Министерство образования, науки и молодежной политики Краснодарского края

Государственное бюджетное образовательное учреждение дополнительного профессионального образования
«Институт развития образования» Краснодарского края
(ГБОУ ИРО Краснодарского края)

ПРИКАЗ

от 28.03.2024 № 211/2

г. Краснодар

Об организационных мероприятиях по обработке и обеспечению безопасности персональных данных, обрабатываемых в государственном бюджетном образовательном учреждении дополнительного профессионального образования «Институт развития образования» Краснодарского края

Во исполнение требований федеральных законов от 27 июля 2008 г. № 152-ФЗ «О персональных данных», в соответствии с постановлениями Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных», необходимых для обеспечения безопасности персональных данных, обрабатываемых в государственном бюджетном образовательном учреждении дополнительного профессионального образования «Институт развития образования» Краснодарского края (далее – институт), установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищённости, п р и к а з ы в а ю:

1. Назначить ответственного за организацию обработки персональных данных руководителя центра цифровизации образования Головнева С.С.

2. Утвердить:

1) положение о порядке организации и проведении работ по обработке и защите персональных данных в государственном бюджетном образовательном учреждении дополнительного профессионального образования «Институт развития образования» Краснодарского края (приложение 1);

2) правила рассмотрения запросов субъектов персональных данных или их представителей в государственном бюджетном образовательном учреждении дополнительного профессионального образования «Институт развития образования» Краснодарского края (приложение 2);

3) правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в государственном бюджетном образовательном учреждении дополнительного профессионального образования «Институт развития образования» Краснодарского края (приложение 3).

4) правила доступа в помещения государственного бюджетного образовательного учреждения дополнительного профессионального образования «Институт развития образования» Краснодарского края (приложение 4);

5) перечень должностей государственного бюджетного образовательного учреждения дополнительного профессионального образования «Институт развития образования» Краснодарского края, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным (приложение 5);

6) перечень информационных ресурсов и систем государственного бюджетного образовательного учреждения дополнительного профессионального образования «Институт развития образования» Краснодарского края (приложение 6);

7) оценку вреда, который может быть причинен субъектам персональных данных государственного бюджетного образовательного учреждения дополнительного профессионального образования «Институт развития образования» Краснодарского края (приложение 7);

8) типовую форму согласия на обработку персональных данных (приложение 8);

9) типовую форму согласия на обработку персональных данных сотрудника (совместителя) и членов его семьи (приложение 9);

10) типовую форму типового обязательства государственного бюджетного образовательного учреждения дополнительного профессионального образования «Институт развития образования» Краснодарского края о неразглашении персональных данных субъектов персональных данных (Приложение 10);

11) типовую форму заявления и согласия на обработку персональных данных слушателя (приложение 11);

12) типовую форму заявление-согласие на обработку персональных данных обучающегося и персональных данных законного представителя (приложение 12).

13) типовую форму Согласие субъекта персональных данных на обработку и передачу оператором персональных данных третьим лицам (приложение 13).

14) типовую форму согласия на обработку персональных данных участника конкурса (приложение 8);

3. Центру цифровизации образования Головнев С.С. ознакомить сотрудников института с настоящим приказом под подпись.

4. Отделу правового сопровождения и кадрового обеспечения Дзекунова Н.М. осуществлять направление в центр цифровизации образования лиц, поступивших в институт на работу для ознакомления с настоящим приказом.

5. Признать утратившими силу «ПОЛОЖЕНИЕ об обработке и защите персональных данных работников государственного бюджетного образовательного учреждения дополнительного профессионального образования «Институт развития образования» Краснодарского края» утвержденного приказом от 09 января 2024 г. № 3 «Об утверждении локальных нормативных актов ГБОУ ИРО Краснодарского края» с даты издания настоящего приказа.

6. Признать утратившими силу, с даты издания настоящего приказа, следующие приказы:

1) приказ от 27 июля 2021 г. № 239 «Об утверждении Положения о порядке организации и проведении работ по обработке и защите персональных данных»;

2) приказ от 27 июля 2021 г. № 240 «Об утверждении Политики в отношении обработки персональных данных субъектов государственного бюджетного образовательного учреждения дополнительного профессионального образования «Институт развития образования» Краснодарского края»;

3) приказ от 27 июля 2021 г. № 242 «Об утверждении инструкции пользователей информационных систем персональных данных в Государственном бюджетном образовательном учреждении дополнительного профессионального образования «Институт развития образования» Краснодарского края»;

4) приказ от 27 июля 2021 г. № 249 «Об утверждении Инструкции по порядку проведения проверок состояния защиты персональных данных Государственного бюджетного образовательного учреждения дополнительного профессионального образования «Институт развития образования» Краснодарского края»;

5) приказ от 27 июля 2021 г. № 250 «Об утверждении Регламента учета средств защиты, документации и электронных носителей персональных данных Государственного бюджетного образовательного учреждения дополнительного профессионального образования «Институт развития образования» Краснодарского края»;

6) приказ от 27 июля 2021 г. № 251 «Об утверждении Инструкции ответственного за организацию обработки персональных данных Государственного бюджетного образовательного учреждения дополнительного профессионального образования «Институт развития образования» Краснодарского края»;

7) приказ от 27 июля 2021 г. № 252 «Об утверждении Инструкции ответственного за обеспечение безопасности персональных данных Государственного бюджетного образовательного учреждения дополнительного профессионального образования «Институт развития образования» Краснодарского края»;

8) приказ от 27 июля 2021 г. № 253 «Об утверждении Порядка доступа сотрудников в помещения, в которых ведется обработка персональных данных

Государственного бюджетного образовательного учреждения дополнительного профессионального образования «Институт развития образования» Краснодарского края»;

9) приказ от 27 июля 2021 г. № 254 «Об утверждении Правил работы с обезличенными персональными данными Государственного бюджетного образовательного учреждения дополнительного профессионального образования «Институт развития образования» Краснодарского края»;

10) приказ от 27 июля 2021 г. № 255 «Об утверждении Правил рассмотрения запросов субъектов персональных данных или их представителей в Государственном бюджетном образовательном учреждении дополнительного профессионального образования «Институт развития образования» Краснодарского края»;

11) приказ от 27 июля 2021 г. № 256 «Об утверждении Плана внутренних проверок состояния защиты персональных данных Государственного бюджетного образовательного учреждения дополнительного профессионального образования «Институт развития образования» Краснодарского края»;

12) приказ от 27 июля 2021 г. № 259 «О создании комиссии по установлению уровня защищённости персональных данных в информационных системах персональных данных Государственном бюджетном образовательном учреждении дополнительного профессионального образования «Институт развития образования» Краснодарского края»;

13) приказ от 27 июля 2021 г. № 261 «О назначении ответственного за организацию обработки персональных данных в Государственном бюджетном образовательном учреждении дополнительного профессионального образования «Институт развития образования» Краснодарского края»;

14) приказ от 30 декабря 2021 г. № 633 «Об утверждении Перечня должностей работников в ГБОУ ИРО Краснодарского края, замещение которых предусматривает осуществление обработки персональных данных, либо осуществление доступа к персональным данным, обрабатываемым в Государственном бюджетном образовательном учреждении дополнительного профессионального образования «Институт развития образования»;

7. Контроль за выполнением настоящего приказа возложить на проректора по воспитательной деятельности, дополнительному образованию и цифровой трансформации Терновую Л.Н.

8. Приказ вступает в силу со дня его подписания.

Исполняющий обязанности ректора Л.Н. Терновая

ЛИСТ СОГЛАСОВАНИЯ
приказа
Об организационных мероприятиях по обработке и обеспечению безопасности персональных данных, обрабатываемых в государственном бюджетном образовательном учреждении дополнительного профессионального образования «Институт развития образования» Краснодарского края

от «28» 03 2024 г. № 211/2

Проект приказа подготовлен:
руководителем центра
цифровизации образования С.С. Головнев

Согласовано:

И.о. начальника отдела правового
сопровождения и кадрового обеспечения И.А. Витушкина

Приложение 1

УТВЕРЖДЕНО
приказом ГБОУ ИРО
Краснодарского края
от 28.03.24 № 211/2г

ПОЛОЖЕНИЕ
о порядке организации и проведении работ по обработке и защите персональных данных в государственном бюджетном образовательном учреждении дополнительного профессионального образования «Институт развития образования» Краснодарского края

г. Краснодар

Содержание

1. Термины и определения

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

Актуальные угрозы безопасности персональных данных - совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

Блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

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

Обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

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.

Оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

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

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

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

Специальные категории персональных данных – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья и интимной жизни.

Трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного

государства, иностранному физическому лицу или иностранному юридическому лицу.

Угрозы безопасности персональных данных - совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных.

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.

2. Общие положения

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

2.2 Настоящее Положение разработано в соответствии со следующими нормативными правовыми актами:

- Конституция Российской Федерации;
- Трудовой кодекс Российской Федерации;
- Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных» в редакции от 21.07.2014;
- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» в редакции от 21.07.2014;
- Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденное Постановлением Правительства Российской Федерации от 15 сентября 2008 г № 687;
- Требования к защите персональных данных при их обработке в информационных системах персональных данных, утвержденное Постановлением Правительства Российской Федерации от 1 ноября 2012 г. №1119;
- Указ Президента РФ от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера»;
- Приказ Роскомнадзора от 5 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных»;
- Трудовой кодекс Российской Федерации;
- Гражданский кодекс Российской Федерации;
- Налоговый кодекс Российской Федерации;
- Уголовный кодекс Российской Федерации;
- нормативные и методические документы ФСБ России, ФСТЭК России, Роскомнадзора;
- Уставом и иными локальными нормативными актами ГБОУ ИРО Краснодарского края.

2.3 Настоящее Положение определяет порядок и условия обработки персональных данных, т.е. любых действий (операций) или совокупности действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу, обезличивание, блокирование, удаление, уничтожение персональных данных в государственном бюджетном образовательном учреждении дополнительного профессионального образования «Институт развития образования» Краснодарского края (далее – ГБОУ ИРО Краснодарского края).

2.4 Настоящее положение определяет правовые, организационные и

технические меры необходимые 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.

2.5 ГБОУ ИРО Краснодарского края вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, на основании заключаемого с этим лицом договора. Лицо, осуществляющее обработку персональных данных по поручению ГБОУ ИРО Краснодарского края, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных». В поручении должен быть определен перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки. Помимо этого, в поручении 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 соответствии со статьей 19 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных».

2.6 Во всех случаях, не урегулированных настоящим Положением или другими нормативными документами ГБОУ ИРО Краснодарского края, необходимо руководствоваться действующим законодательством Российской Федерации.

2.7 Настоящее Положение вступает в силу с момента его утверждения и действует до замены его новым Положением.

2.8 Все изменения в Положение вносятся приказом ректора ГБОУ ИРО Краснодарского края.

2.9 Настоящее Положение и изменения к нему являются обязательными для исполнения всеми сотрудниками ГБОУ ИРО Краснодарского края, имеющими доступ к персональным данным.

3. Принципы обработки персональных данных

3.1 Обработка персональных данных должна осуществляться на законной и справедливой основе.

3.2 Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей.

3.3 Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

3.4 Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

3.5 Обработке подлежат только персональные данные, которые отвечают целям их обработки.

3.6 Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки.

3.7 Обрабатываемые персональные данные не должны быть избыточными

по отношению к заявленным целям их обработки.

3.8 При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных.

3.9 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.

3.10 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.

4. Порядок обработки персональных данных

4.1 Обработка персональных данных субъектов персональных данных ГБОУ ИРО Краснодарского края осуществляется с их письменного согласия, которое действует со дня их поступления на подписания.

4.2 Опубликование и распространение персональных данных субъектов ГБОУ ИРО Краснодарского края допускается в случаях, установленных законодательством Российской Федерации.

4.3 Субъект персональных данных принимает решение о предоставлении персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе.

4.4 Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем.

4.5 Согласие на обработку персональных данных может быть отозвано субъектом персональных данных в соответствии с положением статьи 9 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных».

4.6 В случае отзыва субъектом персональных данных согласия на обработку персональных данных в ГБОУ ИРО Краснодарского края вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии законных оснований.

4.7 Решение, порождающее юридические последствия в отношении субъекта персональных данных или иным образом затрагивающее его права и законные интересы, может быть принято на основании исключительно автоматизированной обработки его персональных данных только при наличии согласия в письменной форме субъекта персональных данных.

4.8 Субъект персональных данных обязан предоставлять ГБОУ ИРО Краснодарского края достоверные сведения о себе.

4.9 Если персональные данные субъекта получены из общедоступных источников, то сроки их хранения не ограничиваются.

4.10 Сроки обработки и хранения персональных данных:

- сотрудников (работников) – 50 лет;

- кандидатов на должность – не более 1 года со дня достижение целей обработки персональных данных или максимальных сроков хранения;
- контрагентов и их представителей – в соответствии с номенклатурой дел;
- иных граждан, обработка которых возложена на ГБОУ ИРО Краснодарского края - в соответствии с внутренней номенклатурой.

4.11 Обработка персональных данных осуществляется допущенными к обработке сотрудниками ГБОУ ИРО Краснодарского края, определенными приказом ректора ГБОУ ИРО Краснодарского края, которые действуют на основании инструкций, предусматривающих выполнение комплекса мероприятий по обеспечению безопасности персональных данных.

5. Особенности обработки персональных данных без использования средств автоматизации

5.1 Обработка персональных данных, осуществляемая без использования средств автоматизации, должна выполняться в соответствии с требованиями «Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утверждённого постановлением Правительства Российской Федерации от 15.09.2008 № 687.

5.2 При разработке и использовании типовых форм документов, необходимых для реализации возложенных на ГБОУ ИРО Краснодарского края полномочий, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовая форма), должны соблюдаться следующие условия:

- типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, адрес ГБОУ ИРО Краснодарского края, фамилию, имя, отчество и адрес субъекта персональных данных, чьи персональные данные вносятся в указанную типовую форму, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки;
- типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации, при необходимости получения согласия на обработку персональных данных;
- типовая форма должна быть составлена таким образом, чтобы каждый из субъектов, чьи персональные данные содержатся в типовой форме, при ознакомлении со своими персональными данными, не имел возможности доступа к персональным данным иных лиц, содержащихся в указанной типовой форме;
- типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

5.3 При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, а также если необходимо обеспечить раздельную обработку зафиксированных на одном материальном носителе персональных данных и информации, не являющейся персональными данными, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:

- при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;
- при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

5.4 Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

5.5 Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

5.6 При составлении типовых форм необходимо, чтобы каждый субъект персональных данных, чьи персональные данные указаны в документе, имел возможность ознакомиться со своими персональными данными, содержащими в документе, не нарушая прав и законных интересов иных лиц.

6. Порядок уничтожения персональных данных

6.1 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.

6.2 Персональные данные уничтожаются или обеспечивается их уничтожение в случае:

- если получен отзыв от субъекта персональных данных;
- если ГБОУ ИРО Краснодарского края не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных» или другими федеральными законами;
- если достигнуты цели обработки персональных данных;
- если представлены субъектом персональных данных или его представителем сведения, подтверждающие, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки;
- если обеспечить правомерность обработки персональных данных невозможно.

6.3 В случае отсутствия возможности уничтожения персональных данных в течение срока, осуществляется блокирование персональных данных или обеспечивается их блокирование и обеспечивается уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

6.4 Об устранении допущенных нарушений или об уничтожении персональных данных ГБОУ ИРО Краснодарского края уведомляет 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.

6.5 Уничтожение персональных данных в ГБОУ ИРО Краснодарского края происходит штатными средствами, либо осуществляется обезличивание персональных данных.

6.6 Уничтожение бумажных носителей персональных данных происходит путём измельчения на бумагорезательной машине, либо сжигания.

6.7 Уничтожение персональных данных осуществляет комиссия в составе членов комиссии и председателя.

6.8 Порядок уничтожения персональных данных должен быть регламентирован в нормативных документах ГБОУ ИРО Краснодарского края.

6.9 Контроль за выполнением процедур уничтожения персональных данных осуществляет ответственный за обеспечение безопасности персональных данных и ответственный за организацию обработки персональных данных.

