УТВЕРЖДАЮ

Директор _____Н.А. Куликов

«_16_»__06_____2023г.

ПОЛИТИКА

муниципального учреждения дополнительного образования
«Спортивная школа олимпийского резерва № 3 им. В.И. Русанова»
(МУ ДО СШОР № 3 им. В.И. Русанова)
в отношении обработки персональных данных

На дату утверждения Политики
в МУ ДО СШОР № 3 им. В.И. Русанова
нет представительного органа работников

Ярославль

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Назначение и область действия.

1.1.1.Настоящая Политика муниципального учреждения дополнительного образования «Спортивная школа олимпийского резерва № 3 им. В.И. Русанова» в отношении обработки персональных данных (далее – Политика) определяет общие принципы обработки персональных данных и содержит сведения о реализуемых требованиях к защите персональных данных в муниципальном учреждении дополнительного образования «Спортивная школа олимпийского резерва № 3 имени В.И. Русанова» (далее –оператор, учреждение).

Целью принятия Политики является обеспечение прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

1.1.2. Действие Политики распространяется на все персональные данные субъектов, обрабатываемые в Учреждении с применением средств автоматизации и без применения таких средств.

1.1.3. Настоящая Политика разработана в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Трудовым кодексом Российской Федерации, Федеральным законом от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», другими законодательными и нормативными правовыми актами (далее – законодательство), определяющими порядок работы с персональными данными и требования к обеспечению их безопасности.

1.1.4. Политика подлежит пересмотру и актуализации с периодичностью не реже 1 (одного) разав 3 (три) года, а также при изменении законодательства в области персональных данных.

1.1.5. К настоящей Политике предоставляется неограниченный доступ любому лицу, желающему с ней ознакомиться.

1.1.6. Настоящая Политика размещается на официальном сайте учреждения в сети Интернет, а также в доступном для посетителей местах проведения занятий.

1.2. Основные понятия, используемые в Политике:

1.2.1. **Оператор персональных данных (оператор) - учреждение** (МУДО СШОР № 3 им. В.И. Русанова), самостоятельно или совместно с другими лицами организующее и (или) осуществляющее обработку персональных данных, а также определяющее цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

1.2.2. **персональные данные** - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

1.2.3. **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;

1.2.4. **автоматизированная обработка персональных данных** - обработка персональных данных с помощью средств вычислительной техники;

1.2.5. **база персональных данных** – упорядоченный массив персональных данных, независимый от вида материального носителя информации и используемых средств его обработки (архивы, картотеки, электронные базы данных);

1.2.6. **распространение персональных данных** - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

1.2.7. **предоставление персональных данных** - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

1.2.8. **блокирование персональных данных** - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

1.2.9. **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;

1.2.10. **обезличивание персональных данных** - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

1.2.11. **информационная система персональных данных** - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

1.2.12. **трансграничная передача персональных данных** - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

1.3. Основные права и обязанности оператора и субъекта(ов) персональных данных:

1.3.1. Субъект персональных данных (здесь и далее по тексту под субъектом персональных данных понимается как сам субъект персональных данных, так и его законный представитель: родитель, опекун, попечитель и иные лица, полномочия которых установлены законодательством Российской Федерации) принимает решение о предоставлении его персональных данных и даёт учреждению согласие на их обработку учреждением свободно, своей волей и в своём интересе. Согласие на обработку персональных данных должно быть конкретным, предметным, информированным, сознательным и однозначным.

Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом.

В случаях, предусмотренных федеральным законом, обработка персональных данных осуществляется только с согласия в письменной форме субъекта персональных данных. Равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью.

В случае получения согласия на обработку персональных данных от представителя субъекта персональных данных полномочия данного представителя на дачу согласия от имени субъекта персональных данных проверяются оператором.

Обязанность предоставить доказательство получения согласия субъекта персональных данных на обработку его персональных данных или доказательство наличия оснований на обработку, предусмотренных законодательством, возлагается на оператора.

1.3.2. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных. В случае отзыва субъектом персональных данных согласия на обработку персональных данных оператор вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии оснований, установленных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

1.3.3. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, если такое право не ограничено в соответствии с законодательством. Субъект персональных данных вправе требовать от учреждения уточнения его персональных данных, 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 меры по защите своих прав.

1.3.4. Обработка учреждением персональных данных в целях продвижения предоставляемых им товаров, работ, услуг путём осуществления прямых контактов с потенциальным потребителем с помощью средств связи допускается только при условии предварительного согласия субъекта персональных данных. Указанная обработка персональных данных признается осуществляемой без предварительного согласия субъекта персональных данных, если оператор не докажет, что такое согласие было получено.

Учреждение обязано немедленно прекратить по требованию субъекта персональных данных обработку его персональных данных в вышеуказанных целях.

1.3.5. В учреждении запрещается принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы, за исключением случаев, предусмотренных законодательством, или при наличии согласия в письменной форме субъекта персональных данных.

1.3.6. Если субъект персональных данных считает, что учреждение осуществляет обработку его персональных данных с нарушением требований законодательства или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие учреждения в уполномоченный орган по защите прав субъектов персональных данных (Роскомнадзор) или в судебном порядке. Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

1.3.7. Оператор, получивший доступ к персональным данным, обязан соблюдать конфиденциальность персональных данных - не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

1.3.8. 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.

1.3.9. При сборе персональных данных оператор обязан предоставить субъекту персональных данных по его просьбе информацию, предусмотренную частью 7 статьи 14 Федерального закона «О персональных данных».

1.3.10. Если предоставление персональных данных является обязательным в соответствии с федеральным законом, оператор обязан разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные.

1.3.11. При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети «Интернет», оператор обязан обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, указанных в пунктах 2, 3, 4, 8 части 1 статьи 6 Федерального закона «О персональных данных».

2. ЦЕЛИ СБОРА ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

2.2. Цели обработки персональных данных происходят в том числе из анализа правовых актов, регламентирующих деятельность оператора, целей фактически осуществляемой оператором деятельности, а также деятельности, которая предусмотрена учредительными документами оператора, и конкретных бизнес-процессов оператора в конкретных информационных системах персональных данных (по структурным подразделениям оператора и их процедурам в отношении определенных категорий субъектов персональных данных).

2.3. К целям обработки персональных данных оператора относятся:

- обеспечение соблюдения федеральных законов и иных нормативных правовых актов Российской Федерации, Ярославской области, муниципальных правовых актов, регулирующих вопросы ведения бухгалтерского, налогового, воинского учета, кадровой работы учреждения;

- заключение, исполнение и прекращение гражданско-правовых договоров;

- ведение кадрового делопроизводства, исполнение обязательств по трудовым договорам, содействие работникам в трудоустройстве, обучении и продвижении по службе, пользовании льготами;

- исполнение требований налогового законодательства по вопросам исчисления и уплаты налога на доходы физических лиц, взносов во внебюджетные фонды и страховых взносов во внебюджетные фонды, пенсионного законодательства при

формировании и передаче в СФР персонифицированных данных о каждом получателе доходов, которые учитываются при начислении взносов на обязательное пенсионное страхование;

- заполнение первичной статистической документации в соответствии с трудовым, налоговым законодательством и иными федеральными законами;

- обеспечения требований к антитеррористической защищенности объектов спорта и объектов с массовым пребыванием людей, обеспечения личной безопасности работников, занимающихся и их законных представителей, опекунов, попечителей, зрителей, обеспечения сохранности принадлежащего им имущества;

- предоставление дополнительных образовательных услуг;

-осуществления видов деятельности, перечисленных в уставе учреждения;

- осуществления учреждением спортивной подготовки на основании утвержденного Учредителем муниципального задания, выполнения работ, оказания услуг в сфере физической культуры и спорта, реализации мероприятий, включенных в Единый календарный план физкультурных и спортивных мероприятий учреждения и города Ярославля, проведения занятий по физической культуре и спорту, реализации прав участников тренировочного процесса;

- обеспечение соблюдения федеральных законов и иных нормативных правовых актов, регламентирующих правоотношение в сфере рассмотрения обращений физических и юридических ли, обеспечения доступа к информации о деятельности учреждения.

3. ПРАВОВЫЕ ОСНОВАНИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Правовым основанием обработки персональных данных являются:

- совокупность правовых актов, во исполнение которых и в соответствии с которыми оператор осуществляет обработку персональных данных в том числе, но не ограничиваясь:

- Конституция Российской Федерации;

- Трудовой кодекс Российской Федерации;

- Гражданский кодекс Российской Федерации;

- Налоговый кодекс;

- Семейный кодекс РФ;

- Федеральный закон от 24 апреля 2008 г. № 48-ФЗ «Об опеке и попечительстве»;

- Федеральный закон от 29 декабря 2012 г. N 273-ФЗ «Об образовании в Российской Федерации»;

- Федеральный закон от 04.12.2007 № 329-ФЗ «О физической культуре и спорте в Российской Федерации»;

- Федеральный закон от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг»;

- Федеральный закон от 2 мая 2006 г. № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации»;

-Федеральный закон от 29 ноября 2010 г. № 326-ФЗ «Об обязательном медицинском страховании в Российской Федерации»;

- Федеральный закон от 16 июля 1999 г. № 165-ФЗ «Об основах обязательного социального страхования»;

- Федеральный закон от 15 декабря 2001 г. № 167-ФЗ «Об обязательном пенсионном страховании в Российской Федерации»;

- Федеральный закон от 29 декабря 2006 г. № 255-ФЗ «Об обязательном социальном страховании на случай временной нетрудоспособности и в связи с материнством»;

- Федеральный закон от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;

- Федеральный закон от 1 апреля 1996 г. № 27-ФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования»;

- Федеральный закон от 28 декабря 2013 г. № 400-ФЗ «О страховых пенсиях»;

- Федеральный закон от 15 декабря 2001 г. № 166-ФЗ «О государственном пенсионном обеспечении в Российской Федерации»;

-Федеральный закон от 28 марта 1998 г. № 53-ФЗ «О воинской обязанности и военной службе»;

- Федеральный закон от 26 февраля 1997 г. № 31-ФЗ «О мобилизационной подготовке и мобилизации в Российской Федерации»;

- Федеральный закон от 6 декабря 2011 г. N 402-ФЗ «О бухгалтерском учете»;

- Постановление Правительства РФ от 27 ноября 2006 г. № 719 «Об утверждении Положения о воинском учете»;

- Федеральный закон от 25 декабря 2008 г. № 273-ФЗ «О противодействии коррупции»;

- Федеральный закон от 6 марта 2006 г. № 35-ФЗ «О противодействии терроризму»

- уставные документы оператора;

- договоры, заключаемые между оператором и субъектом персональных данных;

- согласие на обработку персональных данных (в случаях, прямо не предусмотренных законодательством Российской Федерации, но соответствующих полномочиям оператора).

4. ПРИНЦИПЫ И УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Обработка персональных данных в учреждении осуществляется на основе принципов:

- законности и справедливой основы;

- ограничения обработки персональных данных достижением конкретных, заранее определённых и законных целей;

- недопущения обработки персональных данных, несовместимой с целями сбора персональных данных;

- недопущения объединения баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;

- соответствия содержания и объёма обрабатываемых персональных данных заявленным целям обработки;

- недопущения обработки избыточных персональных данных по отношению к заявленным целям их обработки;

- обеспечения точности, достаточности и актуальности персональных данных по отношению к целям обработки персональных данных;

- хранения персональных данных в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен законодательством, договором, стороной которого является субъект персональных данных;

- уничтожения либо обезличивания персональных данных по достижении целей их обработки или в случае утраты необходимости в достижении этих целей, при невозможности устранения учреждением допущенных нарушений персональных данных, в случае отзыва субъектом своего согласия на обработку персональных данных, если иное не предусмотрено законодательством или договором, стороной которого является субъект персональных данных.

5. ОБЪЕМ И КАТЕГОРИИ ОБРАБАТЫВАЕМЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ, КАТЕГОРИИ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ

5.1. Содержание и объем обрабатываемых персональных данных соответствуют заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

5.2. Обработка персональных данных в учреждении допускается в следующих случаях:

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

- обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом,

для осуществления и выполнения возложенных законодательством на учреждение функций, полномочий и обязанностей;

- обработка персональных данных осуществляется в связи с участием лица в конституционном, гражданском, административном, уголовном судопроизводстве, судопроизводстве в арбитражных судах;

- обработка персональных данных необходима для исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве;

- обработка персональных данных необходима для исполнения полномочий федеральных органов исполнительной власти, органов государственных внебюджетных фондов, исполнительных органов государственной власти субъектов Российской Федерации, органов местного самоуправления и функций организаций, участвующих в предоставлении соответственно государственных и муниципальных услуг, предусмотренных Федеральным законом от 27 июля 2010 года № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», включая регистрацию субъекта персональных данных на едином портале государственных и муниципальных услуг и (или) региональных порталах государственных и муниципальных услуг;

- 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 оператора или третьих лиц, в том числе в случаях, предусмотренных Федеральным законом «О защите прав и законных интересов физических лиц при осуществлении деятельности по возврату просроченной задолженности и о внесении изменений в Федеральный закон «О микрофинансовой деятельности и микрофинансовых организациях», либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

- обработка персональных данных необходима для осуществления прав и законных интересов учреждения или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

- обработка персональных данных необходима для осуществления научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и законные интересы субъекта персональных данных;

- обработка персональных данных осуществляется в статистических или иных исследовательских целях, за исключением целей продвижения товаров, работ, услуг на рынке, а также политической агитации, при условии обязательного обезличивания персональных данных;

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

5.3. К категориям субъектов персональных данных относятся:

5.3.1. Работники оператора, бывшие работники, кандидаты на замещение вакантных должностей.

