МИНИСТЕРСТВО ОБРАЗОВАНИЯ, НАУКИ И МОЛОДЕЖНОЙ ПОЛИТИКИ РЕСПУБЛИКИ КОМИ
Государственное образовательное учреждение дополнительного профессионального образования
«Коми республиканский институт развития образования»

УТВЕРЖДЕНО
Приказом от 15.01.2019 № 3-пд/зпд

ПОЛОЖЕНИЕ
об обработке персональных данных
в ГОУДПО «КРИРО»

Рег. № 12

1. Общие положения

1.1. Настоящее Положение разработано в соответствии с Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Гражданским кодексом Российской Федерации, Федеральным законом № 149-ФЗ от 26.07.2006 г. «Об информации, информационных технологиях и о защите информации», Федеральным законом «О персональных данных» от 27.07.06 № 152-ФЗ и другими нормативными правовыми актами и определяет порядок обработки персональных данных всех субъектов персональных данных, данные которых подлежат обработке в ГОУДПО «КРИРО» (далее – Институт или оператор).

1.2. Требования настоящего Положения являются неотъемлемой частью комплекса мер безопасности и защиты информации в Институте.

1.3. Положение раскрывает способы и принципы обработки Институтом персональных данных, права и обязанности Института при обработке персональных данных, права субъектов персональных данных.

1.4. Положение обязательно для исполнения всеми лицами, непосредственно осуществляющими обработку персональных данных. Нарушение порядка обработки персональных данных, определенного Положением, влечет материальную, дисциплинарную, гражданскую, административную и уголовную ответственность в соответствии с нормами действующего законодательства Российской Федерации.

1.5. Положение распространяется, в том числе, на обработку обезличенных данных, а также персональных данных, сделанных общедоступными субъектом персональных данных.

1.6. Все персональные данные, обрабатываемые Институтом, за исключением обезличенных персональных данных и персональных данных, сделанных общедоступными субъектом персональных данных, признаются информацией ограниченного доступа.

1.7. Требования настоящего Положения распространяются на всех работников структурных подразделений, осуществляющих обработку персональных данных в Институте.

2. Основные термины, сокращения и определения

2.1. Обработка персональных данных — действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

2.2. Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

2.3. Конфиденциальность персональных данных — обязательное для соблюдения назначенного ответственного лица, получившего доступ к

персональным данным, требование не допускать их распространения без согласия субъекта или иного законного основания.

2.4. Распространение персональных данных — действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

2.5. Использование персональных данных — действия (операции) с персональными данными, совершаемые должностным лицом Института в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъектов либо иным образом затрагивающих их права и свободы или права и свободы других лиц.

2.6. Блокирование персональных данных — временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи.

2.7. Уничтожение персональных данных — действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

2.8. Обезличивание персональных данных — действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту.

2.9. Общедоступные персональные данные — персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

2.10. Информация — сведения (сообщения, данные) независимо от формы их представления.

3. Состав персональных данных

3.1. В состав персональных данных субъектов Института входят:

3.1.1. Фамилия, имя, отчество.

3.1.2. Дата рождения

3.1.3. Место рождения

3.1.4. Адрес.

3.1.5. Семейное, социальное и имущественное положение.

3.1.6. Образование и специальность.

3.1.7. Профессия.

3.1.8. Должность.

3.1.9. Заработная плата (оклад, премии, надбавки).

3.1.10. Номера банковских расчетных счетов.

3.1.11. Сведения о социальных льготах.

3.1.12. Судимости и/или наличие обязательств по исполнительным листам.

3.1.13. Паспортные данные.

3.1.14. ИНН.

3.1.15. Информация о воинской обязанности.

3.1.16. Данные страхового полиса обязательного медицинского страхования.

3.1.17. Данные страхового полиса обязательного пенсионного страхования.

3.1.18. Трудовой и общий стаж.

3.1.19. Данные о предыдущих местах работы.

3.1.20. Фотография.

3.1.21. Адрес электронной почты.

3.1.22. Телефон (домашний, сотовый).

3.1.23. Фамилия, имя отчество, дата рождения детей.

3.2. В Институте создаются и хранятся следующие документы, содержащие данные о субъектах персональных данных:

3.2.1. Унифицированная форма Т-2 «Личная карточка работника».

3.2.2. Личное дело работника.

3.2.3. Приказы ректора по кадровому составу.

3.2.4.Докладные записки, объяснительные записки нарушителей трудовой дисциплины.

3.2.5.Книга учета личного состава.

3.2.6. Книга учета принятых и уволенных работников.

3.2.7. Трудовые книжки.

3.2.8. Резюме соискателя – субъекта персональных данных.

3.2.9. Заявления работника – субъекта персональных данных.

3.2.10. Договора на оказание услуг со сторонними организациями.