6.10 После проведенного уничтожения должен быть подготовлен акт об уничтожении персональных данных.

6.11 Иные документы внутреннего обращения, содержащие персональные данные, создаются уполномоченными работниками, хранятся в определенных местах и уничтожаются по исполнении целей обработки в соответствии с общим порядком делопроизводства.

7. Трансграничная передача персональных данных

7.1 Трансграничная передача персональных данных на территории иностранных государств, являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, а также иных иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных, осуществляется в соответствии с Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных».

7.2 ГБОУ ИРО Краснодарского края не осуществляет трансграничную передачу персональных данных.

8. Цель обработки персональных данных

8.1 К субъектам персональных данных в ГБОУ ИРО Краснодарского края относятся:

- сотрудники ГБОУ ИРО Краснодарского края;
- контрагенты, поставщики;
- кандидаты на замещение вакантной должности;
- слушатели, осуществляющие обучение по дополнительным профессиональным программам, участники мероприятий;
- родители (законные представители) детей-инвалидов, дети-инвалиды, инвалиды;
- граждане, обращения которых направленны для рассмотрения Институту учредителем – Министерство образования, науки и молодежной политики Краснодарского края.

8.2 Целью обработки персональных данных является:

- начисление, перечисление заработной платы; предоставление данных в ПФР, ФСС, ИФНС;
- начисление, перечисление по договорам полученных/ оказанных услуг;
- анализ фонда оплаты труда;
- согласование, учет, контроль контрактов;
- заключение соглашений на субсидию, отчетность, согласование и проведение процедур закупок;
- соблюдение трудового законодательства Российской Федерации;
- заключение и исполнение договорной документации;
- заключение и исполнение договорной документации;
- оформление курсовой документации;
- аттестация педагогических кадров и иных работников Института;
- сбор, уточнение информации в рамках проведения мониторингов, организация и проведение краевых мероприятий, краевых форумов по распоряжению Министерства образования и науки Краснодарского края;
- издание распорядительных документов;
- ведение контроля и учета за выданными материальными ценностями;
- участие в обучение детей-инвалидов, инвалидов на дому с применением дистанционных образовательных технологий и электронного обучения и

обеспечение учета движения обучающихся от их поступления в образовательные учреждения до выпуска из учреждений общего, среднего профессионального, высшего образования;
- организация контроля доступа к базам данных, соблюдение требований законодательства РФ.

9. Состав персональных данных

9.1 В ГБОУ ИРО Краснодарского края обрабатываются следующие персональные данные сотрудников:

- фамилия, имя, отчество;
- дата рождения и место рождения;
- анкетные и биографические данные;
- сведения об образовании;
- сведения о трудовом стаже;
- сведения о семейном положении и составе семьи;
- сведения о воинском учете;
- сведения о занимаемой должности;
- сведения о заработной плате;
- сведения о социальных льготах;
- адрес регистрации и фактического места жительства;
- номера контактных телефонов;
- номер счета в банке, на который переводится заработная плата сотрудника;
- сведения, содержащиеся в приказах по личному составу (о поощрениях, взысканиях, назначении проверок, о предоставлении отпусков и т.д.);
- сведения о стажировке, повышении квалификации и переподготовке сотрудников;
- сведения о наградах, почетных званиях;
- иные сведения, содержащиеся в личных карточках сотрудников.

9.2 В ГБОУ ИРО Краснодарского края обрабатываются следующие персональные данные контрагентов, поставщиков:

- наименование (в том числе фамилия, имя, отчество);
- паспортные данные;
- контактная информация;
- банковские реквизиты.

9.3 В ГБОУ ИРО Краснодарского края обрабатываются следующие персональные данные слушателей, осуществляющих обучение по дополнительным профессиональным программам, участников мероприятий:

- фамилия, имя, отчество;
- паспортные данные;
- информация об образовании;
- дата рождения;
- адрес;

- контактные сведения;
- информация о трудовой деятельности.

9.4 В ГБОУ ИРО Краснодарского края обрабатываются следующие персональные данные кандидатов на замещение вакантной должности:

- фамилия, имя, отчество;
- адрес;
- гражданство;
- дата рождения;
- имущественное положение;
- информация о трудовой деятельности;
- контактные сведения;
- место рождения;
- образование;
- паспортные данные;
- профессия;
- сведения о воинском учёте;
- семейное положение;
- состав семьи;
- социальное положение;
- трудоспособность.

9.5 В ГБОУ ИРО Краснодарского края обрабатываются следующие персональные данные родителей (законных представителей) детей-инвалидов, детей-инвалидов, инвалидов:

- фамилия, имя, отчество;
- паспортные данные;
- контактная информация;
- информация о состоянии здоровья;
- информация об установлении инвалидности и сроках переосвидетельствования;
- информация об успеваемости ребенка и рекомендации психолого-медико-педагогической комиссии;
- информация о социально-бытовых условиях и технических условиях на месте установки оборудования для организации обучения детей-инвалидов, инвалидов с использованием дистанционных образовательных технологий.

9.6 В ГБОУ ИРО Краснодарского края обрабатываются следующие персональные данные граждан, обращения которых направленные для рассмотрения Институту учредителем – Министерство образования, науки и молодежной политики Краснодарского края:

- фамилия, имя, отчество;
- паспортные данные;
- дата рождения;
- адрес;

– контактные сведения.

10.Права субъекта персональных данных

10.1 Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

- подтверждение факта обработки персональных данных;
- правовые основания и цели обработки персональных данных;
- цели и применяемые способы обработки персональных данных;
- наименование и место нахождения ГБОУ ИРО Краснодарского края, сведения о лицах (за исключением сотрудников), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с ГБОУ ИРО Краснодарского края или на основании Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных»;
- обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения;
- сроки обработки персональных данных, в том числе сроки их хранения;
- порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных»;
- информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;
- иные сведения, предусмотренные Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных» или другими федеральными законами.

10.2 Субъект персональных данных имеет право на получение сведений, об обработке его персональных данных, за исключением случаев, предусмотренных частью 8 статьи 14 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных».

10.3 Сведения, об обработке персональных данных, предоставляются субъекту персональных данных ГБОУ ИРО Краснодарского края в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных.

10.4 Сведения, об обработке персональных данных, предоставляются субъекту персональных данных или его представителю ГБОУ ИРО Краснодарского края при обращении либо при получении запроса субъекта персональных данных или его представителя.

10.5 Субъект персональных данных вправе обратиться повторно в ГБОУ ИРО Краснодарского края или направить повторный запрос в целях получения сведений об обработке его персональных данных и ознакомления с такими персональными

данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса.

10.6 Субъект персональных данных вправе требовать 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 законом меры по защите своих прав.

10.7 Субъект персональных данных вправе требовать от ГБОУ ИРО Краснодарского края разъяснения о порядке принятия решения на основании исключительно автоматизированной обработки его персональных данных и возможные юридические последствия такого решения, а также, заявить возражение против такого решения.

10.8 Если субъект персональных данных считает, что ГБОУ ИРО Краснодарского края осуществляет обработку его персональных данных с нарушением требований Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие ГБОУ ИРО Краснодарского края в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

10.9 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.

11.Права оператора

11.1 ГБОУ ИРО Краснодарского края вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным частями 4 и 5 статьи 14 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных».

12.Обязанности оператора

12.1 Оператор обязан разъяснить субъекту персональных данных порядок принятия решения на основании исключительно автоматизированной обработки его персональных данных и возможные юридические последствия такого решения, предоставить возможность заявить возражение против такого решения, а также разъяснить порядок защиты субъектом персональных данных своих прав и законных интересов.

12.2 Оператор обязан рассмотреть возражение субъекта персональных данных против принятия решения на основании исключительно автоматизированной обработки его персональных данных, в течение тридцати дней со дня его получения и уведомить субъекта персональных данных о результатах рассмотрения такого возражения.

12.3 Оператор обязан предоставить субъекту персональных данных по его

просьбе информацию, предусмотренную частью 7 статьи 14 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных», за исключением случаев, предусмотренных частью 8 статьи 14 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных».

12.4 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 дает в письменной форме мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 Федерального закона или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий тридцати дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса субъекта персональных данных или его представителя.

12.5 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.

12.6 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.