В данной категории субъектов оператором обрабатываются персональные данные в связи с реализацией трудовых отношений:

- фамилия, имя, отчество (при наличии) (в том числе прежние фамилии, имена и (или) отчества (при наличии));

- пол;

- гражданство;

- дата (число, месяц, год) и место рождения (страна, республика, край, область, район, город, поселок, деревня, иной населенный пункт);

- адрес места проживания (почтовый индекс, страна, республика, край, область, район, город, поселок, деревня, иной населенный пункт, улица, дом, корпус, квартира);

- сведения о регистрации по месту жительства или пребывания (почтовый индекс, страна, республика, край, область, район, город, поселок, деревня, иной населенный пункт, улица, дом, корпус, квартира);

- номера телефонов (домашний, мобильный, рабочий) и (или) сведения о других способах связи (адрес электронной почты и др);

- замещаемая должность;

- сведения об образовании (наименование образовательной организации, дата (число, месяц, год) окончания, специальность и квалификация, ученая степень, звание, реквизиты документа об образовании и о квалификации);

- сведения о получении дополнительного профессионального образования (дата (число, месяц, год), место, программа, реквизиты документов, выданных по результатам);

- сведения о трудовой деятельности (наименования организаций (органов) и занимаемых должностей, продолжительность работы (службы) в этих организациях (органах));

- данные трудовой книжки, вкладыша в трудовую книжку;

- реквизиты паспорта или иного удостоверяющего личность гражданина документа;

- реквизиты страхового свидетельства обязательного пенсионного страхования;

- идентификационный номер налогоплательщика;

- данные полиса обязательного медицинского страхования;

- отношение к воинской обязанности, сведения о воинском учете и реквизиты документов воинского учета;

- сведения о семейном положении, составе семьи и о близких родственниках;

- сведения о дееспособности (реквизиты документа, устанавливающие опеку (попечительство), основания ограничения в дееспособности, реквизиты решения суда);

- сведения о государственных наградах, иных поощрениях и знаках отличия;

- сведения о дисциплинарных взысканиях;

- сведения, содержащиеся в материалах служебных проверок;

- сведения о судимости (наличие (отсутствие) судимости, дата (число, месяц, год) привлечения к уголовной ответственности (снятия или погашения судимости), статья);

- реквизиты полиса обязательного медицинского страхования;

- реквизиты свидетельств государственной регистрации актов гражданского состояния;

- сведения о наличии/отсутствии у гражданина заболевания, препятствующего поступлению на работу в учреждение;

- номер расчетного счета (номера расчетных счетов), номер банковской карты (номера банковских карт), иные реквизиты для безналичной выплаты заработной платы;

- фотография;

- сведения о работе, в том числе: дата принятии на работу или назначения на должность, дата перевода, перемещения на иную должность в Учреждении, наименование должности (профессии) с указанием структурных подразделений, размера заработной платы, результатов аттестации на соответствие замещаемой должности, а также сведения о месте работы по совместительству, прежнем месте работы;

- сведения, содержащиеся в трудовом договоре, дополнительных соглашениях к трудовому договору;

- сведения о профессиональной переподготовке и (или) повышении квалификации;

- сведения о ежегодных оплачиваемых отпусках, учебных отпусках и отпусках без сохранения денежного содержания;

- сведения о социальном статусе;

- иные персональные данные, необходимые для достижения целей, предусмотренных разделом 2 Политики.

5.3.2. Потребители (получатели) услуг и контрагенты оператора (физические лица);

В данной категории субъектов оператором обрабатываются персональные данные, полученные оператором в связи предоставлением физкультурно-оздоровительных, спортивных услуг в рамках уставной деятельности, а также в связи с заключением договора, стороной которого является субъект персональных данных:

- фамилия, имя, отчество;

- пол;

- гражданство;

- дата (число, месяц, год) и место рождения (страна, республика, край, область, район, город, поселок, деревня, иной населенный пункт);

- адрес места проживания (почтовый индекс, страна, республика, край, область, район, город, поселок, деревня, иной населенный пункт, улица, дом, корпус, квартира);

- сведения о регистрации по месту жительства или пребывания (почтовый индекс, страна, республика, край, область, район, город, поселок, деревня, иной населенный пункт, улица, дом, корпус, квартира);

- номера телефонов (домашний, мобильный, рабочий), адрес электронной почты;

- идентификационный номер налогоплательщика (дата (число, месяц, год) и место постановки на учет, дата (число, месяц, год) выдачи свидетельства);

- данные паспорта или иного удостоверяющего личность документа;

- сведения об участии в управлении хозяйствующим субъектом (за исключением жилищного, жилищно-строительного, гаражного кооперативов, садоводческого, огороднического, дачного потребительских кооперативов, товарищества собственников недвижимости и профсоюза, зарегистрированного в установленном порядке), занятии предпринимательской деятельностью;

- номер расчетного счета (банковские реквизиты);

5.3.3. Представители/работники потребителей услуг, контрагентов оператора (юридических лиц).

В данной категории субъектов оператором обрабатываются персональные данные, полученные оператором в связи с заключением договора, стороной которого является потребитель услуг/контрагент (юридическое лицо), и используемые оператором исключительно для исполнения указанного договора:

- фамилия, имя, отчество;

- пол;

- номера телефонов (домашний, мобильный, рабочий), адрес электронной почты;

- замещаемая должность;

- данные паспорта или иного удостоверяющего личность документа;

- реквизиты доверенности, иного документа, подтверждающего полномочия представителя.

5.3.4. Обучающиеся.

В данной категории субъектов оператором обрабатываются персональные данные в связи с реализацией видов деятельности, перечисленных в уставе учреждения:

- фамилия, имя, отчество (при наличии)

- пол;

- дата (число, месяц, год) и место рождения (страна, республика, край, область, район, город, поселок, деревня, иной населенный пункт);

- адрес по месту жительства (месту пребывания) и (или) адрес фактического проживания;

- номер контактного телефона и (или) сведения о других способах связи;

- реквизиты документа, удостоверяющего личность (вид, серия, номер, когда и кем выдан); реквизиты свидетельства о рождении;

- сведения о гражданстве;

- сведения об образовательной организации (школа, класс, группа), в которой обучается несовершеннолетний обучающийся;

- сведения об отсутствии у обучающихся заболевания, препятствующего освоению программ спортивной подготовки учреждения в области физической культуры и спорта;

- сведения о социальном статусе

5.3.5. Законные представители: родители, опекуны, попечители обучающихся / работников.

В учреждении обрабатываются следующие персональные данные законных представителей: родителей, опекунов, попечителей обучающихся / работников:

- фамилия, имя, отчество (при наличии);

- число, месяц, год рождения;

- место рождения;

- адрес по месту жительства (месту пребывания) и (или) адрес фактического проживания;

- реквизиты документа, удостоверяющего личность (вид, серия, номер, когда и кем выдан)

- реквизиты документа, подтверждающего статус родителя, опекуна, попечителя.

- номер контактного телефона и (или) сведения о других способах связи;

5.3.6. Физические лица, обратившиеся в учреждение с жалобой, предложением, заявлением.

В данной категории субъектов оператором обрабатываются персональные данные, полученные у физического лица, обратившегося в учреждение с жалобой, предложением, заявлением, и используемые оператором исключительно для рассмотрения и направления ответа на обращение:

- фамилия, имя, отчество (при наличии);
- почтовый адрес (почтовый индекс, страна, республика, край, область, район, город, поселок, деревня, иной населенный пункт, улица, дом, корпус, квартира);
- номера телефонов (домашний, мобильный, рабочий) и (или) сведения о других способах связи (адрес электронной почты и др).

5.4. Учреждение и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

5.5. Учреждение вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, 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. Лицо, осуществляющее обработку персональных данных по поручению учреждения, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом «О персональных данных». В поручении учреждения должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных. В случае, если учреждение поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет учреждение. Лицо, осуществляющее обработку персональных данных по поручению учреждения, несет ответственность перед учреждением.

5.6. Учреждением не обрабатываются персональные данные, относящиеся к специальным категориям:

- расовая принадлежность;
- национальная принадлежность;

- политические взгляды;

- религиозные или философские убеждения;

- состояния здоровья (за исключением данных о состоянии здоровья работников учреждения, а также данных о состоянии здоровья обучающихся в случаях, предусмотренных федеральными законами и иными нормативными правовыми актами);

- интимная жизнь;

- а также иные персональные данные о частной жизни, о членстве субъектов персональных данных в общественных объединениях.

Обработка указанных категорий персональных данных допускается в случаях, если:

- она прямо предусмотрена федеральными законами и иными нормативными правовыми актами Российской Федерации;

- субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных;

- обработка персональных данных, разрешенных субъектом персональных данных для распространения, осуществляется с соблюдением запретов и условий, предусмотренных статьей 10.1 Федерального закона «О персональных данных».

5.7. Обработка персональных данных о судимости может осуществляться учреждением исключительно в случаях и в порядке, которые определяются в соответствии с федеральными законами.

5.8. Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность - биометрические персональные данные - обрабатываются учреждением только при наличии согласия субъекта персональных данных в письменной форме или в случаях, когда такая обработка осуществляется в связи с реализацией международных договоров Российской Федерации о реадмиссии, в связи с осуществлением правосудия и исполнением судебных актов, в связи с проведением обязательной государственной дактилоскопической регистрации, а также в случаях, прямо предусмотренных законодательством Российской Федерации.

5.9. Учреждение не осуществляет трансграничную передачу персональных данных.

6. ПОРЯДОК И УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. Оператор осуществляет обработку персональных данных - операции, совершаемые 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.

6.2. Обработка персональных данных осуществляется с соблюдением принципов и правил, предусмотренных Федеральным законом «О персональных данных».

6.3. Обработка персональных данных оператором ограничивается достижением конкретных, заранее определенных и законных целей. Обработке подлежат только персональные данные, которые отвечают целям их обработки. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки.

6.4. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

6.5. При осуществлении хранения персональных данных оператор персональных данных обязан использовать базы данных, находящиеся на территории Российской Федерации, в соответствии с ч. 5 ст. 18 Федерального закона «О персональных данных».

6.6. Использование и хранение биометрических персональных данных вне информационных систем персональных данных могут осуществляться только на таких материальных носителях информации и с применением такой технологии ее хранения, которые обеспечивают защиту этих данных от неправомерного или случайного доступа к ним, их уничтожения, изменения, блокирования, копирования, предоставления, распространения.

6.7. Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных данных (далее - материальные носители), в специальных разделах или на полях форм (бланков). При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

6.8. Условием прекращения обработки персональных данных может являться достижение целей обработки персональных данных, истечение срока действия согласия или отзыв согласия субъекта персональных данных на обработку его персональных данных, а также выявление неправомерной обработки персональных данных.

6.9. Оператор вправе поручить обработку персональных данных другому лицу на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта.

Лицо, осуществляющее обработку персональных данных по поручению оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом «О персональных данных».

Кроме того, оператор вправе передавать персональные данные органам дознания и следствия, иным уполномоченным органам по основаниям, предусмотренным действующим законодательством Российской Федерации.

6.10. Оператор и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения, оформляется отдельно от иных согласий субъекта персональных данных на обработку его персональных данных. Оператор обязан обеспечить субъекту персональных данных возможность определить перечень персональных данных по каждой категории персональных данных, указанной в согласии на обработку персональных данных, разрешенных субъектом персональных данных для распространения.

Передача (распространение, предоставление, доступ) персональных данных, разрешенных субъектом персональных данных для распространения, должна быть прекращена в любое время по требованию субъекта персональных данных. Данное требование должно включать в себя фамилию, имя, отчество (при наличии), контактную информацию (номер телефона, адрес электронной почты или почтовый адрес) субъекта персональных данных, а также перечень персональных данных, обработка которых подлежит прекращению. Указанные в данном требовании персональные данные могут обрабатываться только оператором, которому оно направлено.

6.11. Оператор обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами. Состав и перечень мер оператор определяет самостоятельно.

6.12. Оператор при обработке персональных данных принимает необходимые правовые, организационные и технические меры или обеспечивает их принятие 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. СВЕДЕНИЯ О РЕАЛИЗУЕМЫХ ТРЕБОВАНИЯХ К ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

7.1. Безопасность персональных данных, обрабатываемых учреждением, обеспечивается реализацией правовых, организационных и технических мер, необходимых и достаточных для обеспечения требований федерального законодательства в области защиты персональных данных, выявлением и предотвращением инцидентов, связанных с неправомерным доступом к персональными данными и неправомерных действий с ними.

7.2. Для целенаправленного создания в учреждении неблагоприятных условий и труднопреодолимых препятствий для нарушителей, пытающихся осуществить несанкционированный доступ к персональным данным в целях их получения, модификации, блокирования, уничтожения, заражения вредоносным программным кодом и совершения иных несанкционированных действий, учреждением применяются следующие организационно-технические меры:

- назначение должностных лиц, ответственных за организацию обработки и обеспечение безопасности персональных данных;
- ограничение состава работников, обрабатывающих персональные данные и имеющих доступ к персональным данным при выполнении своих трудовых обязанностей, регламентация порядка предоставления такого доступа;
- ознакомление работников с требованиями законодательства и внутренних нормативных документов учреждения по обработке и защите персональных данных;
- обеспечение учёта и хранения материальных носителей персональных данных и установление порядка обращения с ними, направленного на предотвращение их хищения, подмены, несанкционированного копирования и уничтожения;
- определение угроз безопасности информации, содержащей персональные данные, при ее обработке;
- учет машинных носителей информации, содержащей персональные данные;
- установление правил доступа к информации, содержащей персональные данные, обеспечение регистрации и учета всех действий, совершаемых с информацией, содержащей персональные данные, в информационной системе персональных данных;

- регулярная проверка готовности и эффективности используемых средств защиты информации;

- осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных;

- парольная защита доступа пользователей к информационной системе персональных данных;

- применение в необходимых случаях средств криптографической защиты информации для обеспечения безопасности персональных данных при передаче по открытым каналам связи и хранении на машинных носителях информации;

- осуществление антивирусного контроля, предотвращение внедрения в компьютерную сеть вредоносных программ и программных закладок;

- анализ защищённости информационных систем персональных данных учреждения с применением специализированных программных средств (сканеров безопасности);

- обеспечение восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

- обучение работников, использующих средства защиты информации, применяемые в информационных системах персональных данных, правилам работы с ними;

- учёт применяемых средств защиты информации, эксплуатационной и технической документации к ним, машинных носителей персональных данных;

- систематическое проведение мониторинга действий пользователей, проведение разбирательств по фактам нарушения требований безопасности персональных данных;

- размещение технических средств обработки персональных данных в пределах охраняемой территории;

- организация охраны помещений учреждения и собственно технических средств обработки персональных данных;

- поддержание технических средств охраны, сигнализации помещений в состоянии постоянной готовности, ведение видеонаблюдения;

- контроль за принимаемыми мерами.

8. АКТУАЛИЗАЦИЯ, ИСПРАВЛЕНИЕ, УДАЛЕНИЕ И УНИЧТОЖЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОТВЕТЫ НА ЗАПРОСЫ СУБЪЕКТОВ НА ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ.