3.2.11. Списки работников, подлежащих периодическому медицинскому осмотру.

3.2.12. Направления на плановые медосмотры.

3.2.13. Направления на обучение и курсы повышения квалификации.

3.2.14. Журнал регистрации вводного инструктажа.

3.2.15. Материалы расследований несчастных случаев на производстве.

3.2.16. Дипломы и иные документы об образовании.

3.2.17. Журнал учета посетителей.

3.2.18. Командировочные удостоверения

3.2.19. Больничные листы.

3.2.20. Табеля учета рабочего времени.

3.2.21. Визитные карточки работников.

3.3. Ректор назначает лицо, ответственное за организацию обработки персональных данных (далее – ответственное лицо), которое при осуществлении своих функций руководствуется действующим законодательством Российской Федерации, настоящим Положением и Политикой в отношении организации обработки и обеспечения

безопасности персональных данных», своей должностной инструкцией и иным локальными нормативными актами Института в сфере организации обработки и обеспечения безопасности персональных данных.

3.4.Ректором по предложению ответственного лица формируется рабочая группа, состоящая из работников Института. В состав рабочей группы должны входить представители структурных подразделений, в которых обрабатываются персональные данные, а также ответственный работник, на которого возложены обязанности по учету машинных носителей персональных данных. Руководство рабочей группой осуществляется ответственным лицом.

3.5.Решения об инициации новых процессов обработки персональных данных или внесении изменений в существующие процессы обработки персональных данных согласовываются с ответственным лицом.

3.6.Доступ к персональным данным имеют работники Института, которые обязаны осуществлять их обработку в связи с исполнением своих должностных обязанностей.

3.7.Перечень работников Института, осуществляющих обработку персональных данных определяется ответственным лицом и утверждается ректором (является приложением к настоящему Положению).

3.8.Процедура предоставления доступа работника к персональным данным предусматривает:

3.8.1. Подачу руководителем структурного подразделения служебной записки в адрес ответственного лица с указанием фамилии, имени, отчества, должности и подразделения работника, действия (действий) по обработке персональных данных, в котором будет участвовать работник, описания выполняемых работником функций по обработке персональных данных;

3.8.2. Ознакомление работника под роспись с настоящим Положением, другими локальными актами Института по вопросам обработки персональных данных, а также локальными актами, устанавливающими процедуры, направленные на выявление нарушений законодательства Российской Федерации в области обработки и защиты персональных данных и устранение последствий таких нарушений;

3.8.3. Информирование работника о категориях обрабатываемых персональных данных, об особенностях и правилах осуществления обработки персональных данных;

3.8.4. Фиксация в письменной форме обязательства работника, включающего положения:

3.8.4.1. об обеспечении конфиденциальности и безопасности персональных данных, непосредственно обрабатываемых работником;

3.8.4.2. о прекращении обработки персональных данных, ставших известными в связи с исполнением должностных обязанностей, в случае расторжения с работником государственного контракта, муниципального контракта или трудового договора.

3.8.5. Проведение инструктажа и регистрацию ответственным лицом

факта проведения инструктажа в «Журнале учёта проведения инструктажей работников по соблюдению правил обработки и защиты персональных данных».

3.9. В случае увольнения, перевода на другую должность или изменения должностных обязанностей работника, обрабатывающего персональные данные, а также изменении организационно-штатной структуры, руководитель работника, обрабатывающего персональные данные, уведомляет об этом ответственное лицо. Рабочей группой по указанию ответственного лица осуществляется пересмотр прав доступа работника к персональным данным и при необходимости вносятся соответствующие изменения в Перечень работников, допущенных к обработке персональных данных.

3.10. При увольнении работника, имеющего доступ к персональным данным, документы и иные носители, содержащие персональные данные, передаются другому работнику, имеющему доступ к персональным данным по указанию ректора увольняющегося работника.

3.11. Ответственное лицо не реже одного раза в месяц осуществляет проверку/актуализацию Перечня работников, допущенных к обработке персональных данных, а также списка пользователей ИСПДн, электронного журнала обращений пользователей ИСПДн на получение персональных данных. В случае выявления работников, допущенных к обработке персональных данных, которым такой доступ больше не требуется, права доступа такого работника к персональным данным незамедлительно отзываются.

3.12. Допуск работников к обработке персональных данных до прохождения процедуры предоставления доступа запрещается.

3.13. Доступ работников к своим персональным данным осуществляется в соответствии с Федеральным законом «О персональных данных» и трудовым законодательством.

4. Цель обработки персональных данных

4.1. Целью обработки персональных данных субъектов является соблюдение трудового законодательства РФ, законодательства РФ об охране труда и техники безопасности, законодательства РФ об охране здоровья, заключение и исполнение договоров, стороной которых являются субъекты персональных данных, организация однократного пропуска субъекта персональных данных на территорию, на которой находится оператор, зачисление заработной платы работников на банковские карты, выпуск визитных карточек, размещение контактных данных руководителей на сайте Института.