12.7 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.

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

12.9 Если персональные данные получены не от субъекта персональных данных, Оператор, за исключением случаев, предусмотренных частью 4 статьи 18 Федерального закона от 27.07.2006 г. № 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 от 27.07.2006 г. № 152-ФЗ «О персональных данных» права субъекта персональных данных;

5) источник получения персональных данных.

12.10 Оператор обязан сообщить в уполномоченный орган по защите прав субъектов персональных данных по запросу этого органа необходимую информацию в течение тридцати дней с даты получения такого запроса.

12.11 Блокирование персональных данных субъекта персональных данных осуществляется или обеспечивается 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 с момента такого обращения или получения указанного запроса на период проверки;
- 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 с момента такого обращения или получения указанного запроса на период проверки.

12.12 В случае подтверждения факта неточности персональных данных оператор обязан персональные данные либо обеспечивает их уточнение в течение семи рабочих дней со дня представления таких сведений и снимает блокирование персональных данных.

12.13 Обработка персональных данных прекращается или обеспечивается прекращение их обработки в случае:

- выявления неправомерной обработки персональных данных, в срок, не превышающий трех рабочих дней с даты этого выявления;
- достижения цели обработки персональных данных;
- отзыва субъектом персональных данных согласия на обработку его персональных данных.

12.14 Оператор обязан опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных.

13.Передача персональных данных третьим лицам

13.1 ГБОУ ИРО Краснодарского края 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.

13.2 Передача персональных данных сотрудников ГБОУ ИРО Краснодарского края не допускается без письменного согласия, за исключением случаев, установленных федеральными законами.

13.3 Не допускается передача персональных данных по открытым каналам связи, в том числе по телефону.

13.4 Обмен персональными данными при их обработке в информационных системах осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и/или путем применения программных и технических средств.

14. Меры по защите персональных данных

14.1 Комплекс мер по защите персональных данных направлен на предупреждение нарушений доступности, целостности, достоверности и конфиденциальности персональных данных и обеспечивает безопасность информации в процессе деятельности ГБОУ ИРО Краснодарского края.

14.2 ГБОУ ИРО Краснодарского края при обработке персональных данных обязано 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.

14.3 Мероприятия по защите персональных данных определяются настоящим Положением, приказами, инструкциями и другими внутренними документами ГБОУ ИРО Краснодарского края.

14.4 Для защиты персональных данных в ГБОУ ИРО Краснодарского края применяются следующие меры:

- назначение ответственного за обеспечение безопасности персональных данных;
- назначение ответственного за организацию обработки персональных данных;
- назначение администратора информационной безопасности;
- издание, документов, определяющих политику в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;
- осуществление внутреннего контроля и аудита соответствия обработки персональных данных Федеральному закону от 27.07.2006 г. № 152-ФЗ «О персональных данных»;
- оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных»;
- ознакомление сотрудников ГБОУ ИРО Краснодарского края, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику ГБОУ ИРО Краснодарского края в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и обучение указанных сотрудников;
- определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

- применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных;
- учет машинных носителей персональных данных;
- обнаружение фактов несанкционированного доступа к персональным данным и принятием соответствующих мер;
- восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- установление правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;
- контроль за принимаемыми мерами по обеспечению безопасности персональных данных;
- ограничение и регламентация состава сотрудников, функциональные обязанности которых требуют доступа к информации, содержащей персональных данных;
- распределение персональной ответственности между сотрудниками, участвующими в обработке персональных данных, за выполнение требований по обеспечению безопасности персональных данных;
- исключение бесконтрольного пребывания посторонних лиц в помещениях, в которых ведется обработка персональных данных и находится соответствующая вычислительная техника;
- организация порядка уничтожения персональных данных;
- регулярные инструктажи сотрудников по вопросам, связанным с обеспечением безопасности персональных данных;
- закрытие помещений, в которых обрабатываются и хранятся персональные данные субъектов персональных данных, в рабочее время при отсутствии в них сотрудников;
- проведение уборки помещений, в которых хранятся персональные данные, производиться в присутствии соответствующих сотрудников;
- резервирование персональных данных (создание резервных копий).

15. Допуск персонала к обработке персональных данных

15.1 При допуске к обработке персональных данных необходимо руководствоваться приказом о допуске сотрудников ГБОУ ИРО Краснодарского края к обработке персональных данных.

15.2 Доступ конкретных лиц к персональным данным в информационные системы персональных данных осуществляется на основании служебных записок (заявок). Служебные записки на доступ учитываются и хранятся администратором информационной безопасности.

15.3 Конкретный регламент предоставления доступа определен в «Инструкции по внесению изменений в списки пользователей и наделению их

полномочиями доступа к ресурсам информационной системы персональных данных».

16.Обучение персонала, участвующего в обработке персональных данных

16.1 Должно проводиться регулярное обучение сотрудников по вопросам, связанным с обеспечением безопасности персональных данных.

16.2 Определены следующие форматы обучения:

- полные курсы (длительностью 5 дней и более);
- кратковременные курсы (длительностью от 1 до 3 дней);
- внешние и внутренние семинары;
- конференции;
- инструктажи.

16.3 Полные и кратковременные курсы, конференции, внешние семинары проводятся во внешних специализированных организациях для следующих категорий сотрудников:

- ответственный за обеспечение безопасности персональных данных;
- ответственный за организацию обработки персональных данных;
- администратор информационной безопасности.

16.4 Для обучения остальных категорий персонала, участвующих в процессах обработки персональных данных, должны проводиться:

- внутренние семинары;
- инструктажи.

16.5 Внутренние семинары проводятся ответственным за обеспечение безопасности и обработку персональных данных, администратором информационной безопасности информационной системы персональных данных, а также приглашенными специалистами или другими подготовленными лицами. Все семинары следует проводить с использованием презентации.

16.6 Обучение каждой категории сотрудников должно проводиться не реже одного раза в год.

16.7 Инструктажи проводятся в отношении отдельных лиц, по мере необходимости администратором информационной безопасности информационной системы персональных данных, ответственным за обеспечение безопасности и обработку персональных данных.

16.8 При необходимости могут разрабатываться инструкции, описывающие особенности обработки персональных данных в каждой информационной системы персональных данных, для отдельных категорий (групп) персонала.

16.9 Проведения инструктажей должно фиксироваться в « Журнале учета проведения инструктажей по вопросам защиты информации».

17.Защита от несанкционированного физического доступа к элементам информационной системы персональных данных

17.1 Мероприятия по физическому контролю доступа включают:

- контроль доступа на территорию;
- контроль доступа в помещения с оборудованием информационной системы персональных данных;
- контроль доступа к техническим средствам информационной системы персональных данных;
- контроль перемещений физических компонентов информационной системы персональных данных.

17.2 Помещения с серверным, телекоммуникационным и сетевым оборудованием информационной системы персональных данных должны иметь прочные входные двери с надежными замками. Двери должны быть постоянно закрыты на замок и открываться только для санкционированного прохода сотрудников, отвечающих за обслуживание данного оборудования.

17.3 Двери помещений, в которых размещаются автоматизированные рабочие места пользователей информационной системы персональных данных, должны быть оборудованы замками.

17.4 Нахождение в помещении лиц, не участвующих в технологических процессах обработки персональных данных (обслуживающий персонал, другие сотрудники), должно допускаться только в присутствии сотрудников, участвующих в соответствующих технологических процессах.

17.5 Расположение мониторов рабочих станций должно препятствовать их несанкционированному просмотру со стороны других лиц, не являющихся пользователями информационной системы персональных данных.

17.6 В нерабочее время, по окончании рабочего дня двери помещений должны быть закрыты на замок.

17.7 При выносе устройств, хранящих персональные данные, за пределы контролируемой зоны для ремонта, замены и т.п. должно быть обеспечено гарантированное уничтожение информации, хранимой на этих устройствах.

18. Резервирование персональных данных

18.1 Резервирование персональных данных должно обеспечить возможность восстановления информации при нарушении целостности основных хранилищ данных.

18.2 Резервированию должна подвергаться информация на серверах информационной системы персональных данных.

18.3 Резервирование должно осуществляться на магнитные ленты или другие носители информации с соответствующим уровнем надежности и долговечности.