8.1. Оператор обязан сообщить в порядке, предусмотренном статьей 14 Федерального закона «О персональных данных», субъекту персональных данных или

его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя либо в течение десяти рабочих дней с момента обращения либо получения оператором запроса субъекта персональных данных или его представителя. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления оператором в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

8.2. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных оператором, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации. Оператор предоставляет сведения, указанные в части 7 статьи14 Федерального закона «О персональных данных», субъекту персональных данных или его представителю в той форме, в которой направлены соответствующие обращение либо запрос, если иное не указано в обращении или запросе.

8.3. В случае, если запрашиваемые сведения, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно к оператору или направить ему повторный запрос в целях получения таких сведений и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

8.4. Субъект персональных данных вправе обратиться повторно к оператору или направить ему повторный запрос в целях получения сведений, указанных в части 7 статьи 14 Федерального закона «О персональных данных», а также в целях ознакомления с обрабатываемыми персональными данными до истечения тридцатидневного срока, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме

по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в пункте 8.2 настоящей Политики, должен содержать обоснование направления повторного запроса.

8.5. Оператор вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным пунктами 8.2 и 8.4 настоящей Политики. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на операторе.

8.6. В случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или персональных данных субъекту персональных данных или его представителю при их обращении либо при получении запроса субъекта персональных данных или его представителя оператор обязан дать в письменной форме мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 Федерального закона «О персональных данных» или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий десяти рабочих дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса субъекта персональных данных или его представителя. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления оператором в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

8.7. Оператор обязан предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных. В срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, оператор обязан внести в них необходимые изменения. В срок, не превышающий семи рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, оператор обязан уничтожить такие персональные данные. Оператор обязан уведомить субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

8.8. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя либо по запросу субъекта персональных данных или его представителя либо уполномоченного органа

по защите прав субъектов персональных данных оператор обязан осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных оператор обязан осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

8.9. В случае подтверждения факта неточности персональных данных оператор на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязан уточнить персональные данные либо обеспечить их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

8.10. В случае выявления неправомерной обработки персональных данных, осуществляемой оператором или лицом, действующим по поручению оператора, оператор в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению оператора. В случае, если обеспечить правомерность обработки персональных данных невозможно, оператор в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

8.11. В случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных, оператор обязан с момента выявления такого инцидента оператором, уполномоченным органом по защите прав субъектов персональных данных или иным заинтересованным лицом уведомить уполномоченный орган по защите прав субъектов персональных данных:

1) в течение двадцати четырех часов о произошедшем инциденте, о предполагаемых причинах, повлекших нарушение прав субъектов персональных данных, и предполагаемом вреде, нанесенном правам субъектов персональных данных, о принятых мерах по устранению последствий соответствующего инцидента, а также предоставить сведения о лице, уполномоченном оператором на взаимодействие с уполномоченным органом по защите прав субъектов персональных данных, по вопросам, связанным с выявленным инцидентом;

2) в течение семидесяти двух часов о результатах внутреннего расследования выявленного инцидента, а также предоставить сведения о лицах, действия которых стали причиной выявленного инцидента (при наличии).

8.12. В случае достижения цели обработки персональных данных оператор обязан прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом «О персональных данных» или другими федеральными законами.

8.13. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных оператор обязан прекратить их обработку или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого,

выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных настоящим Федеральным законом или другими федеральными законами.

8.14. В случае обращения субъекта персональных данных к оператору с требованием о прекращении обработки персональных данных оператор обязан в срок, не превышающий десяти рабочих дней с даты получения оператором соответствующего требования, прекратить их обработку или обеспечить прекращение такой обработки (если такая обработка осуществляется лицом, осуществляющим обработку персональных данных), за исключением случаев, предусмотренных пунктами 2 - 11 части 1 статьи 6, частью 2 статьи 10 и частью 2 статьи 11 Федерального закона «О персональных данных». Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления оператором в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

8.15. В случае отсутствия возможности уничтожения персональных данных в течение срока, указанного в пунктах 8.10 – 8.14 настоящей Политики, оператор осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

8.16. Подтверждение уничтожения персональных данных в случаях осуществляется в соответствии с требованиями, установленными уполномоченным органом по защите прав субъектов персональных данных.

9. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

9.1. Иные права и обязанности учреждения, связанные с обработкой им персональных данных, определяются законодательством в области персональных данных.

9.2. Должностные лица учреждения, виновные в нарушении норм, регулирующих обработку и защиту персональных данных, несут материальную, дисциплинарную, административную, гражданско-правовую и уголовную ответственность в порядке, установленном законодательством и внутренними нормативными документами учреждения.

УТВЕРЖДАЮ
Директор МУДО СШОР № 3
им. В.И. Русанова
_____ Н.А. Куликов
«_16__» ___06_____ 2023 г.

Инструкция по учёту и хранению съёмных носителей персональных данных В МУ ДО СШОР № 3 им. В.И. Русанова

1. Общие положения

1.1. Настоящая Инструкция по учёту и хранению съёмных носителей персональных данных (далее - Инструкция) определяет порядок работы со съёмными носителями персональных данных в МУ ДО СШОР № 3 им. В.И. Русанова (далее - Оператор) и разработана в соответствии с Федеральным законом от 27 июля 2006 г. N 152-ФЗ «О персональных данных», постановлением Правительства РФ от 1 ноября 2012 г. N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" иными нормативными правовыми актами РФ в области защиты персональных данных.

1.2. С Инструкцией знакомятся под роспись и выполняют её все лица, допущенные к обработке персональных данных Приказом о допуске к обработке персональных данных.

1.3. Определения, используемые в настоящей Инструкции:

Съёмный носитель персональных данных - носитель информации, используемый для хранения и передачи персональных данных в электронной форме.

Пользователь - работник Оператора или сотрудник по договору гражданско-правового характера, допущенный к обработке персональных данных Приказом о допуске к обработке персональных данных.

2. Порядок работы со съёмными носителями

2.1. Ответственный за обеспечение безопасности персональных данных либо уполномоченный им работник выдаёт съёмные носители пользователям только в случаях производственной необходимости.

2.2. Все съёмные носители персональных данных учитываются и выдаются пользователям под роспись.

2.3. Пользователям, получившим съёмные носители персональных данных, запрещается передавать их третьим лицам.

2.4. Ответственный за обеспечение безопасности персональных данных либо уполномоченный им работник изымает съёмные носители персональных данных при увольнении пользователя.

2.5. Все съёмные носители персональных данных хранятся в запираемых шкафах или сейфах (металлических шкафах) с кодовыми или внутренними замками (с не менее чем двумя дубликатами ключей).

2.6. Допускается хранение съёмных носителей персональных данных вне запираемых шкафов или сейфов (металлических шкафов) при условиях уничтожения персональных данных в соответствии с Инструкцией по порядку уничтожения и обезличивания персональных данных либо если на съёмном носителе персональных данных хранятся только персональные данные в зашифрованном или обезличенном виде.

2.7. Право на перемещение съёмных носителей информации за пределы территории, на которой осуществляется обработка, имеют только те лица, которым это необходимо для выполнения своих должностных обязанностей.

2.8. Использование неучтённых съёмных носителей для обработки персональных данных фиксируется как несанкционированное, а ответственный за обеспечение безопасности персональных данных инициирует служебную проверку. По факту выясненных обстоятельств составляется Акт проведения расследования инцидента.

2.9. Пользователи в случаях утраты съёмных носителей персональных данных сообщают об этом ответственному за обеспечение безопасности персональных данных.

2.10. Съёмные носители персональных данных, пришедшие в негодность или отслужившие в установленный срок, подлежат уничтожению в соответствии с Инструкцией по порядку уничтожения и обезличивания персональных данных. По результатам уничтожения составляется Акт уничтожения персональных данных.

3. Порядок организации учёта съёмных носителей

3.1. На каждом съёмном носителе персональных данных размещается этикетка с уникальным учётным номером.

3.2. Ответственный за обеспечение безопасности персональных данных либо уполномоченный им работник при выдаче, приёме, уничтожении съёмных носителей персональных данных вносит в Журнал учета съёмных носителей персональных данных:

- учётный номер, размещённый на этикетке на съёмном носителе персональных данных;
- тип съёмного носителя (USB-накопитель, внешний жёсткий диск, CD/DVD-диск);
- серийный или инвентарный номер съёмного носителя;
- место хранения (номер запираемого шкафа или сейфа, номер помещения);
- дату и номер Акта уничтожения персональных данных в случае уничтожения съёмного носителя;
- подпись.

3.3. Пользователи при получении либо сдаче съёмных носителей персональных данных заносят в Журнал учёта съёмных носителей персональных данных свои фамилию, имя, отчество, ставят дату и подпись.

4. Ответственность

4.1. Все работники Оператора, допущенные в установленном порядке к работе с персональными данными, несут административную, материальную, уголовную ответственность в соответствии с действующим законодательством за обеспечение сохранности и соблюдение правил работы с персональными данными.

4.2. Ответственность за доведение требований настоящей Инструкции до работников Оператора несёт ответственный за организацию обработки персональных данных.

4.3. Ответственность за обеспечение мероприятий по реализации требований настоящей Инструкции, в том числе учёт, выдачу, уничтожение съёмных носителей персональных данных, несёт ответственный за обеспечение безопасности персональных данных.

УТВЕРЖДАЮ

Директор МУДО СШОР № 3
им. В.И. Русанова
_____ Н.А. Куликов
«_16___» _____06___202_3_г.

Приложение
к Инструкции по учёту и хранению съёмных
носителей персональных данных

Журнал учета съёмных носителей персональных данных

N п/п	Учётный номер	Тип носителя	Номер (серийный/инвентарный)	Место хранения	Расписка в получении		Дата и номер акта уничтожения	Подпись ответственного лица	Примечание
					Ф. И. О., дата получения, подпись	Ф. И. О., дата сдачи, подпись			
1	2	3	4	5	6	7	8	9	10

Журнал пронумерован, прошнурован и скреплен печатью: _____ листов

[должность, подпись, инициалы, фамилия]

Муниципальное учреждение дополнительного образования
«Спортивная школа олимпийского резерва № 3 им. В.И. Русанова»
(МУ ДО СШОР № 3 им. В.И. Русанова)

ПРИКАЗ

16.06.2023 г. № 90/1-од

О персональных данных в муниципальном учреждении дополнительного образования «Спортивная школа олимпийского резерва № 3 им. В.И. Русанова»

В соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» приказываю:

1. Утвердить прилагаемые:

Правила обработки персональных данных в муниципальном учреждении дополнительного образования «Спортивная школа олимпийского резерва № 3 им. В.И. Русанова» согласно приложению № 1 к настоящему приказу;

Правила осуществления внутреннего контроля соответствия обработки персональных данных в муниципальном учреждении дополнительного образования «Спортивная школа олимпийского резерва № 3 им. В.И. Русанова» требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами, согласно приложению № 2 к настоящему приказу;

Перечень информационных систем персональных данных в муниципальном учреждении дополнительного образования «Спортивная школа олимпийского резерва № 3 им. В.И. Русанова» согласно приложению № 3 к настоящему приказу;

Перечень должностей муниципального учреждения дополнительного образования «Спортивная школа олимпийского резерва № 3 им. В.И. Русанова», предусматривающих осуществление обработки персональных данных либо осуществление доступа к персональным данным, согласно приложению № 4 к настоящему приказу;

Перечень должностей работников муниципального учреждения дополнительного образования «Спортивная школа олимпийского резерва № 3 им. В.И. Русанова», ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных в случае обезличивания персональных данных, согласно приложению № 5 к настоящему приказу;

Типовое обязательство работника муниципального учреждения дополнительного образования «Спортивная школа олимпийского резерва № 3 им. В.И. Русанова», непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним трудового договора прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей, согласно приложению № 6 к настоящему приказу;

Типовую форму согласия на обработку персональных данных работников муниципального учреждения дополнительного образования «Спортивная школа олимпийского резерва № 3 им. В.И. Русанова», а также иных субъектов персональных данных согласно приложению № 7 к настоящему приказу;

Типовую форму согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения,согласно приложению № 8 к настоящему приказу.

Типовую форму разъяснения субъекту персональных данных юридических последствий отказа представить свои персональные данные согласно приложению № 9 к настоящему приказу.

Форму Акта уничтожения документов или съемных носителей персональных данныхсогласно приложению № 10 к настоящему приказу.

2. Довести настоящий приказ до работников учреждения

3. Контроль за исполнением настоящего приказа оставляю за собой.

Директор школы Н.А. Куликов

Приложение № 1
к приказу МУ ДО СШОР № 3
им. В.И. Русанова
от 16.06.2023 № 90/1-од

Правила обработки персональных данных
в муниципальном учреждении дополнительного образования
«Спортивная школа олимпийского резерва № 3 им. В.И. Русанова»

I. Общие положения

1. Правила обработки персональных данных в муниципальном учреждении дополнительного образования «Спортивная школа олимпийского резерва № 3 им. В.И. Русанова» (далее – Правила) устанавливают процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в области персональных данных, а также определяют цели обработки персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки и порядок их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований в муниципальном учреждении дополнительного образования «Спортивная школа олимпийского резерва № 3 им. В.И. Русанова» (далее - Учреждение).

2. Обработка персональных данных в Учреждении выполняется с использованием средств автоматизации или без использования таких средств и включает сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных субъектов, персональные данные которых обрабатываются в Учреждении.

3. Правила определяют политику Учреждения как оператора, осуществляющего обработку персональных данных и определяющего цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

4. Субъектами персональных данных являются:

- работники оператора, бывшие работники, кандидаты на замещение вакантных должностей.
- потребители (получатели) услуг и контрагенты оператора (физические лица);
- представители/работники потребителей услуг, контрагентов оператора (юридических лиц).
- обучающиеся
- законные представители: родители, опекуны, попечители обучающихся/ работников.
- физические лица, обратившиеся в учреждение с жалобой, предложением, заявлением.
- пользователи официального сайта учреждения в информационно-телекоммуникационной сети «Интернет».

5. Обработка персональных данных в Учреждении осуществляется с соблюдением принципов и условий, предусмотренных законодательством Российской Федерации в области персональных данных, инастоящими Правилами.

