляющими персональные данные, является любая информация, относящаяся к прямо или косвенно определяемому физическому лицу (субъекту персональных данных).

2.2. В зависимости от субъекта персональных данных, СШ обрабатывает персональные данные следующих категорий субъектов персональных данных:

2.2.1. Персональные данные работника СШ - информация, необходимая в связи с трудовыми отношениями и касающиеся конкретного работника. Получаются от работников при заключении трудового договора.

2.2.2. Персональные данные обучающихся, занимающихся, их законных представителей - информация, необходимая СШ для достижения целей обработки и для выполнения требований законодательства Российской Федерации. Получаются от обучающихся, занимающихся, и их представителей на основании согласий.

3. Цели обработки персональных данных

Организация осуществляет обработку персональных данных в следующих целях:

– предоставление информации о контингенте лиц, осваивающих общеобразовательные программы, занимающихся в СШ;

– прогнозирование необходимого количества мест в СШ;

– обеспечение учета обучающихся, занимающихся в СШ;

– порядок поступления в спортивную организацию;

– обеспечение формирования полного набора данных об этапах учебно-тренировочного процесса и достижениях обучающихся в СШ, включая результаты учебно-тренировочного процесса;

– предоставление информации о влиянии учебно-тренировочного процесса на состояние здоровья обучающихся;

– ведение электронных журналов и электронных дневников для предоставления обучающимся и/или его законным представителям информации о достижениях обучающегося в СШ в электронном формате, оказания иных сервисов;

– организации кадрового учета СШ, обеспечения соблюдения законов и иных нормативных правовых актов, заключения и исполнения обязательств по трудовым и гражданско – правовым договорам, ведения кадрового делопроизводства, содействия работникам в трудоустройстве, обучении и продвижении по службе, пользования различного вида льготами, исполнения требований налогового законодательства в связи с исчислением и уплатой налога на доходы физических лиц, а также единого социального налога, пенсионного законодательства при формировании и представлении персонифицированных данных о каждом получателе доходов, учитываемых при начислении страховых взносов на обязательное пенсионное страхование и обеспечение, заполнения первичной статистической документации, в соответствии с Трудовым кодексом Российской Федерации, Налоговым кодексом Российской Федерации, федеральным законом «О персональных данных».

4. Права и обязанности:

4.1. СШ, как оператор персональных данных, вправе:

– отстаивать свои интересы в суде;

– предоставлять персональные данные субъектов третьим лицам, если это предусмотрено действующим законодательством (налоговые, правоохранительные органы и др.);

– отказывать в предоставлении персональных данных в случаях, предусмотренных законодательством;

– использовать персональные данные субъекта без его согласия, в случаях, предусмотренных законодательством.

4.2. Субъект персональных данных имеет право:

– требовать уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав;

– требовать перечень своих персональных данных, обрабатываемых СШ и источник их получения;

– получать информацию о сроках обработки своих персональных данных, в том числе о сроках их хранения;

– требовать извещения всех лиц, которым ранее были сообщены неверные или неполные его персональные данные, обо всех произведенных в них исключениях, исправлениях или дополнениях;

– обжаловать в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке неправомерные действия или бездействия при обработке его персональных данных;

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

5. Принципы и условия обработки персональных данных

5.1. Обработка персональных данных Организацией осуществляется на основе принципов:

– законности и справедливости целей и способов обработки персональных данных;

– соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных;

– соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;

– достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;

– недопустимости объединения созданных для несовместимых между собой целей баз данных, содержащих персональные данные;

– хранения персональных данных в форме, позволяющей определять субъект персональных данных, не дольше, чем этого требуют цели их обработки;

– уничтожения по достижении целей обработки персональных данных или в случае утраты необходимости в их достижении.

5.2. Обработка персональных данных осуществляется на основании условий, определенных законодательством Российской Федерации.

6. Сроки обработки персональных данных

6.1. Началом срока обработки персональных данных считается момент их получения Оператором.

6.2. Оператор осуществляет хранение персональных данных в форме, позволяющей определить субъект персональных данных, не дольше, чем того требуют цели их обработки.