18.4 Хранение резервных копий должно осуществляться в сейфах (запираемых шкафах, ящиках). Хранение (по возможности) должно осуществляться в месте, территориально удаленном от основного хранилища информации.

18.5 Доступ к резервным копиям должен быть строго регламентирован.

18.6 Резервирование должно осуществляться в соответствии с инструкцией

резервного копирования ГБОУ ИРО Краснодарского края.

19. Реагирование на нештатные ситуации

19.1 Для эффективного реагирования на нештатные ситуации, возникающие при обработке персональных данных ГБОУ ИРО Краснодарского края, должны быть регламентированы следующие вопросы:

- порядок определения нештатной ситуации;
- порядок оповещения сотрудников при возникновении различных нештатных ситуаций;
- порядок действий персонала в нештатных ситуациях.

19.2 В ГБОУ ИРО Краснодарского края должны проводиться расследования инцидентов, связанных с несанкционированным доступом и другими несанкционированными действиями.

19.3 В рамках данного процесса должны решаться следующие задачи:

- расследование инцидентов, связанных с безопасностью персональных данных;
- ликвидация последствий инцидентов связанных с безопасностью персональных данных;
- принятие мер по недопущению возникновения подобных инцидентов в дальнейшем.

19.4 Реагирование на нештатные ситуации должно производиться в соответствии с «Инструкцией по действиям пользователей информационной системы персональных данных в нештатных ситуациях».

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

20.1 Ответственность за контроль соблюдения требований по обработке персональных данных возлагается на ответственного за организацию обработки персональных данных в ГБОУ ИРО Краснодарского края.

20.2 Юридические и физические лица, в соответствии со своими полномочиями обрабатывающие информацию о гражданах, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.

20.3 Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

20.4 Каждый сотрудник ГБОУ ИРО Краснодарского края, получающий для работы конфиденциальный документ, несет персональную ответственность за сохранность носителя и конфиденциальность полученной информации.

20.5 В соответствии с Гражданским кодексом Российской Федерации лица, незаконными методами получившие информацию, содержащую персональных данных, обязаны возместить причиненные убытки; такая же обязанность возлагается и на сотрудников, не обладающих правом доступа к персональным данным.

Приложение 2

УТВЕРЖДЕНЫ
приказом ГБОУ ИРО
Краснодарского края
от 28.03.24 № 211/2

ПРАВИЛА
рассмотрения запросов субъектов персональных данных или их представителей в государственном бюджетном образовательном учреждении дополнительного профессионального образования «Институт развития образования» Краснодарского края

1. Общие положения

1.1. Настоящие Правила определяют порядок учета (регистрации), рассмотрения запросов субъектов персональных данных или их представителей (далее – запросы) в государственном бюджетном образовательном учреждении дополнительного профессионального образования «Институт развития образования» Краснодарского края (далее – Институт).

1.2. Настоящие Правила разработаны в соответствии с:

Трудовым кодексом Российской Федерации;

Федеральным законом от 27 июня 2006 г. № 152-ФЗ «О персональных данных» (далее – Федеральный закон «О персональных данных»);

Федеральным законом от 2 мая 2006 г. № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации» (далее – Федеральный закон «О порядке рассмотрения обращений граждан Российской Федерации»);

постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

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» и другими нормативными правовыми актами.

1.3. Настоящие Правила распространяются на работников Института, осуществляющих работу с кандидатами на замещение вакантной должности, с претендентами на вакантные должности, контрагентами, поставщиками, слушателями, дети-инвалиды, инвалиды, граждане, обращения которых направленны для рассмотрения Институту учредителем – Министерство образования, науки и молодежной политики Краснодарского края.

2. Права субъектов персональных данных

2.1. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных в соответствии с частью 7 статьи 14 Федерального закона «О персональных данных», в том числе содержащей:

подтверждение факта обработки персональных данных в Институте;

правовые основания и цели обработки персональных данных;

цели и применяемые в Институте способы обработки персональных данных;

наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора, то есть помимо работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Институтом или на основании Федерального закона, в соответствии с которым осуществляется предоставление персональных данных;

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

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

порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом;

информацию об осуществленной или о предполагаемой трансграничной передаче данных;

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

иные сведения, предусмотренные Федеральным законом «О порядке рассмотрения обращений граждан Российской Федерации».

2.2. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с частью 8 статьи 14 Федерального закона «О персональных данных».

2.3. Субъект персональных данных вправе требовать от Института 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 Федеральным законом «О персональных данных» меры по защите своих прав.

2.4. Сведения, указанные в части 7 статьи 14 Федерального закона «О персональных данных», должны быть предоставлены субъекту персональных данных в доступной форме и в них не должно содержаться персональных данных, относящихся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

2.5. Сведения, указанные в части 7 статьи 14 Федерального закона «О персональных данных», предоставляются субъекту персональных данных или его представителю Институтом, при обращении субъекта персональных данных, либо при получении запроса субъекта персональных данных или его представителя.

3. Правила рассмотрения запросов субъектов

3.1. Запрос субъекта персональных данных 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 Институтом, либо сведения, иным образом подтверждающие факт обработки персональных данных Институтом, подпись субъекта персональных данных или его представителя.

3.2. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации, согласно форме, приведенной в приложении 1.

3.3. Рассмотрение запросов является обязанностью уполномоченных работников Института.

3.4. Работники Института обеспечивают:

проверку достоверности сведений, указанных в запросе;

объективное, всестороннее и своевременное рассмотрение запроса;

принятие мер, направленных на восстановление или защиту нарушенных прав, свобод и законных интересов субъектов персональных данных;

направление письменных ответов по существу запроса.

3.5. Запрос прочитывается и проверяется на повторность, при необходимости сверяется с находящейся в архиве предыдущей перепиской. В случае, если сведения, указанные в части 7 статьи 14 Федерального закона «О персональных данных», а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно в Институт или направить повторный запрос в целях получения сведений, указанных в части 7 статьи 14 Федерального закона «О персональных данных», и ознакомления с такими персональными данными в соответствии с частью 4 статьи 14 Федерального закона «О персональных данных» не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен предусмотренным Федеральным законом «О порядке рассмотрения обращений граждан Российской Федерации».

3.6. Срок предоставления ответов на поступившие запросы от субъектов персональных данных или их представителей в соответствии с частью 1 статьи 20 Федерального закона «О персональных данных» составляет тридцать дней.

3.7. Субъект персональных данных вправе обратиться повторно в Институт или направить повторный запрос в целях получения сведений, указанных в части 7 статьи 14 Федерального закона № 152-ФЗ «О персональных данных», а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в настоящем пункте, 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 с необходимыми сведениями, должен содержать обоснование направления повторного запроса.

3.8. Институт вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным частями 4 и 5 статьи 14 Федерального закона «О персональных данных». Такой отказ должен быть мотивированным.

3.9. Институт обязано сообщить 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 дать письменный ответ, согласно форме, приведенной в приложении 2, в течение тридцати дней с даты получения запроса субъекта персональных данных или его представителя.

3.10. 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, уполномоченные должностные лица Института обязаны дать в письменной форме мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 Федерального закона «О персональных данных» или иного Федерального закона, являющегося основанием для такого отказа, согласно форм отказов, приведенных в приложении 3, 4.

3.11. Институт обязан предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных.

3.12. В соответствии с частью 3 статьи 20 Федерального закона «О персональных данных» Институт:

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, работники Института обязаны 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, работники Института обязаны уничтожить такие персональные данные.

3.13. Институт 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.

3.14. 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, работники Института обязаны осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных с момента такого обращения или получения указанного запроса на период проверки.

3.15. 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, работники Института обязаны осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных, 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.

3.16. В случае подтверждения факта неточности персональных данных работники Института на основании сведений, представленных субъектом персональных данных или его представителем, либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязаны уточнить персональные данные в соответствии с частью 2 статьи 20 Федерального закона «О персональных данных» в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

3.17. В случае выявления неправомерной обработки персональных данных работники Института в срок, в соответствии с частью 3 статьи 20 Федерального закона «О персональных данных», не превышающий трех рабочих дней с даты этого выявления, обязаны прекратить неправомерную обработку персональных данных, а в случае, если обеспечить правомерность обработки персональных данных невозможно, работники Института в срок не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных обязаны уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных Институт обязан уведомить субъекта персональных данных или его представителя. 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 в указанный орган.