Для выявления и предотвращения нарушений, предусмотренных законодательством Российской Федерации в сфере персональных данных, в Учреждении используются следующие процедуры и действия:

1) осуществление внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных;

2) оценка вреда, который может быть причинен субъектам персональных данных;

3) ознакомление работников учреждения непосредственно осуществляющих обработку персональных данных, с законодательством Российской Федерации в сфере персональных данных, а также с нормативными правовыми актами по отдельным вопросам, касающимся обработки персональных данных;

4) ограничение обработки персональных данных в связи с достижением конкретных, заранее определенных и законных целей;

5) осуществление обработки персональных данных в соответствии с принципами и условиями обработки персональных данных, установленными законодательством Российской Федерации в сфере персональных данных;

6) недопущение обработки персональных данных, несовместимых с целями сбора персональных данных;

7) недопущение объединения баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;

8) контроль за соответствием содержания и объема обрабатываемых персональных данных заявленным целям обработки;

9) обеспечение при обработке персональных данных точности персональных данных, их достаточности, а в необходимых случаях и актуальности по отношению к целям обработки персональных данных.

6. Обработка персональных данных субъектов персональных данных осуществляется работниками Учреждения, включенными в перечень должностей Учреждения, работа которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным (приложение № 4 к приказу).

7. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных субъектов персональных данных осуществляется путем:

1) непосредственного получения оригиналов необходимых документов (заявление, трудовая книжка, медицинская книжка, справка об отсутствии судимости, иные документы);

2) копирования оригиналов документов;

3) внесения сведений в учетные формы (на бумажных и электронных носителях);

4) формирования персональных данных в ходе кадровой работы;

5) формирования и обработки персональных данных в ходе реализации дополнительных общеобразовательных программ в области физической культуры и спорта;

6) внесение персональных данных в информационные системы, используемые в Учреждении.

8. В случае возникновения необходимости получения персональных данных у третьей стороны следует заранее известить об этом субъекта персональных данных, получить его письменное согласие и сообщить ему о целях, предполагаемых источниках и способах получения персональных данных (за исключением случаев, установленных частью 4 статьи 18 Федерального закона «О персональных данных»).

9. Запрещается получать, обрабатывать и приобщать к личному делу работников и занимающихся Учреждения персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни.

10. При сборе персональных данных работник, осуществляющий сбор (получение) персональных данных непосредственно субъектов персональных данных, обязан разъяснить указанным субъектам юридические последствия отказа предоставить их персональные данные.

11. Передача (распространение, предоставление, доступ) и использование персональных данных субъектов персональных данных осуществляется лишь в случаях и порядке, предусмотренных законодательством Российской Федерации.

II. Цели обработки персональных данных, перечень персональных данных, а также условия и порядок их обработки в Учреждении

12. Персональные данные субъектов персональных данных обрабатываются в целях заключения и исполнения трудовых договоров, договоров гражданско–правового характера, содействия работникам в трудоустройстве, получении образования и продвижении по службе, контроля количества и качества выполняемой работы и обеспечения сохранности имущества; ведение отчетности, установленной законодательством Российской Федерации, предоставления льгот и налоговых вычетов, принятия решения в приеме, либо отказе в приеме на работу, анализа информации о посетителях сайта учреждения, информирования о руководящем и тренерском составе учреждения, рассмотрения обращений граждан, обеспечения личной безопасности работников, занимающихся и их законных представителей, обеспечения сохранности принадлежащего им имущества, осуществления функций в области физической культуры и спорта, реализации деятельности по дополнительным общеобразовательным программам в области физической культуры и спорта, обеспечения условий для развития на территории г. Ярославля физической культуры и массового спорта, организации проведения официальных физкультурно-оздоровительных и спортивных мероприятий города.

III. Порядок обработки персональных данных в автоматизированных информационных системах в Учреждении

13. Обработка персональных данных в Учреждении осуществляется в автоматизированной информационной базе «1С: Предприятие», Автоматизированная система «Удаленное рабочее место», СБиС«Электронная отчётность и электронный документооборот» (далее - автоматизированные информационные системы) (приложение № 3 к Приказу).

14. Работникам Учреждения, имеющим право осуществлять обработку персональных данных в автоматизированных информационных системах (далее - Работники, имеющие право осуществлять обработку персональных данных), предоставляется уникальный логин и пароль для доступа к соответствующей автоматизированной информационной системе.

Доступ к автоматизированным информационным системам предоставляется в рамках функций, предусмотренных должностными инструкциями лиц, имеющих право осуществлять обработку персональных данных.

Информация может вноситься как в автоматическом режиме, так и в ручном режиме, при получении информации на бумажном носителе или в ином виде, не позволяющем осуществлять ее автоматическую регистрацию.

15. При выявлении нарушений, касающихся порядка обработки персональных данных в автоматизированных информационных системах персональных данных, работники, имеющие право осуществлять обработку персональных данных, обязаны незамедлительно принимать меры по установлению причин возникновения таких нарушений и их устранению.

16. Обеспечение безопасности персональных данных, обрабатываемых в автоматизированных информационных системах Учреждения осуществляется в соответствии с постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» (Собрание законодательства Российской Федерации, 2012, N 45, ст. 6257) и достигается, достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, а также иных неправомерных действий в отношении персональных данных согласно статье 19 Федерального закона «О персональных данных».

IV. Порядок работы с обезличенными данными в случае обезличивания персональных данных

17. Обезличивание персональных данных (далее - обезличивание) осуществляется с целью ведения статистического учета и отчетности, снижения уровня возможного ущерба в случае распространения (передачи) и разглашения защищаемых персональных данных, а также с целью снижения требований, предъявляемых к уровню защищенности информационных систем персональных данных, если иное не предусмотрено законодательством Российской Федерации.

18. Обезличивание осуществляется в соответствии с приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 5 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных» (зарегистрирован Минюстом России 10 сентября 2013 г., регистрационный № 29935).

19. Уполномоченные должностные лица могут осуществлять обезличивание при достижении целей обработки или в случае утраты необходимости в достижении указанных целей, если иное не предусмотрено федеральным законом.

20. Обезличивание осуществляется различными методами, в том числе:

1) уменьшением (сокращением) перечня обрабатываемых персональных данных в соответствии с целями обработки;

2) заменой части персональных данных идентификаторами;

3) обобщением персональных данных;

4) понижением точности отдельных персональных данных (например, в содержании сведений, касающихся места жительства субъекта персональных данных, может быть указан только город проживания);

5) делением персональных данных на части и обработкой этих частей отдельно в разных информационных системах персональных данных.

21. При обезличивании следует соблюдать все регламентные требования, предъявляемые к выбранному методу обезличивания и процедурам обезличивания.

22. Обезличенные персональные данные не подлежат разглашению.

23. Обезличенные данные обрабатываются уполномоченными должностными лицами с использованием или без использования средств автоматизации, в том числе с использованием информационных систем персональных данных.

24. При обработке обезличенных данных с использованием средств автоматизации уполномоченные должностные лица осуществляют:

1) установление паролей для защиты учетных записей в доменах и на рабочих компьютерах;

2) установление на серверное оборудование и локальные компьютеры антивирусных программ;

3) выполнение требований по резервному копированию;

4) контроль соблюдения порядка работы со съемными магнитными (машинными) носителями и иными материальными носителями информации (если они используются), а также доступа в помещения, в которых осуществляется хранение и (или) иная обработка обезличенных данных, в том числе с помощью информационных систем персональных данных.

5) соблюдение порядка доступа в помещения, где расположены информационные системы персональных данных.

25. При обработке обезличенных персональных данных без использования средств автоматизации необходимо соблюдение правил хранения бумажных носителей и порядка доступа в помещения, где они хранятся, в целях исключения несанкционированного доступа к обезличенным персональным данным, а также исключения возможности их несанкционированного уничтожения, изменения, блокирования, копирования, распространения, а также от неправомерных действий в отношении обезличенных персональных данных.

26. Обработка обезличенных данных должна осуществляться с использованием технических и программных средств, соответствующих форме представления и хранения указанных данных.

27. Обезличенные данные в информационных системах персональных данных хранятся в электронном виде.

28. Обезличивание осуществляется перед внесением обезличенных данных (получаемых путем обезличивания) в информационные системы персональных данных.

29. Для достижения целей обработки в информационных системах персональных данных могут обрабатываться обезличенные данные, полученные (истребованные) от третьих лиц.

30. В случаях, когда в целях обработки обезличенных данных требуется восстановление персональных данных (из обезличенных данных), уполномоченные должностные лица осуществляют действия, в результате которых обезличенные данные принимают вид, позволяющий определить их принадлежность конкретному субъекту персональных данных (далее - деобезличивание).

31. Деобезличивание осуществляется в соответствии с процедурами преобразования, обратными процедурам обезличивания (далее - процедуры деобезличивания).

32. Процедуры обезличивания и процедуры деобезличивания должны встраиваться в процессы обработки персональных данных, как их неотъемлемый элемент, и эффективно использовать имеющуюся инфраструктуру, обеспечивающую обработку персональных данных.

33. Обработка персональных данных до обезличивания и после деобезличивания должна осуществляться в соответствии с законодательством Российской Федерации с применением мер по обеспечению безопасности персональных данных.

34. По отношению к персональным данным, полученным в результате деобезличивания (пункт 30 настоящих Правил), должны быть выполнены требования к обеспечению их безопасности:

1) не допускается совместное хранение обрабатываемых обезличенных данных и персональных данных, полученных в результате деобезличивания;

2) после завершения обработки обезличенных данных персональные данные, полученные для целей обработки указанных данных в результате деобезличивания, подлежат обязательному уничтожению.

35. Служебная информация, содержащая параметры методов обезличивания, а также процедур обезличивания (деобезличивания) является конфиденциальной информацией. Хранение и защита служебной информации, содержащей параметры методов обезличивания, процедуры обезличивания (деобезличивания) должны обеспечить выполнение установленного порядка

доступа к обезличенным данным и их резервного копирования, возможность актуализации и (или) восстановления хранимых обезличенных данных.

36. При хранении обезличенных данных должно осуществляться (обеспечиваться) раздельное хранение полученных обезличенных данных и касающейся их служебной информации о выбранном методе обезличивания и примененных параметрах процедуры обезличивания.

37. При передаче вместе с обезличенными данными служебной информации о выбранном методе обезличивания и примененных параметрах процедуры обезличивания должна быть обеспечена конфиденциальность канала (способа) передачи указанных сведений.

38. Использование обезличенных данных осуществляется без согласия субъекта персональных данных.

V. Сроки обработки и хранения персональных данных в муниципальном учреждении «Спортивная школа олимпийского резерва № 3 имени В.И. Русанова»

39. Персональные данные хранятся на бумажных и электронных носителях в подразделениях учреждения, в функции которых входит обработка персональных данных, а также в электронном виде в автоматизированных электронных системах.

40. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

41. Персональные данные, полученные Учреждением на бумажном и/или электронном носителях хранятся у работников Учреждения, должности, которых предусматривают осуществление обработки персональных данных либо осуществление доступа к персональным данным (приложение № 4 к приказу).

42. Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности, путем фиксации их на разных материальных носителях персональных данных, в специальных разделах или на полях форм (бланков).

43. Необходимо обеспечивать раздельное хранение персональных данных на разных материальных носителях, обработка которых осуществляется в целях, определенных настоящими Правилами.

44. Контроль за хранением и использованием материальных носителей персональных данных, не допускающий несанкционированное использование, уточнение, распространение и уничтожение персональных данных, находящихся на этих носителях, осуществляет лицо, ответственное за организацию обработки персональных данных в Учреждении, а также комиссия по осуществлению внутреннего контроля соответствия обработки персональных данных требованиям законодательства.

45. Срок хранения персональных данных, внесенных в автоматизированные информационные системы, должен соответствовать сроку хранения бумажных оригиналов.

VI. Порядок уничтожения персональных данных при достижении целей обработки или при наступлении иных законных оснований

46. Уничтожение персональных данных, используемых в обработке, производится при достижении целей обработки или в случае утраты в них необходимости, если иное не предусмотрено Федеральным законом «О персональных данных», либо при наступлении иных законных оснований.

47. Целью уничтожения персональных данных является прекращение существования персональных данных, содержащихся на бумажных, электронных, магнитных носителях информации, а также на немагнитных пленках (далее - материальные носители информации), либо достижение таких условий (результатов), когда становится невозможным осуществить считывание или восстановление таких данных с материальных носителей информации.

48. Уничтожение персональных данных осуществляется после выбора способа их уничтожения.

49. Выбор способа уничтожения персональных данных производится в зависимости от вида содержащего их материального носителя информации и характера персональных данных, подлежащих уничтожению.

50. Уничтожение персональных данных производится следующими способами:

1) уничтожением материальных носителей, содержащих персональные данные, когда исключается возможность дальнейшего использования указанных носителей информации в целях обработки персональных данных;

2) безвозвратным удалением («стиранием») персональных данных и остаточной информации, касающейся персональных данных, с электронных и магнитных носителей информации.

51. Лицом, ответственным за документооборот и архивирование, осуществляется систематический контроль и выделение документов, содержащих персональные данные с истекшими сроками хранения и подлежащими уничтожению.

52. Вопрос об уничтожении выделенных документов, содержащих персональные данные, рассматривается на заседании комиссии Учреждения, состав которой утверждается приказом директора.

По итогам заседания составляются протокол и акт о выделении к уничтожению документов, опись уничтожаемых дел, проверяется их комплектность, акт подписывается председателем и членами комиссии и утверждается директором Учреждения.

53. Комиссия сопровождает документы, содержащие персональные данные к месту уничтожения и присутствует при процедуре уничтожения документов

54. По окончании процедуры уничтожения членами комиссии составляется соответствующий акт об уничтожении документов, содержащих персональные данные.

55. Уничтожение по окончании срока обработки персональных данных на бумажных носителях производится любым способом (механическое, химическое уничтожение, сжигание), не позволяющим произвести считывание или восстановление персональных данных.

56. Уничтожение по окончании срока обработки персональных данных на электронных (или магнитных) носителях производится путем механического нарушения целостности носителя, не позволяющего произвести считывание или восстановление персональных данных, или удалением с электронных носителей методами и средствами гарантированного удаления остаточной информации.

57. Акты об уничтожении персональных данных (материальных носителей информации) подшиваются в соответствующие номенклатурные дела Учреждения.