7. Обеспечение безопасности персональных данных

7.1. Оператор при обработке персональных данных принимает необходимые правовые, организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления,

распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

7.2. Обеспечение безопасности персональных данных достигается, в частности:

– – назначением ответственных лиц за организацию обработки персональных данных;

– назначением лиц, непосредственно осуществляющих обработку персональных данных;

– осуществлением внутреннего контроля соответствия обработки персональных данных Федеральному закону от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, внутренним распорядительным документам Оператора;

– – ознакомлением работников Оператора, непосредственно осуществляющих

– обработку персональных данных, с положениями законодательства Российской Федерации в области персональных данных, в том числе требованиями к защите персональных данных, внутренних распорядительных документов Оператора в отношении обработки персональных данных, и (или) обучением указанных работников;

– применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных;

– учетом машинных носителей персональных данных;

– обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;

– восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

– контролем за принимаемыми мерами по обеспечению безопасности персональных данных.

8. Доступ к персональным данным Субъекта

8.1. Список работников СШ, имеющих доступ к персональным данным, утверждается приказом руководителя.

8.2. Передача Персональных данных третьим лицам возможна только с согласия Субъекта в письменной форме или без его согласия в случаях, предусмотренных законодательством РФ.

9. Требования к персоналу по обеспечению защиты ПДН

9.1. Все сотрудники СШ, являющиеся пользователями ИСПДн, должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности ПДн.

9.2. При вступлении в должность нового работника непосредственный начальник подразделения, в которое он поступает, обязан организовать его ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования по защите ПДн, а также обучение навыкам

выполнения процедур, необходимых для санкционированного использования ИСПДн.

Работник должен быть ознакомлен под роспись с положениями настоящей Политики, принятых процедур работы с элементами ИСПДн и СЗПДн.

9.3. Работник, использующие технические средства аутентификации, должны обеспечивать сохранность идентификаторов (электронных ключей) и не допускать НСД к ним, а также возможность их утери или использования третьими лицами. Пользователи несут персональную ответственность за сохранность идентификаторов.

9.4. Работники должны следовать установленным процедурам поддержания режима безопасности ПДн при использовании паролей (если не используются технические средства аутентификации).

9.5. Работники СШ должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица. Все пользователи должны знать требования по безопасности ПДн и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.

9.6. Работникам запрещается устанавливать постороннее программное обеспечение, подключать личные мобильные устройства и носители информации, а также записывать на них защищаемую информацию.

9.7. Работникам запрещается разглашать защищаемую информацию, которая стала им известна при работе с информационными системами СШ, третьим лицам.

9.8. При работе с ПДн в ИСПДн работники СШ обязаны обеспечить отсутствие возможности просмотра ПДн третьими лицами с мониторов АРМ или терминалов.

9.9. При завершении работы с ИСПДн работники обязаны защитить АРМ или терминалы с помощью блокировки ключом или эквивалентного средства контроля, например, доступом по паролю, если не используются более сильные средства защиты.

9.10. Работники СШ должны быть проинформированы об угрозах нарушения режима безопасности ПДн и ответственности за его нарушение. Они должны быть ознакомлены с утвержденной формальной процедурой наложения дисциплинарных взысканий на работников, которые нарушили принятые политику и процедуры безопасности ПДн.

9.11. Работники обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы ИСПДн, могущих повлечь за собой угрозы безопасности ПДн, а также о выявленных ими событиях, затрагивающих безопасность ПДн, руководству подразделения и лицу, отвечающему защиту информации.

9.12. В ИСПДн можно выделить следующие группы пользователей, участвующих в обработке и хранении ПДн:

– Администратора ИСПДн;

– Пользователь ИСПДн.

9.13. Должностные обязанности пользователей ИСПДн отражаются в следующих документах:

– «Инструкция администратора ИСПДн»;

– «Инструкция пользователя ИСПДн».

10. Заключительное положение

10.1. Настоящая Политика является документом, разработанным в СШ, является общедоступной и подлежит размещению на официальном сайте.

10.2. Настоящая Политика подлежит изменению, дополнению в случае появления новых законодательных актов и специальных нормативных документов по обработке и защите персональных данных, но не реже одного раза в три года. Изменения в настоящую Политику вносятся приказом руководителя.

10.3. Контроль исполнения требований настоящей Политики осуществляется сотрудником, ответственными за организацию обработки персональных данных в СШ.

10.4. 8.4. Ответственность должностных лиц СШ, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных, определяется в соответствии законодательством Российской Федерации и внутренними документами СШ.