Департамент образования мэрии города Новосибирска

муниципальное автономное учреждение дополнительного образования города Новосибирска «Детско-юношеский центр «Планетарий» имени космонавта Анны Кикиной»

630114, г. Новосибирск, ул. Ключ-Камышенское плато, 1/1
ОГРН 1115476113818 ОКПО 30743690, ИНН/КПП 5405442038/540501001
Тел. 347-77-07, e-mail: dyuc_planeta@edu54.ru

Приложение № 4
к приказу от 02.11.2023 № 66/01-02

СОГЛАСОВАНО:
Председатель первичной профсоюзной организации МАУ ДО ДЮЦ «Планетарий» имени космонавта Анны Кикиной
_____ Е.В. Зейналова
«2» ноября 2023г.

УТВЕРЖДЕНО:
приказом от «2» ноября 2023г. № 66/01-02
Директор МАУ ДО ДЮЦ «Планетарий» имени космонавта Анны Кикиной
_____ Т.А. Белоусова

П О Л О Ж Е Н И Е

о внутреннем контроле и (или) аудите соответствия обработки персональных данных в МАУ ДО ДЮЦ «Планетарий» имени космонавта Анны Кикиной требованиям законодательства в сфере обработки персональных данных

г. Новосибирск, 2023г.

П О Л О Ж Е Н И Е
о внутреннем контроле и (или) аудите соответствия обработки персональных данных в МАУ ДО ДЮЦ «Планетарий» имени космонавта Анны Кикиной требованиям законодательства в сфере обработки персональных данных

1. Общие положения

1.1. Настоящее Положение о внутреннем контроле и (или) аудите соответствия обработки персональных данных в МАУ ДО ДЮЦ «Планетарий» имени космонавта Анны Кикиной требованиям законодательства в сфере обработки персональных данных (далее – Положение) разработано в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

1.2. Положение определяет порядок осуществления внутреннего контроля соответствия обработки персональных данных в МАУ ДО ДЮЦ «Планетарий» имени космонавта Анны Кикиной (далее – учреждение) требованиям к защите персональных данных, установленным законодательством Российской Федерации.

1.3. Исполнение Положения обязательно для всех работников учреждения, осуществляющих обработку персональных данных, как без использования средств автоматизации, так и в информационных системах обработки персональных данных.

1.4. В Положении используются основные понятия в значениях, определенных статье 3 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

Внутренний контроль соответствия обработки персональных данных – контроль соответствия обработки персональных данных в учреждении требованиям законодательства в сфере обработки персональных данных, проводимый силами учреждения в соответствии с Положением и другими локальными нормативными актами организации.

Внутренний аудит соответствия обработки персональных данных – контроль соответствия обработки персональных данных в учреждении требованиям законодательства в сфере обработки персональных данных, проводимый специализированными организациями, привлекаемыми учреждением по договорам оказания услуг в соответствии с Положением и другими локальными нормативными актами организации.

2. Порядок проведения внутреннего контроля

2.1. Внутренний контроль соответствия обработки персональных данных осуществляется комиссией по плану мероприятий внутреннего контроля, утверждаемому ежегодно директором учреждения.

2.2. Мероприятия внутреннего контроля могут быть внеплановыми по решению комиссии, если есть фактические основания полагать, что процедура обработки персональных данных в учреждении не соответствует требованиям законодательства Российской Федерации. Порядок проведения внепланового контроля совпадает с порядком проведения планового контроля.

2.3. Состав комиссии утверждается директором учреждения.

2.4. Мероприятия внутреннего контроля могут осуществляться как непосредственно на рабочих местах исполнителей, участвующих в обработке персональных данных, так и путем направления запросов и рассмотрения документов, необходимых для осуществления внутреннего контроля.

2.5. При проведении внутреннего контроля должен присутствовать начальник проверяемого отдела (подразделения).

2.6. В ходе проведения внутреннего контроля осуществляется:

- контроль выполнения организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн, необходимых для выполнения требований к защите ПДн;
- анализ изменения угроз безопасности ПДн в ИСПДн, возникающих в ходе ее эксплуатации;
- проверка параметров настройки и правильности функционирования программного обеспечения и средств защиты информации (далее – СЗИ);
- контроль состава технических средств, программного обеспечения и СЗИ;
- состояние учета СЗИ;
- состояние учета средств шифровальной (криптографической) защиты информации;
- состояние учета съемных машинных носителей ПДн;
- соблюдение правил доступа к ПДн;
- контроль наличия (отсутствия) фактов несанкционированного доступа к ПДн;
- соблюдение пользователями ИСПДн парольной политики;
- соблюдение пользователями ИСПДн антивирусной политики;
- соблюдение пользователями ИСПДн правил работы со съемными машинными носителями ПДн;

- контроль соблюдения работниками требований локальных нормативных актов, в т.ч. требований законодательства по вопросам обработки и защиты ПДн;

- выявление уязвимостей в ИСПДн с использованием специализированных средств инструментального анализа защищенности.

2.7. При проведении мероприятия внутреннего контроля должны быть полностью, объективно и всесторонне установлены:

- порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;

- порядок и условия применения средств защиты информации;

- эффективность принимаемых мер по обеспечению безопасности персональных данных;

- состояние учета машинных носителей персональных данных;

- соблюдение правил доступа к персональным данным;

- наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер;

- мероприятия по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

- осуществление мероприятий по обеспечению целостности персональных данных.

2.8. Комиссия при проведении внутреннего контроля имеет право:

- запрашивать у работников, осуществляющих обработку персональных данных, информацию и (или) документы, необходимые для осуществления внутреннего контроля;

- требовать у ответственных за обработку персональных данных уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;

- принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства Российской Федерации;

- вносить предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке в учреждении;

- вносить предложения о привлечении к дисциплинарной ответственности работников, виновных в нарушении законодательства Российской Федерации в отношении обработки персональных данных.

2.9. В отношении персональных данных, ставших известными в ходе проведения мероприятий внутреннего контроля, должна обеспечиваться конфиденциальность.

2.10. Мероприятие внутреннего контроля не может длиться больше 10 рабочих дней. Срок мероприятия может быть продлен распорядительным актом директора учреждения при наличии оснований, не позволяющих закончить контрольное мероприятие за 10 рабочих дней.

2.11. При выявлении в ходе планового/внепланового контроля нарушений требований по обработке и защите персональных данных осуществляется оперативное устранение выявленных нарушений.

2.12. Выявленные нарушения должны быть устранены в срок не превышающий 30 дней с момента утверждения Акта о проведении внутреннего контроля.

2.13. По истечению срока, данного на устранение замечаний, комиссия проводит повторный контроль.

3. Оформление итогов внутреннего контроля

3.1. Результаты внутреннего контроля соответствия обработки персональных данных оформляются комиссий в виде акта внутреннего контроля, составленного по форме согласно Приложению № 1 к Положению. Члены комиссии обязаны составлять докладные записки по итогам контрольных мероприятий, если это предусматривает план мероприятий внутреннего контроля или распорядительный акт директора учреждения.

3.2. Акт внутреннего контроля подписывается всеми членами комиссии.

3.3. В акте внутреннего контроля указываются:

- перечень проведенных мероприятий;
- выявленные нарушения;
- мероприятия по устранению нарушений;
- решения по результатам внутреннего контроля;
- сроки устранения нарушений.

3.4. Выявленные в ходе внутреннего контроля нарушения фиксируются в акте внутреннего контроля с предложениями мероприятий по устранению нарушений и сроков их выполнения.

3.5. О результатах внутреннего контроля и мерах, необходимых для устранения выявленных нарушений, по мере необходимости комиссия

докладывает на очередном совещании при директоре учреждения, если иное не установлено распорядительным актом директора.

3.6. Акты внутреннего контроля, докладные записки по итогам контрольных мероприятий хранятся в запирающемся шкафу в кабинете бухгалтерии.

4. Порядок проведения внутреннего аудита

4.1. Внутренний аудит соответствия обработки персональных данных проводится в случаях, когда учреждение не может объективно оценить соответствие обработки персональных данных в учреждении требованиям законодательства в сфере обработки персональных данных.

4.2. Внутренний аудит организуется на основании распорядительного акта директора учреждения.

4.3. Внутренний аудит проводит организация, которая в соответствии со своими учредительными документами занимается оценкой рисков в обработке персональных данных и возможного вреда, который может быть причинен субъектам персональных данных в случае нарушения требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

4.4. На время проведения внутреннего аудита директор учреждения назначает ответственного, который должен взаимодействовать с организацией, проводящей аудит (далее – аудитор).

4.5. Ответственный обязан:

- обеспечить аудитора всей необходимой информацией;
- организовать условия для работы;
- оказывать помощь при возникновении трудностей;
- контролировать работу аудитора;
- принимать все отчеты аудитора и доводить их до сведения директора учреждения.

4.6. Действия и обязанности аудитора определяются заключенным договором оказания услуг по проведению внутреннего аудита.

4.7. Документы внутреннего аудита, в том числе итоговые отчеты, хранятся в запирающемся шкафу в кабинете бухгалтерии.

5. Срок действия и порядок внесения изменений

5.1. Порядок ввода в действие и изменения Положения:

5.1.1. Настоящее Положение вступает в силу с момента его утверждения директором Учреждения и действует бессрочно, до замены его новым Положением.

5.1.2. Все изменения в Положение вносятся приказом директора.

Приложение №1
к Положению о внутреннем контроле и (или) аудите
соответствия обработки персональных данных
в МАУ ДО ДЮЦ «Планетарий» имени космонавта Анны Кикиной
требованиям законодательства в сфере обработки персональных данных

Акт
№ ___ от «__» _____ 202_г.
внутреннего контроля соответствия обработки персональных данных в МАУ ДО ДЮЦ «Планетарий» имени космонавта Анны Кикиной требованиям законодательства в сфере обработки персональных данных

Комиссия, наделенная полномочиями приказом директора от «__» _____ 202_г. № _____, «О создании комиссии и проведении внутреннего контроля работы с персональными данными», в составе:

Председателя:

_____ _____

Членов комиссии:

1. _____ _____
2. _____ _____
3. _____ _____

провела внутренний контроль соответствия обработки персональных данных в МАУ ДО ДЮЦ «Планетарий» имени космонавта Анны Кикиной (далее – учреждение) требованиям законодательства в сфере обработки персональных данных в соответствии с планом внутреннего контроля на 202_/202_ год (учебный год).

В ходе контрольных мероприятий проверены:

- документы, определяющие основания обработки персональных данных;
- утвержденный перечень работников учреждения, имеющих доступ к персональным данным в силу своих служебных обязанностей;
- своевременность мероприятий по уничтожению либо обезличиванию персональных данных, обрабатываемых в учреждении, в связи с достижением целей обработки или утраты необходимости в достижении этих целей;
- отсутствие неправомерно размещенных персональных данных граждан на сайте учреждения и иных общедоступных местах;
- <…>…

Выявленные нарушения:

1. Политика обработки персональных данных МАУ ДО ДЮЦ «Планетарий» имени космонавта Анны Кикиной не соответствует требованиям законодательства – нет положений о согласии на обработку персональных данных, разрешенных субъектом персональных данных для распространения.
2. <…>

Меры по устранению нарушений:

1. Необходимо внести изменения в Политику обработки персональных данных МАУ ДО ДЮЦ «Планетарий» имени космонавта Анны Кикиной и привести нормы о согласии на обработку персональных данных в соответствие с действующим законодательством.
2. <…>

Срок устранения нарушений: «__» _____ 202_г.

Ответственный за исполнение: _____

Правильность произведенных записей в акте проверена.

Подписи членов комиссии:

Председатель:

_____ _____ _____

Члены комиссии:

_____ _____ _____

_____ _____ _____

_____ _____ _____


Всего прошито, пронумеровано
и скреплено печатью
8 (восемь) листов
цифрами прописью
Должность директор
Подпись
« 2 » ноября 20
МП