VII. Рассмотрение запросов субъектов персональных данных или их представителей.

58. Субъекты персональных данных имеют право на получение информации, касающейся обработки их персональных данных, в том числе содержащей:

1) подтверждение факта обработки персональных данных в Учреждении;

2) правовые основания и цели обработки персональных данных;

3) применяемые в Учреждении способы обработки персональных данных;

4) наименование и место нахождения Учреждения, сведения о лицах (за исключением работников Учреждения), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Учреждением или на основании федерального закона;

5) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких персональных данных не предусмотрен законодательством Российской Федерации;

6) сроки обработки персональных данных, в том числе сроки их хранения в Учреждении;

7) порядок осуществления субъектом персональных данных прав, предусмотренных законодательством Российской Федерации в области персональных данных;

8) сведения об осуществленной или предполагаемой трансграничной передаче персональных данных;

9) наименование организации или фамилию, имя, отчество (при наличии) и адрес лица, осуществляющего обработку персональных данных по поручению Учреждения, если обработка поручена или будет поручена такой организации или лицу;

10) иную информацию, предусмотренную законодательством Российской Федерации в области персональных данных.

Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами, в том числе если:

1) обработка персональных данных, включая персональные данные, полученные в результате оперативно-разыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;

2) обработка персональных данных осуществляется органами, осуществившими задержание субъекта персональных данных по подозрению в совершении преступления, либо предъявившими субъекту персональных данных обвинение по уголовному делу, либо применившими к субъекту персональных данных меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством Российской Федерации случаев, если допускается ознакомление подозреваемого или обвиняемого с такими персональными данными;

3) обработка персональных данных осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;

4) доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц;

5) обработка персональных данных осуществляется в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов

личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

59. Субъекты персональных данных вправе требовать от Учреждения уточнения их персональных данных, 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 Российской Федерации меры по защите своих прав.

60. Информация, предусмотренная пунктом 58 настоящих Правил, должна быть предоставлена субъекту персональных данных оператором в доступной форме, и в ней не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, когда имеются законные основания для раскрытия таких персональных данных. Указанная информация предоставляется субъекту персональных данных или его представителю оператором в течение десяти рабочих дней с момента обращения либо получения оператором запроса субъекта персональных данных или его представителя. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления оператором в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

61. Информация, предусмотренная пунктом 58 настоящих Правил, предоставляется субъекту персональных данных или его представителю работником Учреждения, осуществляющего обработку соответствующих персональных данных, при обращении либо при получении запроса субъекта персональных данных или его представителя, содержащего:

1) номер, серию документа, удостоверяющего личность субъекта персональных данных или его представителя, дату выдачи, наименование органа, выдавшего его;

2) информацию, подтверждающую участие субъекта персональных данных в правоотношениях с Учреждением, либо информацию, иным образом подтверждающую факт обработки персональных данных в Учреждении, заверенную подписью субъекта персональных данных или его представителя.

Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

62. В случае если информация, предусмотренная пунктом 58 настоящих Правил, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных, субъект персональных данных вправе повторно обратиться в Учреждение лично или направить повторный запрос в целях получения указанной информации и ознакомления с персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен законодательством Российской Федерации или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

63. Субъект персональных данных вправе повторно обратиться в Учреждение лично или направить повторный запрос в целях получения информации, предусмотренной пунктом 58 настоящих Правил, а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в пункте 62 настоящих Правил, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в пункте 61 настоящих Правил, должен содержать обоснование направления повторного запроса.

64. Учреждение вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным пунктами 61 и 63 настоящих Правил. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на операторе.

65. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами, в том числе, если доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц.

IX. Порядок доступа в помещения, в которых ведется обработка персональных данных

66. Настоящий Порядок определяет правила доступа в помещения Учреждения, где хранятся и обрабатываются персональные данные, в целях исключения несанкционированного доступа к персональным данным, а также обеспечения безопасности персональных данных от уничтожения, изменения, блокирования, копирования, распространения, а также от неправомерных действий в отношении персональных данных.

67. Доступ в помещения Учреждения, в которых ведется обработка персональных данных, в том числе хранятся персональные данные, содержащиеся на материальных носителях информации, имеют уполномоченные должностные лица, определенные на основании списков (перечней) таких лиц, утвержденных в соответствии с п.6 настоящих Правил.

68. Пребывание лиц, не имеющих право на осуществление обработки персональных данных либо на осуществление доступа к персональным данным в помещениях, в которых ведется обработка персональных данных, возможно только в сопровождении должностных лиц, указанных в пункте 67 настоящих Правил.

69. Для помещений, в которых хранятся и обрабатываются персональные данные, организуется режим обеспечения безопасности, при котором обеспечивается сохранность носителей информации, содержащих персональные данные, а также исключается возможность неконтролируемого проникновения и пребывания в этих помещениях посторонних лиц. Данный режим должен обеспечиваться в том числе:

1) запиранием помещения на ключ, в том числе при выходе из него в рабочее время;

2) закрытием металлических шкафов и сейфов, где хранятся носители информации, содержащие персональные данные, во время отсутствия в помещении уполномоченных работников Учреждения, обязанности которых предусматривают осуществление обработки персональных данных либо осуществление доступа к персональным данным.

70. Внутренний контроль за соблюдением в Учреждении Порядка доступа в помещения, в которых ведется обработка персональных данных, и требований к защите персональных данных, осуществляется лицами, ответственными за организацию обработки персональных данных.

Ответственность за соблюдение порядка доступа в помещения, в которых ведется обработка или хранение персональных данных, возлагается:

1) для помещений, расположенных по адресу: г. Ярославль, пр-кт Ленина, д.30 – на работника Учреждения, ответственного за организацию обработки персональных данных в Учреждении;

2) для помещений, расположенных в структурном подразделении - на руководителя структурного подразделения.

X. Ответственный за организацию обработки персональных данных

71. Ответственный за организацию обработки персональных данных в Учреждении (далее - ответственный за обработку персональных данных) назначается приказом директора из числа работников Учреждения.

72. Ответственный за обработку персональных данных в своей работе руководствуется законодательством Российской Федерации и настоящими Правилами.

73. Ответственный за обработку персональных данных обязан:

1) организовывать принятие правовых, организационных и технических мер для обеспечения защиты персональных данных, обрабатываемых в Учреждении, от неправомерного или случайного доступа к ним, их уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий;

2) осуществлять внутренний контроль за соблюдением работниками, уполномоченными на обработку персональных данных, требований законодательства Российской Федерации в области персональных данных, в том числе требований к защите персональных данных;

3) доводить до сведения работников, уполномоченных на обработку персональных данных, положения законодательства Российской Федерации в области персональных данных, локальных актов по вопросам обработки персональных данных, требования к защите персональных данных;

4) организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей, а также осуществлять контроль за приемом и обработкой таких обращений и запросов в Учреждении;

5) в случае нарушения в Учреждении требований к защите персональных данных принимать необходимые меры по восстановлению нарушенных прав субъектов персональных данных.

74. Ответственный за обработку персональных данных вправе:

1) иметь доступ к информации, касающейся обработки персональных данных в Учреждении и включающей:

цели обработки персональных данных;

категории обрабатываемых персональных данных;

категории субъектов персональных данных, персональные данные которых обрабатываются;

правовые основания обработки персональных данных;

перечень действий с персональными данными, общее описание используемых в Учреждении способов обработки персональных данных;

описание мер, предусмотренных статьями 18.1 и 19 Федерального закона «О персональных данных», в том числе сведения о наличии шифровальных (криптографических) средств и наименования этих средств;

дату начала обработки персональных данных;

срок или условия прекращения обработки персональных данных; сведения о наличии или об отсутствии трансграничной передачи персональных данных в процессе их обработки;

сведения об обеспечении безопасности персональных данных в соответствии с Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119;

2) привлекать к реализации мер, направленных на обеспечение безопасности персональных данных, обрабатываемых в Учреждении, иных работников Учреждения с возложением на них соответствующих обязанностей и закреплением ответственности.

75. Ответственный за обработку персональных данных несет ответственность за надлежащее выполнение функций по организации обработки персональных данных в Учреждении в соответствии с законодательством Российской Федерации.

Приложение № 2
к приказу МУ ДО СШОР № 3
им. В.И. Русанова
от 16.06.2023 № 90/1-од

Правила осуществления внутреннего контроля соответствия обработки персональных данных в муниципальном учреждении дополнительного образования «Спортивная школа олимпийского резерва № 3 им. В.И. Русанова» требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами

1. Настоящими Правилами определяются процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, основания, порядок, формы и методы проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.

2. В целях осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в Учреждении организовывается проведение периодических проверок условий обработки персональных данных на предмет соответствия Федеральному закону от 27 июля 2006 г. № 152-ФЗ «О персональных данных», принятым в соответствии с ним нормативным правовым актам и локальными актами Учреждения (далее - проверки).

3. Проверки проводятся в Учреждении на основании ежегодного плана (плановые проверки) или на основании поступившего в Учреждение письменного заявления о нарушениях правил обработки персональных данных (внеплановые проверки).

Ежегодный план проверок разрабатывается и утверждается комиссией Учреждения для осуществления внутреннего контроля соответствия обработки персональных данных требованиям, предусмотренным Федеральным законом «О персональных данных» (далее - Комиссия).

4. В плане по каждой проверке устанавливаются объект и предмет (тематика) внутреннего контроля, проверяемый период, срок проведения проверки, ответственные исполнители.

5. Состав Комиссии определяется приказом директора Учреждения, в котором также определяется периодичность осуществляемых проверок. В проведении проверки не может участвовать работник Учреждения, прямо или косвенно заинтересованный в ее результатах. В работе Комиссии, как постоянный член Комиссии, может участвовать лицо, ответственное за организацию обработки персональных данных в Учреждении, которое в рамках своих полномочий при проведении проверок дает пояснения по вопросам, связанным с объектом и предметом проверки.

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

7. Проведение проверки по письменному обращению заявителя организуется в течение 5 рабочих дней, начиная со дня, следующего за датой его поступления.

8. Срок проведения проверки не может превышать месяц со дня принятия решения о ее проведении.

9. 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. По результатам каждой проверки Комиссией проводится заседание. Решения, принятые на заседаниях Комиссии, оформляются протоколом и подписываются членами комиссии.

11. По существу поставленных в обращении (жалобе) вопросов Комиссия в течение 5 рабочих дней со дня окончания проверки дает письменный ответ заявителю.

12. Внутренний контроль соблюдения порядка доступа уполномоченных должностных лиц Учреждения в помещения, в которых ведется обработка персональных данных, вне проверок осуществляется лицом, ответственным за организацию обработки персональных данных в Учреждении.

Приложение № 3
к приказу МУ ДО СШОР № 3
им. В.И. Русанова
от 16.06.2023 № 90/1-од

Перечень автоматизированных информационных систем персональных данных в муниципальном учреждении дополнительного образования «Спортивная школа олимпийского резерва № 3 им. В.И. Русанова»

1. Автоматизированная информационная система «1С: Предприятие»,
2. Автоматизированная информационаая система «Удаленное рабочее место»,
3. Автоматизированная информационаая система СБиС «Электронная отчётность и документооборот».

Приложение № 4
к приказу МУ ДО СШОР № 3
им. В.И. Русанова
от 16.06.2023 № 90/1-од

Перечень должностей муниципального учреждения дополнительного образования «Спортивная школа олимпийского резерва № 3 имени В.И. Русанова», работа которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным

1. Директор.
2. Заместитель директора
3. Руководитель структурного подразделения
4. Главный бухгалтер
5. Бухгалтер
6. Юрисконсульт
7. Секретарь
8. Инструктор-методист
9. Старший инструктор-методист
10. Тренер-преподаватель
11. Старший тренер-преподаватель
12. Заведующий хозяйством

Приложение № 5
к приказу МУ ДО СШОР № 3
им. В.И. Русанова
от 16.06.2023 № 90/1-од

Перечень должностей работников муниципального учреждения дополнительного образования «Спортивная школа олимпийского резерва № 3 им. В.И. Русанова», ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных в случае обезличивания персональных данных

1. Директор
2. Заместитель директора
3. Руководитель структурного подразделения
4. Главный бухгалтер
5. Бухгалтер
6. Делопроизводитель
7. Инструктор-методист
8. Старший инструктор-методист

Приложение № 6
к приказу МУ ДО СШОР № 3
им. В.И. Русанова
от «__» _____ 202__ г. № ___

Типовое обязательство работника муниципального учреждения дополнительного образования «Спортивная школа олимпийского резерва № 3 им. В.И. Русанова», непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним трудового договора прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей

г. Ярославль «__» _____202__г.

1. Я,_____,
(указываются полностью: фамилия, имя, отчество (при его наличии) работника
_____,
МУДО СШОР № 3 им. В.И. Русанова, наименование должности, наименование и реквизиты документа,
_____,
удостоверяющего личность: серия, номер, дата выдачи, наименование органа и код подразделения органа
_____
(при его наличии), выдавшего документ)

Зарегистрированный (ая) по месту жительства по адресу:_____
_____
обязуюсь прекратить обработку персональных данных субъектов персональных данных, ставших известными мне в связи с исполнением трудовых обязанностей в МУДО СШОР № 3 им. В.И. Русанова, со дня расторжения со мной трудового договора.

2. Я уведомлен (а) о том, что в соответствии со статьей 7 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» персональные данные являются конфиденциальной информацией и я обязан(а) не раскрывать третьим лицам и не распространять персональные данные субъектов персональных данных, ставшие известными мне в связи с исполнением трудовых обязанностей в МУДО СШОР № 3 им. В.И. Русанова, без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

3. Ответственность, предусмотренная законодательством Российской Федерации за невыполнение указанных обязанностей, мне разъяснена.

4. Настоящее обязательство заполнено и подписано мною собственноручно.

