Приложение № 2 к приказу
директора МАУ ДО
«ДЮСШ «Спринт»»
от 30.08.2022 № 57/1-ОД

ПРАВИЛА
осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных
Муниципального автономного учреждения дополнительного образования
«Детско-юношеская спортивная школа «Спринт»»
МАУ ДО «ДЮСШ «Спринт»»)

Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее – Правила) определяют порядок организации и осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в МАУ ДО «ДЮСШ «Спринт»» (далее – Учреждение).

1. Общие положения

1.1. Настоящими Правилами определяются процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных.

1.2. Настоящие Правила разработаны в соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее – Федеральный закон), постановлением Правительства Российской Федерации от 01 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

1.3. В настоящих Правилах используются основные понятия в значениях, определѐнных статьѐй 3 Федерального закона.

1.4. Внутренний контроль соответствия обработки персональных данных требованиям к защите персональных данных (далее – внутренний контроль) в Учреждении осуществляется с целью определения наличия несоответствий между требуемым уровнем защиты персональных данных и его фактическим состоянием, а также выработки мер по их устранению и недопущению в дальнейшем.

1.5. Внутренний контроль осуществляется ответственным за организацию обработки персональных данных, на соответствие обработки персональных данных в Учреждении требованиям к защите персональных данных (далее – комиссия) путѐм проведения проверок.

1.6. Внутренний контроль проводится в форме плановых и внеплановых проверок.

Плановые проверки соответствия обработки персональных данных установленным требованиям проводятся один раз в квартал в Учреждении. План проведения внутреннего контроля на очередной год формируется заместителем директора по ФСР до 10 декабря и утверждается директором Учреждения.

Сроки проведения плановых проверок доводятся до сведения проверяемых лиц не позднее, чем за 10 дней до начала проверки.

Проведение внеплановой проверки организуется заместителем директора по ФСР в течение 3-х рабочих дней с даты поступления письменного заявления субъекта персональных данных о нарушении правил обработки персональных данных.

Внеплановые проверки могут быть контрольными и по частным вопросам:

1.6.1. Контрольные проверки проводятся для установления полноты выполнения рекомендаций плановых проверок.

Сроки проведения контрольных проверок доводятся до сведения проверяемых лиц не позднее, чем за 24 часа до начала проверки;

1.6.2. Проверки по частным вопросам охватывают отдельные направления по защите персональных данных и могут проводиться в случаях, когда стали известны факты несанкционированного доступа, утечки либо утраты персональных данных субъектов персональных данных Учреждения или нарушения требований по защите персональных данных.

Проверки по частным вопросам могут проводиться без уведомления проверяемых лиц.

2. Порядок подготовки к проверке

2.1. За 3-4 дня до начала проверки ответственный за организацию обработки персональных данных должен изучить материалы предыдущих проверок, уточнить наличие защищаемых ресурсов, сил и средств защиты персональных данных, а также особенности их функционирования.

3. Порядок проведения проверки

3.1. На период проведения контрольных мероприятий обработку персональных данных необходимо по возможности прекращать.

3.2. В ходе осуществления контроля выполнения требований по защите персональных данных в Учреждении проверке могут подлежать следующие показатели:

3.2.1. В части общей организации работ по защите персональных данных:

- соответствие информации, указанной в уведомлении об обработке персональных данных, реальному положению дел;

- наличие нормативных документов по защите персональных данных;

- знание нормативных документов сотрудниками, имеющими доступ к персональным данным;

- полнота и правильность выполнения требований нормативных документов сотрудниками, имеющими доступ к персональным данным;

- выполнение обязанностей сотрудников, имеющими доступ к персональным данным;

- наличие согласий на обработку персональных данных субъектов персональных данных. Соответствие объѐма персональных данных и сроков обработки целям обработки персональных данных;

- соответствие схемы контролируемой зоны, перечня мест хранения материальных носителей, перечня лиц, допущенных к обработке персональных данных, фактическому состоянию;

3.2.2. В части защиты персональных данных в информационных системах персональных данных (далее – ИСПДн):

- соответствие средств вычислительной техники ИСПДн показателям, указанным в документации на ИСПДн;

- структура и состав локальных вычислительных сетей, организация разграничения доступа пользователей к сетевым информационным ресурсам, порядок защиты охраняемых сведений при передаче (обмене) персональных данных в сети передачи данных (СПД);

- контроль целостности пломб на аппаратных средствах, с которыми осуществляется штатное функционирование средств криптографической защиты информации;

- соблюдение установленного порядка использования средств вычислительной техники ИСПДн;