3.18. Для проверки фактов, изложенных в запросах, при необходимости организуются служебные проверки в соответствии с законодательством Российской Федерации.

3.19. По результатам служебной проверки составляется мотивированное заключение, которое должно содержать объективный анализ собранных материалов. Если при проверке выявлены факты совершения работниками Института действия (бездействия), содержащего признаки административного правонарушения или состава преступления, информация передается незамедлительно в правоохранительные органы. Служебная проверка проводится в соответствии с установленными в Институте правилами.

Приложение 1
к правилам рассмотрения
запросов субъектов
персональных данных или их
представителей в ГБОУ ИРО
Краснодарского края

ФОРМА

Ректору ГБОУ ИРО
Краснодарского края
Т.А. ГАйдук

_____
Ф.И.О. субъекта персональных данных

_____
Номер основного документа, удостоверяющего личность

_____
Наименование выдавшего органа

_____
Дата выдачи

Заявление (запрос) о доступе субъекта персональных данных к своим персональным данным

Прошу подтвердить факт обработки моих персональных данных и предоставить мне для ознакомления информацию, составляющую мои персональные данные, на основании:

_____

_____
(указать 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)

_____ _____ _____
дата подпись расшифровка подписи

Приложение 2
к правилам рассмотрения
запросов субъектов
персональных данных или их
представителей в ГБОУ ИРО
Краснодарского края

ФОРМА

Ответ на запрос о предоставлении субъекту его персональных данных

Уведомление

Уважаемый(ая) _____
(фамилия, имя, отчество)

В ответ на Ваш запрос от _____
(дд.мм.гг.)

сообщаем, что в государственном бюджетном образовательном учреждении дополнительного профессионального образования «Институт развития образования» Краснодарского края (далее – Оператор), расположенный по адресу: 350080, г. Краснодар, ул. Сормовская, 167, осуществляется обработка следующих Ваших персональных данных:

_____
_____
(перечислить персональные данные)

Указанные персональные данные получены

_____
_____
(непосредственно от Вас / указать источник получения персональных данных)

Персональные данные обрабатываются и используются Оператором в целях и на основании

_____
_____
(перечислить цели и правовые основания обработки)

Ваши персональные данные обрабатываются (нужное подчеркнуть) автоматизированным/неавтоматизированным/смешанным способом.

Перечень лиц (за исключением работников Оператора), которые имеют доступ к Вашим персональным данным или которым могут быть раскрыты Ваши персональные данные на основании договора с оператором или на основании федерального закона:

_____
_____
(перечислить юридические и физические лица)

Сроки обработки и хранения персональных данных определяются целями обработки (персональные данные обрабатываются до тех пор, пока соответствуют целям обработки).

дата	подпись	расшифровка подписи

Настоящее уведомление на руки получил(а):

дата	подпись	расшифровка подписи

Приложение 3
к правилам рассмотрения
запросов субъектов
персональных данных или их
представителей в ГБОУ ИРО
Краснодарского края

ФОРМА

Отказ в выполнении повторного запроса
субъекта персональных данных

Уведомление

Уважаемый(ая) _____
(фамилия, имя, отчество)

На основании _____
_____
(ссылка на положение части 4 или 5 статьи 14 Федерального закона от 27 июля 2006 года № 152-ФЗ "О персональных данных" или на иной федеральный закон, являющийся основанием для такого отказа)

Государственное бюджетное образовательное учреждение дополнительного профессионального образования «Институт развития образования» Краснодарского края вынуждено отказать Вам в выполнении повторного запроса на доступ к Вашим персональным данным.

_____ _____ _____
дата подпись расшифровка подписи

Настоящее уведомление на руки получил(а):

_____ _____ _____
дата подпись расшифровка подписи

Приложение 4
к правилам рассмотрения
запросов субъектов
персональных данных или их
представителей в ГБОУ ИРО
Краснодарского края

ФОРМА

Отказ в предоставлении доступа субъекта персональных данных к его персональным данным

Уведомление

Уважаемый(ая) _____
(фамилия, имя, отчество)

На основании _____
_____
(ссылка на положение части 8 статьи 14 Федерального закона от 27 июля 2006 года № 152-ФЗ "О персональных данных" или на иной федеральный закон, являющийся основанием для такого отказа)

Государственное бюджетное образовательное учреждение дополнительного профессионального образования «Институт развития образования» Краснодарского края вынуждено отказать Вам в предоставлении доступа к Вашим персональным данным.

_____ _____ _____
дата подпись расшифровка подписи

Настоящее уведомление на руки получил(а):

_____ _____ _____
дата подпись расшифровка подписи

Приложение 3

УТВЕРЖДЕНЫ
приказом ГБОУ ИРО
Краснодарского края
от 28.03.24 № 211/2

ПРАВИЛА
осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в государственном бюджетном образовательном учреждении дополнительного профессионального образования «Институт развития образования» Краснодарского края

1. Общие положения

1.1. Настоящие правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в государственном бюджетном образовательном учреждении дополнительного профессионального образования «Институт развития образования» Краснодарского края (далее – Правила) определяют порядок осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным законодательством Российской Федерации и принятыми в соответствии с ним нормативными правовыми актами.

1.2. Настоящие Правила разработаны в соответствии с:

Федеральным законом от 27 июня 2006 г. № 152-ФЗ «О персональных данных» (далее – Федеральный закон «О персональных данных»);

постановлением Правительства Российской Федерации от 15 августа 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

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» и другими нормативными правовыми актами;

постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке информационных системах персональных данных».

1.3. Настоящими Правилами в своей работе должны руководствоваться:

работники государственного бюджетного образовательного учреждения дополнительного профессионального образования «Институт развития

образования» Краснодарского края (далее – Институт), осуществляющие внутренний контроль соответствия обработки персональных данных требованиям к защите персональных данных.

2. Структура процессов по внутреннему контролю

2.1. Контроль выполнения требований по защите персональных данных в структурных подразделениях Института 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.

2.2. Контроль выполнения требований по защите персональных данных в структурных подразделениях Института осуществляет ответственный за организацию обработки персональных данных в Институте и администратор информационной безопасности Института.

2.3. Общий контроль выполнения требований по обеспечению безопасности персональных данных осуществляет ответственный за выполнение мероприятий по контролю исполнения в структурных подразделениях Института требований документов по обеспечению безопасности персональных данных.

2.4. Контроль проводится в форме плановых и внеплановых проверок. Внеплановые проверки могут быть контрольными и по частным вопросам.

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

2.6. 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 или нарушения требований по защите персональных данных.

2.7. Сроки проведения контрольных проверок доводятся руководителям проверяемых структурных подразделений Института не позднее, чем за 24 часа до начала проверки.

2.8. Проверки по частным вопросам могут проводиться без уведомления руководителей структурных подразделений Института.

2.9. Периодичность и сроки проведения плановых проверок структурных подразделений Института устанавливаются планом проверок на календарный год. Сроки проведения плановых проверок доводятся руководителям проверяемых подразделений не позднее, чем за 10 суток до начала проверки.

3. Порядок подготовки к проверке

3.1. Общий контроль выполнения требований по обеспечению безопасности персональных данных в структурных подразделениях Института осуществляется в соответствии с Планом проведения внутренних проверок соответствия обработки персональных данных требованиям к защите персональных данных Института (форма представлена в приложении 1), утвержденным Ректором государственного бюджетного образовательного

учреждения дополнительного профессионального образования «Институт развития образования» Краснодарского края.

3.2. Ответственный за выполнение мероприятий по контролю исполнения структурных подразделений Института требований документов по обеспечению безопасности персональных данных подготавливает предложения по составу комиссии или группы проверяющих лиц.

3.3. Контроль в структурных подразделениях Института, осуществляемый ответственными за обеспечение контроля процессов обеспечения безопасности персональных данных структурных подразделений Института, осуществляется в соответствии с Планом проведения внутренних проверок соответствия обработки персональных данных требованиям к защите персональных данных структурных подразделений Института (форма представлена в приложении 2). Данные Планы утверждаются руководителями структурных подразделений Министерства и согласовываются с ответственным за выполнение мероприятий по контролю исполнения структурных подразделений Института, требований документов по обеспечению безопасности персональных данных.

3.4. Проверяющие лица обязаны получить у руководителей проверяемых структурных подразделений Института информацию об условиях обработки персональных данных, необходимую для достижения целей проверки. Перед началом проверки они должны изучить материалы предыдущих проверок данного структурного подразделения Института.

4. Порядок проведения проверки

4.1. Руководитель проверяемого структурного подразделения Института обязан оказывать содействие комиссии по проверке или группе проверяющих лиц и в случае необходимости определяет должностное лицо, ответственное за сопровождение проверки.

4.2. Допуск проверяющих лиц к конкретным информационным ресурсам, защищаемым сведениям и техническим средствам должен исключать ознакомление проверяющих лиц с конкретными персональными данными.

4.3. Должны быть согласованы конкретные вопросы по объему, содержанию, срокам проведения проверки, а также каких работников структурных подразделений Института необходимо привлечь к проверке и какие помещения следует посетить.

4.4. Общий порядок проведения проверки включает:

выявление работников, задействованных в обработке персональных данных;

проверка факта ознакомления работников проверяемого структурного подразделения Института с нормативными документами, регламентирующими вопросы обработки и защиты персональных данных;

получение при содействии работников проверяемого структурного подразделения Института документов, касающихся обработки и защиты персональных данных в данном структурном подразделении; анализ полученной документации;

непосредственная проверка выполнения установленного порядка обработки и защиты персональных данных и требований законодательства Российской Федерации в области защиты персональных данных.

4.5. В ходе осуществления контроля выполнения требований по защите персональных данных в структурном подразделении Института рассматриваются следующие показатели работ по защите персональных данных:

наличие согласий на обработку персональных данных субъектов персональных данных, в случаях, предусмотренных законодательствам Российской Федерации;

соответствие состава и сроков обработки целям обработки ПДн;

соответствие Перечня должностей Института, трудовые функции которых предусматривают осуществление обработки персональных данных либо осуществление доступа к персональным данным реальному составу работников;

соответствие Перечня лиц, имеющих доступ в помещения, в которых ведется обработка персональных данных реальному составу работников;

наличие нормативных документов по защите персональных данных;

знание нормативных документов и уровень подготовки работников, имеющих доступ к персональным данным;

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

наличие документов, подтверждающих учет и сохранность материальных носителей персональных данных.

4.6. В ходе осуществления контроля выполнения требований по защите персональных данных в структурном подразделении Института дополнительно рассматриваются следующие показатели работ по защите персональных данных:

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

наличие и корректность перечня информационных систем;

наличие документа, подтверждающего:

правильность определения уровня защищенности персональных данных, обрабатываемых в информационных системах, а также классов защищенности информационных систем;

наличие документа, подтверждающего факт определения угроз безопасности персональных данных, а также его актуальность (срок актуальности документа не может превышать 3 года);

соответствие состава средств вычислительной техники информационных систем указанному в документации на информационную систему;

соответствие требованиям по организации разграничения доступа пользователей к информационным ресурсам (в том числе сетевым);

порядок защиты персональных данных при передаче по сети;

применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

оценка эффективности принимаемых мер по обеспечению безопасности персональных данных.

4.7. Во время проведения проверки, выявленные нарушения требований по обработке и защите персональных данных должны быть по возможности

устранены. Проверяющие лица могут дать рекомендации по устранению на месте отмечаемых нарушений и недостатков.

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

5. Оформление результатов проверки

5.1. Результаты проверки оформляются актом.

5.2. Акт составляется в одном экземпляре и подписывается членами комиссии. Оригинал документа с результатами проверки хранится (передается) у ответственного за выполнение мероприятий по контролю исполнения структурными подразделениями Института требований документов по обеспечению безопасности персональных данных. Копия документа о проверке передается в проверяемое структурное подразделение Института.

5.3. Результаты проверок подразделений периодически обобщаются ответственным за выполнение мероприятий по контролю исполнения структурными подразделениями Института и доводятся до сведения ответственного за организацию обработки и обеспечение безопасности персональных данных Института.

5.4. При необходимости принятия решений по результатам проверки структурного подразделения Института – ответственному за организацию обработки и обеспечение безопасности персональных данных Института готовится соответствующая служебная записка.

6. Корректирующие мероприятия и контроль за их исполнением

6.1. Руководитель структурного подразделения Института анализирует акт о результатах внутренней проверки и в пятидневный срок определяет перечень мероприятий, необходимых для устранения нарушений и их причин.

6.2. Перечень мероприятий согласуется с ответственным за организацию обработки и обеспечение безопасности персональных данных Института.

6.3. Если корректирующие мероприятия касаются других структурных подразделений Института, то к анализу привлекаются специалисты соответствующих структурных подразделений.

6.4. Выполнение корректирующих мероприятий и их достаточность определяется ответственным за организацию обработки и обеспечение безопасности персональных данных Института.

6.5. Внутренняя проверка считается оконченной после выполнения всех корректирующих мероприятий и устранения выявленных нарушений.

Приложение 1
к Правилам осуществления
внутреннего контроля соответствия
обработки персональных данных
требованиям к защите
персональных данных в
ГБОУ ИРО Краснодарского края

ПЛАН
проведения внутренних проверок соответствия обработки персональных данных требованиям к защите персональных данных государственного бюджетного образовательного учреждения дополнительного профессионального образования «Институт развития образования» Краснодарского края

№ п/п	Наименование структурного подразделения государственного бюджетного образовательного учреждения дополнительного профессионального образования «Институт развития образования» Краснодарского края	Наименование мероприятия	Период проведения проверки	Отметка о выполнении (№ акта проверки)	Отметка о выполнении корректирующих мероприятий	Примечание
1	2	3	4	5	6	7

Приложение 2
к Правилам осуществления
внутреннего контроля соответствия
обработки персональных
данных требованиям к защите
персональных данных в ГБОУ ИРО
Краснодарского края

ПЛАН
проведения внутренних проверок соответствия обработки персональных данных требованиям к защите персональных данных структурных подразделений государственного бюджетного образовательного учреждения дополнительного профессионального образования «Институт развития образования» Краснодарского края

№ п/п	Наименование мероприятия	Период проведения проверки	Отметка о выполнении (№ акта проверки)	Отметка о выполнении корректирующих мероприятий	Примечание
1	2	3	4	5	6

Приложение 4

УТВЕРЖДЕНЫ
приказом ГБОУ ИРО
Краснодарского края
от 28.03.24 № 211/2

ПРАВИЛА
доступа в помещения государственного бюджетного образовательного учреждения дополнительного профессионального образования «Институт развития образования» Краснодарского края, в которых ведется обработка защищаемой информации, в том числе персональных данных

1. Общие положения

1.1. Настоящие Правила устанавливают порядок доступа в помещения государственного бюджетного образовательного учреждения дополнительного профессионального образования «Институт развития образования» Краснодарского края (далее – Институт), в которых ведется обработка конфиденциальной и защищаемой информации, в том числе персональных данных (далее – Информация).

1.2. Правила разработаны в целях обеспечения безопасности информации, обрабатываемой в Институте, на средствах вычислительной техники информационных систем, на материальных носителях информации, а также для обеспечения внутриобъектового режима.

1.3. Настоящий Порядок устанавливает правила доступа в следующие помещения Института:

помещения, в которых происходит обработка Информации, как с использованием средств автоматизации, так и без таковых, в том числе серверные помещения;

помещения, в которых хранятся материальные носители Информации и их резервные копии;

помещения, в которых установлены средства криптографической защиты информации (далее – СКЗИ) и хранятся носители ключевой информации, в том числе средства электронной подписи (далее – Спецпомещения).

1.4. Настоящий Порядок разработан в соответствии с:

Федеральным законом Российской Федерации от 27 июня 2006 г. № 152-ФЗ «О персональных данных» (далее – Федеральный закон «О персональных данных»);

постановлением Правительства Российской Федерации от 15 августа 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

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»;

приказом Федеральной службой безопасности России от 10 июля 2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

приказом Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13 июня 2001 г. № 152 «Об утверждении инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».