_____ _____
(подпись) (инициалы, фамилия)

Приложение № 7
к приказу МУ ДО СШОР № 3
им. В.И. Русанова
от 16.06.2023 № 90/1-од

Типовая форма согласия на обработку персональных данных работников муниципального учреждения дополнительного образования «Спортивная школа олимпийского резерва № 3 им. В.И. Русанова», а также иных субъектов персональных данных

Я _____,
(фамилия, имя, отчество (при наличии)

зарегистрированный(ая) по адресу: _____
_____,
паспорт серия _____ №_____, выдан _____,
(дата)
_____
(кем выдан)

свободно, своей волей и в своем интересе даю согласие уполномоченным должностным лицам МУ ДО СШОР № 3 им. В.И. Русанова, расположенного по адресу: 150054, г. Ярославль, пр-кт, Ленина, д. 30 на обработку (любое действие (операцию) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (предоставление, доступ), обезличивание, блокирование, удаление, уничтожение) моих персональных данных, в том числе:

1) фамилия, имя, отчество (при наличии) (в том числе прежние фамилии, имена и (или) отчества (при наличии), дата, место и причина их изменения);

2) число, месяц, год рождения;

3) место рождения;

4) сведения об образовании (когда и какие образовательные, научные и иные организации окончил, номера документов об образовании, направление подготовки или специальность по документу об образовании, квалификация);

5) сведения об ученой степени, ученом звании;

6) адрес и дата регистрации (снятия с регистрационного учета) по месту жительства (месту пребывания), адрес фактического проживания;

7) номер контактного телефона и (или) сведения о других способах связи;

8) реквизиты документа, удостоверяющего личность (вид, серия, номер, когда и кем выдан);

9) реквизиты паспорта гражданина Российской Федерации, удостоверяющего личность гражданина Российской Федерации за пределами территории Российской Федерации (серия, номер, когда и кем выдан);

10) реквизиты страхового свидетельства обязательного пенсионного страхования;

11) идентификационный номер налогоплательщика;

12) отношение к воинской обязанности, сведения о воинском учете и реквизиты документов воинского учета;

13) сведения о семейном положении, составе семьи и о близких родственниках (в том числе бывших);

14) сведения о государственных наградах, иных наградах и знаках отличия;

15) сведения о наличии или отсутствии судимости;

16) реквизиты полиса обязательного медицинского страхования;

17) реквизиты свидетельств государственной регистрации актов гражданского состояния;

18) сведения об отсутствии у гражданина заболевания, препятствующего осуществления трудовой деятельности в учреждении;

19) номер расчетного счета (номера расчетных счетов), номер банковской карты (номера банковских карт), иные реквизиты для безналичной выплаты заработной платы;

20) биометрические персональные данные: цветное цифровое фотографическое изображение лица, полученное при приеме на работу, копия фотографического изображения лица, содержащаяся в паспорте; собственноручная подпись;

21) сведения о трудовой деятельности, в том числе: дата, основания поступления работу, дата, основания назначения, перевода, перемещения на иную должность, наименование Замещаемых должностей с указанием структурных подразделений, размера заработной платы, результатов аттестации, а также сведения о прежнем месте работы;

22) сведения, трудовом договоре, дополнительных соглашениях к трудовому договору;

23) сведения о профессиональной переподготовке и (или) повышении квалификации;

24) сведения о ежегодных оплачиваемых отпусках, учебных отпусках и отпусках без сохранения денежного содержания;

25) сведения о гражданстве

26) иные персональные данные в соответствии с законодательными и иными нормативными правовыми актами Российской Федерации.

Вышеуказанные персональные данные предоставляю для обработки в целях:_____

указать цель обработки (реализация трудовых отношений, договорных отношений, предоставления физкультурно-оздоровительных услуг и т. д.)

Я ознакомлен(а) с тем, что:

1) согласие на обработку персональных данных действует с даты подписания настоящего согласия в течение всего следующего срока: _____

(срока осуществления трудовой деятельности в учреждении, срока хранения документации, до отзыва согласия и т.д.)

2) согласие на обработку персональных данных может быть отозвано на основании письменного заявления в произвольной форме;

3) в случае отзыва согласия на обработку персональных данных учреждение вправе продолжить обработку персональных данных без согласия при наличииоснований, указанных в пунктах 2-9.1 и 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных";

4) после прекращения взаимоотношений с учреждением персональные данные будут храниться вучреждении в течение предусмотренного законодательством Российской Федерации срока хранения документов;

5) персональные данные, предоставляемые в отношении третьих лиц, будут обрабатываться только в целях осуществления и выполнения возложенных

законодательством Российской Федерации на учреждение функций, полномочий и обязанностей.

Дата начала обработки персональных данных:

_____

(число, месяц, года) (подпись)

Приложение № 8
к приказу МУ ДО СШОР № 3
им. В.И. Русанова
от 16.06.2023 № 90/1-од

Типовая форма согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения

Муниципальное учреждение дополнительного образования «Спортивная школа олимпийского резерва№ 3 им. В.И. Русанова» (МУ ДО СШОР № 3 им. В.И. Русанова)
(наименование оператора персональных данных)
ИНН 7606030535 **ОГРН** 1027600845293
Адрес: 150054, Ярославль, пр-кт Ленина, д.30

от _____
(фамилия, имя, отчество (при наличии) субъекта персональных данных)

номер телефона: _____
адрес электронной почты: _____
почтовый адрес: _____

Я, _____
фамилия, имя, отчество (при наличии)
в соответствии со ст. 9 и ст. 10.1 Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных" даю свое согласие
Муниципальному учреждению дополнительного образования спортивная школа олимпийского резерва№ 3 им. В.И. Русанова
на распространение (передачу, предоставление) своих персональных данныхс целью:
_____
указать цель

в следующем порядке:

Категории и перечень персональных данных, на обработку которых дается согласие:

N п/п	Персональные данные	Согласие	
		ДА	НЕТ
1. Общие персональные данные			

2. Специальные категории персональных данных			
3. Биометрические персональные данные			

Категории и перечень персональных данных, для обработки которых устанавливаются условия и запреты*:

N п/п	Персональные данные	Перечень устанавливаемых условий и запретов
1. [**Категория персональных данных**]		

***Примечание. Указанное поле заполняется по желанию субъекта персональных данных.**
Условия, при которых полученные персональные данные могут передаваться оператором, осуществляющим обработку персональных данных, только по его внутренней сети, обеспечивающей доступ к информации лишь для строго определенных сотрудников, либо с использованием информационно-телекоммуникационных сетей, либо без передачи полученных персональных данных.

Настоящее согласие действует:_____*
(указать срок действия согласия)

Примечание. Субъект персональных данных вправе отозвать данное согласие на обработку своих персональных данных, письменно уведомив об этом оператора.

«___» _____ 2021 г. _____ / _____ /
(подпись) расшифровка

Приложение № 9
к приказу МУ ДО СШОР № 3
им. В.И. Русанова
от 16.06.2023 № 90/1-од

Типовая форма разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные

г.Ярославль «___» _____202__г.

1. Мне,_____,
(указываются полностью фамилия, имя, отчество (при его наличии):

_____
реквизиты документа, удостоверяющего личность: серия, номер, дата выдачи, наименование органа и код подразделения органа (при его наличии), выдавшего документ)

_____,
зарегистрированному(ой) по месту жительства по адресу:_____
_____

разъяснены юридические последствия отказа предоставить свои персональные данные (далее - персональные данные) уполномоченным лицам МУ ДО СШОР № 3 им. В.И. Русанова, а равно подписать согласие на обработку персональных данных по типовой форме такого согласия, установленного в МУ ДО СШОР № 3 им. В.И. Русанова, или отзыва указанного согласия.

2. Я предупрежден(а) о том, что в случае моего отказа предоставить персональные данные МУ ДО СШОР № 3 им. В.И. Русанова не сможет осуществлять их обработку.

3. Мне также известно, что МУ ДО СШОР № 3 им. В.И. Русанова в целях реализации функций, полномочий и обязанностей в установленной сфере деятельности в соответствии с законодательством Российской Федерации, имеет право запрашивать мои персональные данные у третьих лиц, а также осуществлять их обработку без моего согласия при наличии оснований, указанных пунктах 2-9.1 и 11 части 1 статьи 6, части 2 статьи 10 и части2 статьи 11 Федерального закона от 27 июля 2006 г. № 152-ФЗ «Оперсональных данных».

4. Настоящее разъяснение заполнено и подписано мною собственноручно.

_____ _____
(подпись) (инициалы, фамилия)

Приложение № 10
к приказу МУ ДО СШОР № 3
им. В.И. Русанова
от 16.06.2023 № 90/1-од

Форма Акта
уничтожения документов или съемных носителей персональных данных

г. Ярославль «___» _____202__г.

Комиссия, наделенная полномочиями приказом №_____ от «___» _____202__г.

в составе:_____

_____

(должности, ФИО)

провела отбор документов и (или) съемных носителей персональных данных,не подлежащих дальнейшему хранению:

№ п/п	Дата	Наименование документа /учетный номер съемного носителя с персональными данными	Пояснения
1	2	3	4

Всего документов_____

(цифрами и прописью)
Всего съемных носителей _____
(цифрами и прописью)

На бумажных/съемных носителях уничтожена конфиденциальная информация путем:

_____

указать способ уничтожения, например, путем стирания ее на устройстве гарантированного уничтожения информации/механического уничтожения/сжигания и т. п.

Перечисленные носители информации уничтожены

_____

путем (разрезания, демонтажа и т.п.),

_____

измельчены и сданы для уничтожения предприятию по утилизацивторичного сырья

_____ _____

(наименование предприятия) дата

Председатель комиссии:
Члены комиссии:

Подписи Дата

УТВЕРЖДАЮ
Директор МУ ДО СШОР № 3
им. В.И. Русанова
_____ Н.А. Куликов
«16» 06 2023 г.

Инструкция по проведению мониторинга информационной безопасности и антивирусного контроля при обработке персональных данных в МУДО СШОР № 3 им. В.И. Русанова

1. Общие положения

1.1. Настоящая Инструкция устанавливает порядок планирования и проведения мониторинга информационной безопасности автоматизированных систем, обрабатывающих персональные данные, от несанкционированного доступа, распространения, искажения и утраты информации в МУ ДО СШОР № 3 им. В.И. Русанова

2. Виды мониторинга информационной безопасности

2.1. Мониторинг работоспособности аппаратных компонентов автоматизированных систем, обрабатывающих персональные данные, осуществляется в процессе их администрирования и при проведении работ по техническому обслуживанию оборудования.

Наиболее существенные компоненты системы, имеющие встроенные средства контроля работоспособности (серверы, активное сетевое оборудование), должны контролироваться постоянно в рамках работы администраторов соответствующих систем.

2.2. Мониторинг парольной защиты и контроль надежности пользовательских паролей предусматривают:

- установление сроков действия паролей (не более 6 месяцев);
- периодическую (не реже 1 раза в квартал) проверку пользовательских паролей на количество символов и очевидность с целью выявления слабых паролей, которые легко угадать или дешифровать с помощью специализированных программных средств (взломщиков паролей).

2.3. Мониторинг целостности программного обеспечения включает следующие действия:

- проверку контрольных сумм и цифровых подписей каталогов и файлов сертифицированных программных средств при загрузке операционной системы;
- обнаружение дубликатов идентификаторов пользователей;
- восстановление системных файлов администраторами систем с резервных копий.

2.4. Мониторинг попыток несанкционированного доступа осуществляется с использованием средств операционной системы и специальных программных средств и предусматривает:

- фиксацию неудачных попыток входа в систему в системном журнале;
- протоколирование работы сетевых сервисов;
- выявление фактов сканирования определенного диапазона сетевых портов в короткие промежутки времени с целью обнаружения сетевых анализаторов, изучающих систему и выявляющих ее уязвимости.

2.5. Мониторинг производительности автоматизированных систем, обрабатывающих персональные данные, производится по обращениям пользователей в ходе администрирования систем и проведения профилактических работ для выявления попыток несанкционированного доступа, повлекших существенное уменьшение производительности систем.

3. Порядок проведения системного аудита

3.1. Системный аудит производится ежеквартально и в особых ситуациях.

3.2. Системный аудит включает проведение обзоров безопасности, тестирование системы, контроль внесения изменений в системное программное обеспечение.

3.3. Обзоры безопасности проводятся с целью проверки соответствия текущего состояния систем, обрабатывающих персональные данные, уровню безопасности, удовлетворяющему требованиям политики безопасности.

3.4. Обзоры безопасности должны включать:

- отчеты о безопасности пользовательских ресурсов, включающие наличие повторяющихся пользовательских имен и идентификаторов, неправильных форматов регистрационных записей, пользователей без пароля, неправильной установки домашних каталогов пользователей и уязвимостей пользовательских окружений;
- проверку содержимого файлов конфигурации на соответствие списку для проверки;
- обнаружение изменений системных файлов со времени проведения последней проверки (контроль целостности системных файлов);
- проверку прав доступа и других атрибутов системных файлов (команд, утилит и таблиц);
- проверку правильности настройки механизмов аутентификации и авторизации сетевых сервисов;
- проверку корректности конфигурации системных и активных сетевых устройств (мостов, маршрутизаторов, концентраторов и сетевых экранов).

3.5. Активное тестирование надежности механизмов контроля доступа производится путем осуществления попыток проникновения в систему (с помощью автоматического инструментария или вручную).

3.6. Пассивное тестирование механизмов контроля доступа осуществляется путем анализа конфигурационных файлов системы.

Информация об известных уязвимостях извлекается из документации и внешних источников, затем осуществляется проверка конфигурации системы с целью выявления опасных состояний системы, т. е. таких состояний, в которых могут проявлять себя известные уязвимости. Если система находится в опасном состоянии, то с целью нейтрализации уязвимостей необходимо либо изменить конфигурацию системы (для ликвидации условий проявления уязвимости), либо установить программные коррекции, либо установить другие версии программ, в которых данная уязвимость отсутствует, либо отказаться от использования системного сервиса, содержащего данную уязвимость.

3.7. Внесение изменений в системное программное обеспечение осуществляется администраторами систем, обрабатывающих персональные данные, с обязательным документированием изменений в соответствующем журнале, уведомлением каждого сотрудника, которого касается изменение, разработкой планов действий в аварийных ситуациях для восстановления работоспособности системы, если внесенное в нее изменение вывело ее из строя.

4. Порядок антивирусного контроля

4.1. Для защиты серверов и рабочих станций необходимо использовать антивирусные программы:

- резидентные антивирусные мониторы, контролирующие подозрительные действия программ;
- утилиты для обнаружения и анализа новых вирусов.

4.2. К использованию допускаются только лицензионные средства защиты от вредоносных программ и вирусов или сертифицированные свободно распространяемые антивирусные средства.

4.3. При подозрении на наличие не выявленных установленными средствами защиты заражений следует использовать Live CD с другими антивирусными средствами.

4.4. Установка и настройка средств защиты от вредоносных программ и вирусов на рабочих станциях и серверах автоматизированных систем, обрабатывающих персональные данные, осуществляется администраторами соответствующих систем в соответствии с руководствами по установке приобретенных средств защиты.

4.5. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено администратором системы на отсутствие вредоносных программ и компьютерных вирусов. Непосредственно после установки (изменения) программного обеспечения рабочей станции должна быть выполнена антивирусная проверка.

4.6. Запуск антивирусных программ должен осуществляться автоматически по заданию, централизованно созданному с использованием планировщика задач (входящим в поставку операционной системы либо поставляемым вместе с антивирусными программами).

4.7. Антивирусный контроль рабочих станций должен проводиться ежедневно в автоматическом режиме. Если проверка всех файлов на дисках рабочих станций занимает неприемлемо большое время, то допускается проводить выборочную проверку загрузочных областей дисков, оперативной памяти, критически важных инсталлированных файлов операционной системы и загружаемых файлов по сети или с внешних носителей. В этом случае полная проверка должна осуществляться не реже одного раза

в неделю в период неактивности пользователя. Пользователям рекомендуется осуществлять полную проверку во время перерыва на обед путем перевода рабочей станции в соответствующий автоматический режим функционирования в запертом помещении.

4.8. Обязательному антивирусному контролю подлежит любая информация (исполняемые файлы, текстовые файлы любых форматов, файлы данных), получаемая пользователем по сети или загружаемая со съемных носителей (магнитных дисков, оптических дисков, флеш-накопителей и т. п.). Контроль информации должен проводиться антивирусными средствами в процессе или сразу после ее загрузки на рабочую станцию пользователя. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль.

4.9. Устанавливаемое (изменяемое) на серверы программное обеспечение должно быть предварительно проверено администратором системы на отсутствие компьютерных вирусов и вредоносных программ. Непосредственно после установки (изменения) программного обеспечения сервера должна быть выполнена антивирусная проверка.

4.10. На серверах систем, обрабатывающих персональные данные, необходимо применять специальное антивирусное программное обеспечение, позволяющее:

- осуществлять антивирусную проверку файлов в момент попытки записи файла на сервер;
- проверять каталоги и файлы по расписанию с учетом нагрузки на сервер.

4.11. На серверах электронной почты необходимо применять антивирусное программное обеспечение, обеспечивающее проверку всех входящих сообщений. В случае если проверка входящего сообщения на почтовом сервере показала наличие в нем вируса или вредоносного кода, отправка данного сообщения должна блокироваться. При этом должно осуществляться автоматическое оповещение администратора почтового сервера, отправителя сообщения и адресата.

4.12. На всех рабочих станциях и серверах необходимо организовать регулярное обновление антивирусных баз.

4.13. Администраторы систем должны проводить регулярные проверки протоколов работы антивирусных программ с целью выявления пользователей и каналов, через которые распространяются вирусы.

4.14. При обнаружении зараженных вирусом файлов администратор системы должен выполнить следующие действия:

- отключить от компьютерной сети рабочие станции, представляющие вирусную опасность, до полного выяснения каналов проникновения вирусов и их уничтожения;
- немедленно сообщить о факте обнаружения вирусов непосредственному начальнику с указанием предположительного источника (отправителя, владельца и т. д.) зараженного файла, типа зараженного файла, характера содержащейся в файле информации, типа вируса и выполненных антивирусных мероприятий.

5. Порядок анализа инцидентов

5.1. Если администратор системы, обрабатывающей персональные данные, подозревает или получил сообщение о том, что его система подвергается атаке или уже была скомпрометирована, то он должен установить:

- факт попытки несанкционированного доступа (НСД);
- продолжается ли НСД в настоящий момент;
- кто является источником НСД;
- что является объектом НСД;
- когда происходила попытка НСД;
- как и при каких обстоятельствах была предпринята попытка НСД;
- точка входа нарушителя в систему;
- была ли попытка НСД успешной;
- определить системные ресурсы, безопасность которых была нарушена;
- какова мотивация попытки НСД.

5.2. Для выявления попытки НСД необходимо:

- установить, какие пользователи в настоящее время работают в системе, на каких рабочих станциях;
- выявить подозрительную активность пользователей;
- проверить, что все пользователи вошли в систему со своих рабочих мест, и никто из них не работает в системе необычно долго;

- проверить, что никто из пользователей не выполняет подозрительных программ и программ, не относящихся к его области деятельности.

5.3. При анализе системных журналов администратору необходимо произвести следующие действия:

- проверить наличие подозрительных записей системных журналов, сделанных в период предполагаемой попытки НСД, включая вход в систему пользователей, которые должны бы были отсутствовать в этот период времени, входы в систему из неожиданных мест, в необычное время и на короткий период времени;
- проверить, не уничтожен ли системный журнал и нет ли в нем пробелов;
- просмотреть списки команд, выполненных пользователями в рассматриваемый период времени;
- проверить наличие исходящих сообщений электронной почты, адресованных подозрительным хостам;
- проверить наличие мест в журналах, которые выглядят необычно;
- выявить попытки получить полномочия суперпользователя или другого привилегированного пользователя;
- выявить наличие неудачных попыток входа в систему.

5.4. В ходе анализа журналов активного сетевого оборудования (мостов, переключателей, маршрутизаторов, шлюзов) необходимо:

- проверить наличие подозрительных записей системных журналов, сделанных в период предполагаемой попытки НСД;
- проверить, не уничтожен ли системный журнал и нет ли в нем пробелов;
- проверить наличие мест в журналах, которые выглядят необычно;
- выявить попытки изменения таблиц маршрутизации и адресных таблиц;
- проверить конфигурацию сетевых устройств с целью определения возможности нахождения в системе программы, просматривающей весь сетевой трафик.

5.5. Для обнаружения в системе следов, оставленных злоумышленником, в виде файлов, вирусов, троянских программ, изменения системной конфигурации необходимо:

- составить базовую схему того, как обычно выглядит система;
- провести поиск подозрительных файлов, скрытые файлы, имена файлов и каталогов, которые обычно используются злоумышленниками;
- проверить содержимое системных файлов, которые обычно изменяются злоумышленниками;
- проверить целостность системных программ;
- проверить систему аутентификации и авторизации.

5.6. В случае заражения значительного количества рабочих станций после устранения его последствий проводится системный аудит.

УТВЕРЖДАЮ
Директор МУ ДО СШОР № 3
им. В.И. Русанова
_____Н.А. Куликов
«16» 06 202_3_ г.

Функциональные обязанности
ответственного за организацию обработки персональных данных
в МУ ДО СШОР № 3 им. В.И. Русанова

Настоящая должностная инструкция разработана и утверждена в соответствии с положениями Трудового кодекса Российской Федерации и иных нормативно-правовых актов, регулирующих трудовые правоотношения.

1. Общие положения

1.1. Ответственный за организацию обработки персональных данных относится к категории специалистов и непосредственно подчиняется директору учреждения, его заместителям.

1.2. На должность ответственного за организацию обработки персональных данных назначается лицо, имеющее высшее профессиональное образование без предъявления требований к стажу работы или среднее профессиональное образование и стаж работы в должностях, замещаемых специалистами со средним профессиональным образованием, не менее двух лет.

1.3. Ответственный за организацию обработки персональных данных должен знать:

- законодательство Российской Федерации в области персональных данных основывается;
- порядок систематизации, учета и ведения документации с использованием современных информационных технологий;
- основы экономики, организации труда, производства и управления;
- средства вычислительной техники, коммуникаций и связи;
- правила и нормы охраны труда.

2. Должностные обязанности

Ответственный за организацию обработки персональных данных обязан:

2.1. Осуществлять внутренний контроль за соблюдением законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;

2.2. Доводить до сведения работников организации положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;

2.3. Организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.

2.4. Организовывать принятие правовых, организационных и технических мер для обеспечения защиты персональных данных, обрабатываемых в учреждении от неправомерного или случайного доступа к ним, их уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий.

2.5. В случае нарушения в МУ ДО СШОР № 3 им. В.И. Русанова требований к защите персональных данных принимать необходимые меры по восстановлению нарушенных прав субъектов персональных данных.

3. Права

Ответственный за организацию обработки персональных данных имеет право:

3.1. На все предусмотренные законодательством социальные гарантии.

3.2. Знакомиться с проектами решений руководства организации, касающимися его деятельности.

3.3. Вносить на рассмотрение руководства предложения по совершенствованию работы, связанной с обязанностями, предусмотренными настоящей инструкцией.

3.4. Подписывать и визировать документы в пределах своей компетенции.

3.5. Осуществлять взаимодействие с руководителями структурных служб организации, получать информацию и документы, необходимые для выполнения своих должностных обязанностей.

3.6. Вести переписку с организациями по вопросам, входящим в его компетенцию.

3.7. Требовать от руководства организации оказания содействия в исполнении своих должностных обязанностей и прав.

3.8. Повышать свою профессиональную квалификацию.

3.9. Другие права, предусмотренные трудовым законодательством.

4. Ответственность

Ответственный за организацию обработки персональных данных несет ответственность:

4.1. За неисполнение или ненадлежащее исполнение своих должностных обязанностей, предусмотренных настоящей должностной инструкцией, - в пределах, определенных действующим трудовым законодательством РФ;

4.2. За причинение материального ущерба работодателю - в пределах, определенных действующим трудовым и гражданским законодательством РФ;

4.3. За правонарушения, совершенные в процессе осуществления своей деятельности, - в пределах, определенных действующим административным, уголовным, гражданским законодательством РФ.

С Должностной инструкцией ознакомился _____/_____/.
«___» _____ 202 __ года.

Экземпляр данной должностной инструкции получил_____/_____/.
«___» _____202 __ года.

УТВЕРЖДАЮ
Директор МУ ДО СШОР № 3 им. В.И. Русанова
_____ Н.А.Куликов

ПОЛОЖЕНИЕ
о работе с персональными данными работников муниципального учреждения дополнительного образования «Спортивная школа олимпийского резерва № 3 им. В.И. Русанова»

1.Общие положения

1.1. Положение о работе с персональными данными работников муниципального учреждения дополнительного образования «Спортивная школа олимпийского резерва № 3 им. В.И. Русанова» (далее по тексту - Положение) разработано в соответствии с Конституцией РФ, Трудовым кодексом РФ, Федеральным законом «Об информации, информационных технологиях и о защите информации» №149-ФЗ от 27.07.2006 года, Федеральным законом «О персональных данных» № 152-ФЗ от 27.07.2006 года и другими определяющими случаи и особенности обработки персональных данных нормативно-правовыми актами.

1.2. Настоящее Положение определяет порядок работы (сбора, обработки, использования, хранения и т. д.) с персональными данными работников и гарантии конфиденциальности сведений о работнике, предоставленных работником работодателю.

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

1.4. Персональные данные работников относятся к категории конфиденциальной информации. Режим конфиденциальности персональных данных физических лиц снимается в случаях обезличивания или по истечении 50/75 лет срока хранения, если иное не определено законом[1].

1.5. Настоящее Положение является обязательным для исполнения всеми работниками муниципального учреждения дополнительного образования «Спортивная школа олимпийского резерва № 3 имени В.И. Русанова» (далее по тексту - оператор, работодатель, учреждение), имеющими доступ к персональным данным.

2. Получение и обработка персональных данных работников

2.1. Персональные данные работника - любая информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника.

2.2. Обработка персональных данных работника осуществляется исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, получении образования и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

2.3. Персональные данные работника работодатель получает непосредственно от работника.

Если персональные данные работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Работодатель обязан сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение.

---

[1] Здесь и далее срок хранения 50/75 лет означает, что указанные документы, законченные делопроизводством до 1 января 2003 года, хранятся 75 лет; законченные делопроизводством после 1 января 2003 года, хранятся 50 лет.

Работодатель вправе получать персональные данные работника от третьих лиц только при наличии письменного согласия работника или в иных случаях, прямо предусмотренных в законодательстве.

2.3. Работодатель не вправе требовать от работника представления информации о политических и религиозных убеждениях, сведений о частной жизни работника.

2.4. Работодатель не имеет права получать и обрабатывать сведения о работнике, относящиеся в соответствии с законодательством Российской Федерации в области персональных данных к специальным категориям персональных данных, за исключением случаев, предусмотренных Трудовым кодексом и другими федеральными законами;

2.5. Работодатель не имеет права получать и обрабатывать персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральными законами.

2.6. Работник обязан предоставить работодателю или его представителю комплекс достоверных, документированных персональных данных, состав которых установлен Трудовым кодексом РФ и иными федеральными законами. Работодатель проверяет достоверность сведений, сверяя данные, представленные работником, с имеющимися у работника документами.

2.7. При изменении персональных данных работник обязан в кратчайший срок уведомить работодателя о таких изменениях. В случае неуведомления работодателя об изменении персональных данных работник принимает на себя риск возможных неблагоприятных последствий.

2.8. По мере необходимости работодатель истребует у работника дополнительные сведения. Работник представляет требуемые сведения и в случае необходимости предъявляет документы, подтверждающие достоверность этих сведений.

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

2.10. Работники и их представители должны быть ознакомлены под роспись с документами работодателя, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области;

2.11. Работники не должны отказываться от своих прав на сохранение и защиту тайны в области персональных данных.

2.12. При сборе персональных данных оператор обязан предоставить субъекту персональных данных по его просьбе информацию, предусмотренную частью 7 статьи 14 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных».

2.13. Если предоставление персональных данных является обязательным в соответствии с федеральным законом, оператор обязан разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные.

2.14. Если персональные данные получены не от субъекта персональных данных, оператор, за исключением случаев, предусмотренных частью 4 статьи 18 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных», до начала обработки таких персональных данных обязан предоставить субъекту персональных данных следующую информацию:

1) наименование либо фамилия, имя, отчество и адрес оператора или его представителя;

2) цель обработки персональных данных и ее правовое основание;

3) предполагаемые пользователи персональных данных;

4) установленные Федеральным законом «О персональных данных» права субъекта персональных данных;

5) источник получения персональных данных.

2.15. Оператор освобождается от обязанности предоставить субъекту персональных данных сведения, предусмотренные частью 3 статьи 18 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных», в случаях, если:

1) субъект персональных данных уведомлен об осуществлении обработки его персональных данных соответствующим оператором;

2) персональные данные получены оператором на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных;

3) обработка персональных данных, разрешенных субъектом персональных данных для распространения, осуществляется с соблюдением запретов и условий, предусмотренных статьей 10.1 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»;

4) оператор осуществляет обработку персональных данных для статистических или иных исследовательских целей, для осуществления профессиональной деятельности журналиста либо научной, литературной или иной творческой деятельности, если при этом не нарушаются права и законные интересы субъекта персональных данных;

5) предоставление субъекту персональных данных сведений, предусмотренных частью 3 статьи 18 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных», нарушает права и законные интересы третьих лиц.

2.16. Обработка персональных осуществляется оператором с согласия субъекта персональных данных за исключением случаев, установленных Федеральными законами.

2.17. 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 предусматривает ответственность в соответствии с законодательством.

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

2.19. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя либо по запросу субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных оператор обязан осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки.

2.20. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных оператор обязан осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

2.21. В случае подтверждения факта неточности персональных данных оператор на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязан уточнить персональные данные либо обеспечить их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по

поручению оператора) в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

2.22. В случае выявления неправомерной обработки персональных данных, осуществляемой оператором или лицом, действующим по поручению оператора, оператор в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению оператора. В случае, если обеспечить правомерность обработки персональных данных невозможно, оператор в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

2.23. В случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных, оператор обязан с момента выявления такого инцидента оператором, уполномоченным органом по защите прав субъектов персональных данных или иным заинтересованным лицом уведомить уполномоченный орган по защите прав субъектов персональных данных:

1) в течение двадцати четырех часов о произошедшем инциденте, о предполагаемых причинах, повлекших нарушение прав субъектов персональных данных, и предполагаемом вреде, нанесенном правам субъектов персональных данных, о принятых мерах по устранению последствий соответствующего инцидента, а также предоставить сведения о лице, уполномоченном оператором на взаимодействие с уполномоченным органом по защите прав субъектов персональных данных, по вопросам, связанным с выявленным инцидентом;

2) в течение семидесяти двух часов о результатах внутреннего расследования выявленного инцидента, а также предоставить сведения о лицах, действия которых стали причиной выявленного инцидента (при наличии).

2.24. В случае достижения цели обработки персональных данных оператор обязан прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом «О персональных данных» или другими федеральными законами.

2.25. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных оператор обязан прекратить их обработку или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в срок, не превышающий тридцати дней с даты

поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом «О персональных данных» или другими федеральными законами.

2.26. В случае обращения субъекта персональных данных к оператору с требованием о прекращении обработки персональных данных оператор обязан в срок, не превышающий десяти рабочих дней с даты получения оператором соответствующего требования, прекратить их обработку или обеспечить прекращение такой обработки (если такая обработка осуществляется лицом, осуществляющим обработку персональных данных), за исключением случаев, предусмотренных пунктами 2 - 11 части 1 статьи 6, частью 2 статьи 10 и частью 2 статьи 11 Федерального закона «О персональных данных». Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления оператором в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

2.27. В случае отсутствия возможности уничтожения персональных данных в течение срока, указанного в пунктах 2.19 - 2.26 настоящего Положения, оператор осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

2.28. Персональные данные работника используются для целей, связанных с выполнением работником трудовых функций.

2.29. Работодатель использует персональные данные, в частности, для решения вопросов продвижения работника по службе, очередности предоставления ежегодного отпуска, выплаты пособия по временной нетрудоспособности и в связи с материнством, установления размера зарплаты, установления льгот, гарантий и компенсаций, исчисления и уплаты налогов и сборов.

На основании персональных данных работника решается вопрос о допуске его к информации, составляющей служебную или коммерческую тайну.

2.30. При принятии решений, затрагивающих интересы работника, работодатель не имеет права основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронного получения.

2.31. Работодатель также не вправе принимать решения, затрагивающие интересы работника, основываясь на данных, имеющих двоякое толкование. В случае если на основании персональных данных работника невозможно достоверно установить какой-либо факт, работодатель предлагает работнику представить письменные разъяснения.

2.32. Работодатели, работники и их представители должны совместно вырабатывать меры защиты персональных данных работников.

2.33. Для обеспечения выполнения обязанностей, предусмотренных законодательством о персональных данных, Работодатель назначает ответственного за организацию обработки персональных данных.

2.34. Работодатель при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие 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.

2.35. Работодатель осуществляет внутренний контроль и (или) аудит соответствия обработки персональных данных федеральному законодательству, требованиям к защите персональных данных, политике Работодателя в отношении обработки персональных данных, настоящему Положению.

2.36. Работодатель обязан ознакомить работников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику Работодателя в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучить указанных работников.

3. Передача персональных данных работников

3.1. Передача персональных данных субъекта персональных данных возможна только с его согласия или в случаях, предусмотренных законодательством.

3.2. При передаче персональных данных субъекта персональных данных оператор должен соблюдать следующие требования:

- не сообщать персональные данные третьей стороне без письменного согласия субъекта персональных данных, за исключением случаев, когда это необходимо в целях предупреждения угрозы его жизни и здоровью, а также в случаях, установленных федеральным законом;
- не сообщать персональные данные субъекта персональных данных в коммерческих целях без его письменного согласия;
- 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 это правило соблюдено. Лица, получающие персональные данные, обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется на обмен персональными данными в порядке, установленном федеральными законами;
- не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции;
- передавать персональные данные работника представителям работников в порядке, установленном трудовым законодательством, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.

3.3. 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.

3.4. В случае если лицо, обратившееся с запросом, не уполномочено федеральным законом или настоящим Положением на получение информации, относящейся к персональным данным работника, работодатель обязан отказать лицу в выдаче информации. Лицу, обратившемуся с

запросом, выдается уведомление об отказе в выдаче информации, копия уведомления подшивается в личное дело работника.

3.5. Персональные данные работника могут быть переданы представителям работников в порядке, установленном Трудовым кодексом РФ, в том объеме, в каком это необходимо для выполнения указанными представителями их функций.

4. Хранение персональных данных работников

4.1. Информация, относящаяся к персональным данным работника, хранится в его личном деле. Ведение личных дел возложено на работника, ответственного за ведение кадрового делопроизводства.

4.2. Личные дела и личные карточки хранятся в бумажном виде в папках, прошитые и пронумерованные по страницам. Личные дела и личные карточки находятся в методическом кабинете в специально отведенном шкафу, обеспечивающем защиту от несанкционированного доступа. В конце рабочего дня все личные дела и личные карточки передаются ответственному за ведение кадрового делопроизводства.

4.3. Персональные данные работников могут также храниться в электронном виде в локальной компьютерной сети. Доступ к электронным базам данных, содержащим персональные данные работников, обеспечивается двухступенчатой системой паролей: на уровне локальной компьютерной сети и на уровне баз данных. Пароли устанавливаются самостоятельно работниками учреждения, имеющим доступ к персональным данным работников.

4.4. Изменение паролей должно осуществляться работниками не реже одного раза в шесть месяцев.

4.5. В целях повышения безопасности по обработке, передаче и хранению персональных данных работников в информационных системах проводится их обезличивание. Для обезличивания персональных данных применяется метод введения идентификаторов, то есть замена части сведений персональных данных идентификаторами с созданием таблиц соответствия идентификаторов исходным данным.

4.6. Доступ к персональным данным работника имеют лица, включенные в перечень должностей Учреждения, работа которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным.

Указанные лица имеют доступ только к тем персональным данным, которые необходимы для выполнения конкретных функций.

Надзорно-контрольные органы имеют доступ к информации, содержащей персональные данные, исключительно в пределах своей компетенции.

4.7. Копировать и делать выписки из персональных данных работника разрешается исключительно в служебных целях с письменного разрешения руководителя организации, либо его заместителей.

4.8. Запросы на получение персональных данных работников, а также факты предоставления персональных данных по этим запросам регистрируются в Журнале регистрации входящих документов и Журнале регистрации исходящей документации.

5.Защита персональных данных

5.1. 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.

5.2. 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.

5.3. Защита персональных данных представляет собой процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и, в конечном счёте, обеспечивающий достаточно надёжную безопасность информации.

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

5.5. Электронные носители, содержащие файлы с персональными данными, должны быть защищены паролем.

5.6. Обеспечению защиты персональных данных способствуют следующие меры:

- порядок приёма, учёта и контроля деятельности посетителей;
- технические средства охраны, сигнализации, видеонаблюдения;
- порядок охраны территории, зданий, помещений;
- требования к защите информации при интервьюировании и собеседованиях.

5.7. Все лица, связанные с получением, обработкой и защитой персональных данных, в обязательном порядке подписывают обязательство о неразглашении персональных данных, к которым они имеют доступ.

5.8. По возможности персональные данные обезличиваются.

5.9. Для обеспечения защиты персональных данных работников необходимо соблюдать ряд мер:

- ограничение и регламентация состава работников, должностные и 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 законодательных и локальных актов, регламентирующих работу с персональными данными;
- наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;
- организация порядка уничтожения информации;
- своевременное выявление нарушения в работе с персональными данными;
- воспитательная и разъяснительная работа с сотрудниками по предупреждению утраты ценных сведений при работе с конфиденциальными документами;
- не допускается передача персональных данных по телефону или факсу;
- не допускается передача персональных данных работников с использованием социальных сетей и мессенджеров;
- при работе с электронной почтой запрещается пересылать в теле письма информацию, содержащую персональные данные граждан, также запрещается пересылать незащищенные паролем вложения, файлы (документы, архивы, массивы данных), содержащие персональные данные;
- работникам оператора запрещается распространять посторонним лицам сведения об обработке персональных данных, условиях и местах хранения носителей данной информации.
- своевременное выявление нарушения требований разрешительной системы доступа к конфиденциальной информации;
- использование антивирусной защиты;
- выполнение резервного копирования.

5.10. Личные дела могут выдаваться на рабочие места только руководителю учреждения, его заместителям, лицу, ответственному за ведение кадрового делопроизводства и в исключительных случаях с разрешения руководителя учреждения работникам бухгалтерии.

5.11. Все папки на электронных носителях, содержащие персональные данные работников, должны быть защищены паролем.

5.12. Для защиты конфиденциальноой информации создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лица, пытающегося совершить несанкционированный доступ и овладение информацией.

5.13. Работодатель должен осуществлять комплекс мероприятий по исключению несанкционированного доступа к информационным ресурсам с целью предотвращения овладения конфиденциальными сведениями, их использованием, а также видоизменения, уничтожения, внесения вирусов, подмены, фальсификации содержания, реквизитов документа и пр.

5.14. Под посторонними лицами понимаются любые лица, не имеющие непосредственного отношения к деятельности учреждения, посетители.

5.15. Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и мест хранения документов, дел и рабочих материалов в службе персонала.

6 . Права и обязанности субъектов персональных данных

6.1. В целях обеспечения защиты персональных данных, хранящихся у работодателя, работники имеют право на:

- полную информацию об их персональных данных и обработке этих данных;
- свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные работника, за исключением случаев, предусмотренных федеральными законами.
- определение своих представителей для защиты своих персональных данных;
- требование об исключении или исправлении неверных или неполных персональных данных, а также данных, полученных и обработанных с нарушением требований законодательства. При отказе работодателя исключить или исправить персональные данные работника он имеет право заявить в письменной форме работодателю о своем несогласии с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера работник имеет право дополнить заявлением, выражающим его собственную точку зрения;
- требование об извещении работодателем всех лиц, которым ранее были сообщены неверные или неполные персональные данные работника, обо всех произведенных в них исключениях, исправлениях или дополнениях;
- обжалование в суд любых неправомерных действий или бездействия работодателя при обработке и защите его персональных данных.
- сохранение и защиту своей личной и семейной тайны.

6.2. Работник вправе требовать от оператора уничтожения его персональных данных в случае, если персональные данные не являются необходимыми для заявленной цели обработки.

6.3. Сведения должны быть предоставлены субъекту персональных данных оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

6.4. В целях защиты частной жизни, личной и семейной тайны субъекты персональных данных не должны отказываться от своего права на обработку персональных данных только с их согласия, поскольку это может повлечь причинение морального, материального вреда.

6.5. Доступ к своим персональным данным предоставляется работнику или его законному представителю оператором при обращении либо при получении от него соответствующего запроса. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись субъекта персональных данных

или его законного представителя. Запрос может быть направлен в электронной форме и подписан электронной цифровой подписью в соответствии с законодательством Российской Федерации.

6.6. Работник имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

1) подтверждение факта обработки персональных данных оператором;

2) правовые основания и цели обработки персональных данных;

3) цели и применяемые оператором способы обработки персональных данных;

4) наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;

5) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

6) сроки обработки персональных данных, в том числе сроки их хранения;

7) порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом «О персональных данных»;

8) информацию об осуществленной или о предполагаемой трансграничной передаче данных;

9) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;

10) иные сведения, предусмотренные Федеральным законом «О персональных данных» или другими федеральными законами.

6.7. Право работника на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами, в том числе если:

1) обработка персональных данных, включая персональные данные, полученные в результате оперативно-разыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;

2) обработка персональных данных осуществляется органами, осуществившими задержание субъекта персональных данных по подозрению в совершении преступления, либо предъявившими субъекту персональных данных обвинение по уголовному делу, либо применившими к субъекту персональных данных меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством Российской Федерации случаев, если допускается ознакомление подозреваемого или обвиняемого с такими персональными данными;

3) обработка персональных данных осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;

4) доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц;

5) обработка персональных данных осуществляется в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

6.8. Работодатель обязан сообщить в порядке, предусмотренном статьей 14 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных», субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя

либо десяти рабочих дней с момента обращения либо получения оператором запроса субъекта персональных данных или его представителя. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления оператором в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

6.9. В случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или персональных данных субъекту персональных данных или его представителю при их обращении либо при получении запроса субъекта персональных данных или его представителя оператор обязан дать в письменной форме мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 «О персональных данных» или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий десяти рабочих дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса субъекта персональных данных или его представителя. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления оператором в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

6.10. Оператор обязан предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных. В срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, оператор обязан внести в них необходимые изменения. В срок, не превышающий семи рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, оператор обязан уничтожить такие персональные данные. Оператор обязан уведомить субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

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

Оператор не вправе раскрывать третьим лицам и распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

7.1. Работник учреждения, получающий для работы конфиденциальный документ, несёт единоличную ответственность за сохранность носителя и конфиденциальность информации.

7.2. Должностные лица, в обязанность которых входит ведение персональных данных физического лица, обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.

7.3. 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 – влечёт привлечение должностных лиц к административной ответственности.

7.4. 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 дисциплинарные взыскания, предусмотренные трудовым законодательством.

7.5. Лица, виновные в нарушении положений законодательства Российской Федерации в области персональных данных при обработке персональных данных работника, привлекаются к

дисциплинарной и материальной ответственности в порядке, установленном настоящим Кодексом и иными федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

7.6. Моральный вред, причиненный работнику вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных федеральным законодательством, а также требований к защите персональных данных подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных работником убытков.

Приложение:

Лист ознакомления работников с Положением о работе с персональными данными работников муниципального учреждения дополнительного образования «Спортивная школа олимпийского резерва № 3 имени В.И. Русанова»