- наличие и эффективность применения средств и методов защиты персональных данных, обрабатываемых на средствах электронно-вычислительной техники (ЭВТ);

- соблюдение требований, предъявляемых к паролям на информационные ресурсы;

- соблюдение требований и правил антивирусной защиты персональной электронно-вычислительной машины (ПЭВМ) и программ;

- тестирование реализации правил фильтрации межсетевого экрана, процесса регистрации, процесса идентификации и аутентификации запросов, процесса идентификации и аутентификации администратора межсетевого экрана, процесса регистрации действий администратора межсетевого экрана, процесса контроля за целостностью программной и информационной части, процедуры восстановления настроек межсетевого экрана;

3.2.3. В части защиты информационных ресурсов и помещений:

- правильность отнесения обрабатываемой информации к персональным данным;

- правильность классификации информационной системы;

- закрепление гражданско-правовой ответственности в сфере информационной безопасности и соблюдения режима конфиденциальности персональных данных в правилах внутреннего трудового распорядка, положениях, должностных инструкциях сотрудников и трудовых договорах;

- порядок передачи персональных данных органам государственной власти, местного самоуправления и сторонним организациям (контрагентам);

- действенность принимаемых мер по защите охраняемых сведений в ходе подготовки материалов к открытому опубликованию и при изготовлении буклетов;

- состояние конфиденциального делопроизводства, соблюдение установленного порядка подготовки, учѐта, использования, хранения и уничтожения документов, содержащих персональные данные; - выполнение требований по правильному оборудованию защищаемых помещений и предотвращению утечки охраняемых сведений при проведении мероприятий конфиденциального характера;

- соответствие защищаемых помещений их техническим паспортам.

3.3. Ответственный за организацию обработки персональных данных при проверке имеет право:

3.3.1. Запрашивать у руководителей, заместителя директора по ФСР Учреждения информацию и (или) документы, необходимые для осуществления внутреннего контроля;

3.3.2. Требовать от уполномоченных на обработку персональных данных должностных лиц уточнения, блокирования или уничтожения недостоверных или полученных незаконным путѐм персональных данных.

3.4. Проверка должна быть завершена не позднее чем через 15 дней с даты начала проверки.

3.5. В ходе работы проверяющий должен принимать меры по устранению на месте отмечаемых нарушений и недостатков. Для этого с должностными лицами, ответственными за конкретные участки работы, где отмечались недостатки, одновременно должны проводиться разъяснения требований руководящих документов и оказываться практическая помощь в правильной постановке работы.

Недостатки, которые не могут быть устранены на месте, включаются в итоговый документ по результатам проверки.

4. Оформление результатов проверки

4.1. Результаты проверки оформляются в виде акта внутреннего контроля, составленного по форме согласно Приложению к настоящим Правилам. Акт составляется в двух экземплярах, подписывается ответственным, докладывается под роспись руководителю Учреждения.

4.2. Один экземпляр документа хранится у ответственного за организацию обработки персональных данных в Учреждении. Второй экземпляр документа передаѐтся непосредственному руководителю.

4.3 В случае несогласия с выводами непосредственный руководитель может выразить в письменном виде своѐ особое мнение (прилагается к акту).

4.4. Результаты проверок периодически обобщаются ответственным и доводятся до сведения руководителя. При необходимости принятия решений по результатам проверок, о мерах, необходимых для устранения выявленных нарушений, директору Учреждения ответственным готовится соответствующая служебная записка.

Приложение № 1

с. Викулово «__» ___ 20___г

Акт
внутреннего контроля соответствия обработки персональных данных в Учреждении требованиям к защите персональных данных

Результаты рассмотрения вопросов по предметам контроля:

Предмет контроля	Результат рассмотрения	Примечание
Документы, определяющие основания обработки персональных данных в Учреждении		
Утвержденные списки должностных лиц доступ которых к персональным данным, обрабатываемым в информационных системах, необходим для выполнения ими трудовых обязанностей		
Утвержденные перечни информационных систем персональных данных, эксплуатируемых в Учреждении		
Своевременность мероприятий по уничтожению либо обезличиванию персональных данных, обрабатываемых в Учреждении в связи с достижением целей обработки или утраты необходимости в достижении этих целей		
Условия хранения и состояние учета машинных носителей персональных данных		
Порядок и условия применения средств защиты информации при наличии таковых		
Соблюдение требований к паролям доступа		
Отсутствие неправомерно размещенных персональных данных граждан в закрепленных за Учреждением разделах официального сайта		

Ответственный за организацию обработки персональных данных:

_____ /_____/

Ознакомлены: