ИНСТИТУТ ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
INSTITUTE OF PROFESSIONAL EDUCATION
115114, г. Москва, Дербеневская набережная, д. 11 Тел.: (495) 120-79-01
Научная автономная некоммерческая организация «Институт профессионального образования»
Р/с 40703810338000016474 в ПАО СБЕРБАНК, к/с 30101810400000000225, БИК 044525225
ИНН 9725024950 КПП 772501001 ОКАТО 45296559000 ОКПО 42319365 ОКВЭД 72.20 ОГРН 1197700016623

ПРИКАЗ

г. Москва

«29» декабря 2022 г. № 3-ПД

Об внутреннем контроле и (или) аудите
соответствия обработки персональных данных
в Научной автономной некоммерческой организации «Институт профессионального образования»
(*далее- НАНО «ИПО») требованиям законодательства*
в сфере обработки персональных данных

В соответствии с п. 4 части 1 ст. 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», **приказываю:**

1. Утвердить Положение о внутреннем контроле и (или) аудите соответствия обработки персональных данных в НАНО «ИПО» требованиям законодательства в сфере обработки персональных данных (Приложение 1).

2. Создать и утвердить комиссию по проверке обработки персональных данных в НАНО «ИПО» в следующем составе: председатель комиссии: Ильин А.А.

Члены комиссии: Арбузова А.А.

Акматалиева А.

3. Утвердить План-график внутреннего контроля работы с персональными данными (Приложение 2)

4. Комиссии по проведению внутреннего контроля соответствия обработки персональных данных:

- провести мероприятия внутреннего контроля в соответствии с Планом-графиком, указанным в пункте 3 настоящего приказа, и положением о внутреннем контроле и (или) аудите соответствия обработки персональных данных в НАНО «ИПО» требованиям законодательства в сфере обработки персональных данных;

- представить итоги внутреннего контроля в срок, указанный в Плане-графике мероприятий внутреннего контроля соответствия обработки персональных данных на 2022 год.

5. Ректору НАНО «ИПО», Бородиной М.И., ознакомить с настоящим приказом работников под роспись в срок до 29 января 2023 г.

6. Контроль за исполнением настоящего Приказа оставляю за собой.

Ректор
НАНО «ИПО» Бородина М.И.

М.П.

Приложение
к приказу НАНО «ИПО»
от «29» декабря 2022 г. № 3-ПД

Положение о внутреннем контроле и (или) аудите соответствия обработки персональных данных в НАНО «ИПО» 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 НАНО «ИПО» 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 НАНО «ИПО» (далее – образовательная организация) требованиям к защите персональных данных, установленным законодательством Российской Федерации.

1.3. Исполнение Положения обязательно для всех работников образовательной организации, 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 образовательной организации требованиям законодательства в сфере обработки персональных данных, проводимый силами образовательной организации в соответствии с Положением и другими локальными нормативными актами организации. Внутренний аудит соответствия обработки персональных данных – контроль соответствия обработки персональных данных в образовательной организации требованиям законодательства в сфере обработки персональных данных, проводимый специализированными организациями, привлекаемыми образовательной организацией по договорам оказания услуг в соответствии с 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 Ректором образовательной организации.

2.2. Мероприятия внутреннего контроля могут быть внеплановыми по решению комиссии, если есть фактические основания полагать, что процедура обработки персональных данных в образовательной организации не соответствует требованиям законодательства Российской Федерации.

2.3. Состав комиссии утверждается Ректором образовательной организации.

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 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.

2.6. 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 образовательной организации;

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

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

2.8. Мероприятие внутреннего контроля не может длиться больше 10 рабочих дней. Срок мероприятия может быть продлен распорядительным актом Ректора образовательной организации при наличии оснований, не позволяющих закончить контрольное мероприятие за 10 рабочих дней.

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 к Положению. Члены комиссии обязаны составлять докладные записки по итогам контрольных мероприятий, если это предусматривает план мероприятий внутреннего контроля или распорядительный акт Ректора образовательной организации.

3.2. Акт внутреннего контроля подписывается всеми членами комиссии.

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

3.4. О результатах внутреннего контроля и мерах, необходимых для устранения выявленных нарушений, по мере необходимости комиссия докладывает на очередном совещании при Ректоре образовательной организации, если иное не установлено локальными актами образовательной организации.

3.5. Акты внутреннего контроля, докладные записки по итогам контрольных мероприятий хранятся в запирающемся шкафу в кабинете 47 образовательной организации.

4. Порядок проведения внутреннего аудита

4.1. Внутренний аудит соответствия обработки персональных данных проводится в случаях, когда образовательная организация не может объективно оценить соответствие обработки персональных данных в образовательной организации требованиям законодательства в сфере обработки персональных данных.

4.2. Внутренний аудит организуется на основании распорядительного акта руководителя образовательной организации.

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 руководитель образовательной организации 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 Ректора образовательной организации.

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 руководителя образовательной организации.

Приложение № 1
к Положению о внутреннем контроле и (или) аудите
соответствия обработки персональных данных
в НАНО «ИПО» требованиям
законодательства в сфере обработки
персональных данных

АКТ
Внутреннего контроля соответствия обработки персональных данных
в НАНО «ИПО» требованиям законодательства
в сфере обработки персональных данных

г. Москва

«13» октября 2023 г . № 1

Комиссия НАНО «ИПО» в составе:
Ильин А.А.
Арбузова А.А.
Акматалиева А.
провела внутренний контроль соответствия обработки персональных данных в НАНО «ИПО» требованиям законодательства в сфере обработки персональных данных в соответствии с планом внутреннего контроля на 2022/2023 учебный год, утвержденным приказом Ректора НАНО «ИПО» от 29 декабря 2022г. № 3-ПД.
В ходе контрольных мероприятий проверены:

- документы, определяющие основания обработки персональных данных;
- утвержденный перечень работников НАНО «ИПО», имеющих доступ к персональным данным в силу своих служебных обязанностей;
- своевременность мероприятий по уничтожению либо обезличиванию персональных данных, обрабатываемых в НАНО «ИПО», в связи с достижением целей обработки или утраты необходимости в достижении этих целей;
- отсутствие неправомерно размещенных персональных данных граждан на сайте НАНО «ИПО» и иных общедоступных местах;
- анализ содержания сайта НАНО «ИПО».

Выявленные нарушения:

1. На сайте НАНО «ИПО» не определено предоставление пользователям сайта НАНО «ИПО» согласия на обработку персональных посредством метрических программ Яндекс. Метрика, GoogleAnalitics.
2. Не своевременно проведены мероприятия по уничтожению персональных данных, обрабатываемых в НАНО «ИПО».
3. На сайте НАНО «ИПО» не размещена политика оператора в отношении обработки персональных данных.
4. В согласии на обработку персональных данных, размещённом на сайте НАНО «ИПО», не указан способ отзыва указанного согласия, а также перечень обрабатываемых персональных данных и лиц, которым персональные данные передаются.

Меры по устранению нарушений:

1. Необходимо разместить на сайте НАНО «ИПО» Политику конфиденциальности, а также, согласие на обработку персональных пользователей сайта НАНО «ИПО» посредством метрических программ Яндекс. Метрика, GoogleAnalitics.
2. Необходимо провести мероприятия по уничтожению персональных данных, обрабатываемых в НАНО «ИПО» согласно Политике в отношении обработки персональных данных и действующему законодательству Российской Федерации в отношении обработки персональных данных.
3. Необходимо разместить на сайте НАНО «ИПО» политику оператора в отношении обработки персональных данных.
4. Необходимо заменить на сайте НАНО «ИПО» согласие на обработку персональных данных на

актуальное.

Срок устранения нарушений: 20 октября 2023 г.

Ответственный за исполнение: Ильин А.А.

Подписи членов комиссии:_____
_____
_____

Приложение № 2
к Положению о внутреннем контроле и (или) аудите
соответствия обработки персональных данных
в НАНО «ИПО» требованиям
законодательства в сфере обработки
персональных данных

План-график мероприятий внутреннего контроля
соответствия обработки персональных данных на 2022 год

Мероприятие	**Ответственный**	**Срок исполнения**
Проверка соблюдения правил доступа к персональным данным	еженедельно	Ответственный за обеспечение безопасности персональных данных
Проверка соблюдения режима защиты	ежедневно	Ответственный за обеспечение безопасности персональных данных
Проверка выполнения антивирусной политики	еженедельно	Ответственный за обеспечение безопасности персональных данных
Проверка обновления ПО и единообразия применяемого ПО на всех устройствах, используемых при обработке персональных данных	еженедельно	Ответственный за обеспечение безопасности персональных данных
Проверка актуальности локальных нормативных актов в сфере обработки персональных данных	ежегодно	Ответственный за обеспечение безопасности персональных данных
Рассмотрение итогов мероприятий внутреннего контроля на совещании при Ректоре	ежегодно	Ответственный за обеспечение безопасности персональных данных