1.5. В каждом структурном подразделении Института назначается ответственное лицо за доступ в Помещения.

1.6. Работники Института, допущенные в помещения, обязаны:

выполнять требования обеспечения безопасности Информации;

соблюдать режим конфиденциальности при обращении с Информацией, носителями Информации и СКЗИ (в том числе ключевыми документами к ним);

своевременно выявлять попытки посторонних лиц получить сведения об Информации, об используемых СКЗИ или ключевых документах к ним;

предусматривать раздельное безопасное хранение действующих и резервных ключевых документов, предназначенных для применения в случае компрометации действующих криптоключей.

2. Общие требования к оборудованию помещений и регламентации доступа в них

2.1. Режим обеспечения безопасности помещений, в которых осуществляется обработка Информации (далее – Помещения) должен быть организован таким образом, чтобы препятствовать возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения.

2.2. Ограждающие конструкции Помещений, должны предполагать существенные трудности для нарушителя по их преодолению (например, металлические решетки на окнах, металлическая дверь, система контроля и управления доступом и так далее).

2.3. Помещения должны быть оснащены надежными входными дверьми с замками, а также средствами опечатывания помещений по окончании рабочего дня.

2.4. Окна Помещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в помещения посторонних лиц, должны быть оборудованы металлическими решетками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в помещения.

2.5. В Институте определяется перечень помещений, в которых разрешена обработка Информации. Форма перечня представлена в приложении 1.

2.6. Доступ работников в Помещения Института должен быть организован согласно перечню лиц, допущенных в Помещения обработки Информации (форма перечня представлена в приложении 2). Перечень работников, доступ которых разрешен в Помещения, размещается на внутренней стороне двери этого помещения.

2.7. В Помещениях определяются места хранения материальных носителей Информации и лиц, ответственных за их сохранность (форма перечня представлена в приложении 3).

2.8. Указанные перечни разрабатываются ответственными за доступ в Помещения лицами и утверждаются Ректором государственного бюджетного образовательного учреждения дополнительного профессионального образования «Институт развития образования» Краснодарского края либо лицом его замещающем.

2.9. Доступ посторонних лиц в Помещения, должен осуществляться только ввиду служебной необходимости и под контролем сопровождающего лица из числа работников, допущенных в Помещение. При этом должны быть приняты меры, исключающие ознакомление посторонних лиц с защищаемой Информацией. Такими мерами являются:

размещение мониторов, исключающее или существенно затрудняющее просмотр отображаемой информации;

размещение документации на бумажных носителях, содержащих Информацию, исключающее просмотр Информации на них (документация убирается в папки, ящики тумбочек/столов, либо переворачивается лицевой стороной вниз, либо накрывается сверху непрозрачными объектами, закрывающими область текста).

2.10. В нерабочее время все окна и двери в помещениях (в том числе в смежные помещения), в которых ведется обработка Информации, должны быть надежно закрыты, материальные носители должны быть убраны в запираемые шкафы (сейфы), компьютеры выключены либо заблокированы.

2.11. При необходимости повышенного уровня обеспечения безопасности Помещений могут использоваться системы видеонаблюдения и системы контроля и управления доступом.

3. Особенности доступа в серверные помещения

3.1. Учет доступа в серверные помещения третьих лиц (осуществляющих обслуживание, техническое сопровождение, настройку серверного и активного сетевого оборудования) должен отражаться в Журнале доступа в серверные помещения (форма журнала приведена в приложении 4 к настоящей Политике).

3.2. Двери серверных помещений должны быть оборудованы устройствами, обеспечивающими постоянное закрытие дверей на замок и их открытие только для санкционированного прохода.

3.3. Уборка серверных помещений должна происходить только под контролем сопровождающего лица из числа работников, допущенных в Помещение.

3.4. Нахождение в серверных помещениях посторонних лиц без сопровождающего запрещено.

3.5. При возникновении чрезвычайных ситуаций природного и техногенного характера, аварий, катастроф, стихийных бедствий, а также других ситуаций, которые могут создавать угрозу жизни и здоровью граждан, доступ в серверные помещения, в целях оказания помощи гражданам, предотвращения, ликвидации предпосылок и последствий нештатной ситуации, может осуществляться без согласования с ответственным за доступ в Помещения лицом.

3.6. Работники органов Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий (далее – МЧС), аварийных служб, врачи «скорой помощи» допускаются в серверные помещения для ликвидации нештатной ситуации, иных чрезвычайных ситуаций или оказания медицинской помощи в сопровождении работника, допущенного в Помещение.

4. Особенности доступа в спецпомещения

4.1. Спецпомещения выделяют с учетом размеров контролируемых зон, регламентированных эксплуатационной и технической документацией к средствам криптографической защиты информации. Спецпомещения должны иметь прочные входные двери с замками, гарантирующими надежное закрытие помещений в нерабочее время.

4.2. Расположение Спецпомещений, специальное оборудование и организация режима в Спецпомещениях должны исключить возможность неконтролируемого проникновения или пребывания в них посторонних лиц, а также просмотра посторонними лицами ведущихся там работ.

4.3. Двери Спецпомещений должны быть оборудованы устройствами, обеспечивающими постоянное закрытие дверей на замок и их открытия только для санкционированного прохода.

4.4. При утрате ключа от входной двери в Спецпомещение замок необходимо заменить или переделать его секрет с изготовлением к нему новых ключей (с документальным оформлением).

4.5. Доступ работников в Спецпомещения в нерабочее время допускается на основании служебных записок (или иных видов разрешающих документов).

4.6. При возникновении чрезвычайных ситуаций природного и техногенного характера, аварий, катастроф, стихийных бедствий, а также ситуаций, которые могут создавать угрозу жизни и здоровью граждан, в целях оказания помощи гражданам, предотвращения, ликвидации предпосылок и последствий нештатной ситуации, может осуществляться доступ в Спецпомещения иных лиц из числа работников Института.

4.7. Работники органов МЧС и аварийных служб, врачи «скорой помощи» допускаются в Спецпомещения для ликвидации нештатной ситуации, иных чрезвычайных ситуаций или оказания медицинской помощи в сопровождении руководителя Подразделения или замещающего его лица.

4.8. Нахождение в Спецпомещениях посторонних лиц в нерабочее время запрещается.

Приложение 1
к Правилам доступа в помещения
ГБОУ ИРО Краснодарского края,
в которых ведется обработка
защищаемой информации, в том
числе персональных данных

ФОРМА

ПЕРЕЧНЬ
помещений, в которых разрешена обработка
конфиденциальной информации
(в том числе персональных данных)

№ п/п	Наименование структурного подразделения	№ кабинета	Ответственное лицо (Ф.И.О., должность)	Подпись
1	2	3	4	5

Приложение 2
к Правилам доступа в помещения
ГБОУ ИРО Краснодарского края,
в которых ведется обработка
защищаемой информации, в том
числе персональных данных

ФОРМА

ПЕРЕЧНЬ
лиц, допущенных в помещения обработки конфиденциальной информации (в том числе персональных данных)

№ п/п	Наименование структурного подразделения	№ кабинета	Ф.И.О. работника	Должность
1	2	3	4	5

Приложение 3
к Правилам доступа в помещения
ГБОУ ИРО Краснодарского края,
в которых ведется обработка
защищаемой информации, в том
числе персональных данных

ФОРМА

ПЕРЕЧНЬ
мест хранения материальных носителей конфиденциальной информаций (в том числе персональных данных) и лиц, ответственных за их сохранность

№ п/п	Наименование структурного подразделения	Место хранения (номер помещения, № сейфа/шкафа)	Ответственное лицо (ФИО, должность)	Подпись
1	2	3	4	5

Приложение 4
к правилам доступа в помещения
ГБОУ ИРО Краснодарского края,
в которых ведется обработка
защищаемой информации, в том
числе персональных данных

ФОРМА

ЖУРНАЛ
доступа в серверное помещение

№ п/п	Номер помещения	Название организации (проводящей работы) Ф.И.О. и должность работника	Перечень проводимых работ и оборудования, к которому осуществляется доступ	Основание проводимых работ	Дата и время		Ф.И.О. должность работника, сопровождающего третье лицо	Подпись
					начала работ	завершения работ		
1	2	3	4	5	6	7	8	9