4.2. Условием прекращения обработки персональных данных является ликвидация Института.

5. Сбор, обработка и защита персональных данных

5.1. Порядок получения (сбора) персональных данных:

5.1.1. Все персональные данные субъекта следует получать у него лично с его письменного согласия, кроме случаев, определенных в п. 5.1.4 и 5.1.6 настоящего Положения и иных случаях, предусмотренных законами.

5.1.2. Форма заявления-согласия субъекта, являющегося работником Института, на обработку персональных данных представлена в приложении № 1 к настоящему положению. Форма заявления-согласия субъекта, не являющегося работником Института (слушатели), на обработку персональных данных представлена в приложении № 2 к настоящему положению.

5.1.3. Согласие субъекта на обработку персональных данных действует в течение неопределенного срока Отзыв согласия на обработку персональных данных представлен в приложении № 3 к настоящему положению.

5.1.4. Если персональные данные субъекта возможно получить только у третьей стороны, субъект должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие (Приложение № 4 к настоящему положению). Третье лицо, предоставляющее персональные данные субъекта, должно обладать согласием субъекта на передачу персональных данных Института. Институт обязан получить подтверждение от третьего лица, передающего персональные данные субъекта персональных данных о том, что персональные данные передаются с согласия субъекта. Института обязан при взаимодействии с третьими лицами заключить с ними соглашение о конфиденциальности информации, касающейся персональных данных субъектов.

5.1.5. Институт обязан сообщить субъекту персональных данных о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа субъекта персональных данных дать письменное согласие на их получение.

5.1.6. Обработка персональных данных субъектов без их согласия осуществляется в следующих случаях:

5.1.6.1. Персональные данные являются общедоступными.

5.1.6.2. По требованию полномочных государственных органов в случаях, предусмотренных федеральным законом.

5.1.6.3. Обработка персональных данных осуществляется на основании федерального закона, устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия оператора.

5.1.6.4. Обработка персональных данных осуществляется в целях заключения и исполнения договора, одной из сторон которого является субъект персональных данных.

5.1.6.5. Обработка персональных данных осуществляется для статистических целей при условии обязательного обезличивания персональных данных.

5.1.6.6. В иных случаях, предусмотренных законом.

5.1.7. Институт не имеет права получать и обрабатывать персональные данные субъекта о его расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, интимной жизни.

5.2. Порядок обработки персональных данных:

5.2.1. Субъект персональных данных предоставляет сотруднику Института, уполномоченному вести обработку персональных данных, достоверные сведения о себе.

5.2.2. На основании полученной информации сотрудник Институт проверяет наличие данного субъекта, зарегистрированного в информационной системе. Если субъект отсутствует в информационной системе, то операционный сотрудник заносит полную информацию о субъекте, после получения письменного согласия последнего. В случае наличия информации о субъекте в информационной системе – сверяет данные с ранее предоставленными (при необходимости вносит соответствующие изменения).

5.2.3. Своевременно, в срок не превышающий пяти рабочих дней, субъект персональных данных обязан лично или через своего законного представителя сообщать работнику, ответственному за сбор информации, об изменениях своих персональных данных с предоставлением соответствующих документов.

5.2.4. Институт обязуется прекратить обработку персональных данных в случае увольнения субъекта персональных данных.

5.3. Защита персональных данных:

5.3.1. Под защитой персональных данных субъекта понимается комплекс мер (организационно-распорядительных, технических, юридических), направленных на предотвращение неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных субъектов, а также от иных неправомерных действий.

5.3.2. Защита персональных данных субъекта осуществляется за счёт Институт в порядке, установленном соответствующими федеральными законами и внутренними организационными документами Института.

5.3.3. Институт при защите персональных данных субъектов принимает все необходимые организационно-распорядительные, юридические и технические меры, в том числе:

5.3.3.1. Шифровальные (криптографические) средства при передаче персональных данных.

5.3.3.2. Антивирусная защита.

5.3.3.3. Организация режима обеспечения безопасности помещений, в которых размещена информационная система и обрабатываются персональные данные, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения, а именно:

- Запрещение нахождение работников в таких помещениях, в целях, не связанных со служебной деятельностью;
- Нахождение лиц, не участвующих в обработке персональных данных в таких помещениях возможно только в присутствии лиц, осуществляющих обработку персональных данных;
- После исполнения своих обязанностей в таких помещениях работнику необходимо убрать все документы ограниченного пользования в специально отведенное для этого место, выключить всю аппаратуру, если это не препятствует технологическому процессу обработки информации, запереть помещение и произвести его опечатывание.
- При начале работы, а также после продолжительного отсутствия на рабочем месте следует проверить отсутствие несанкционированного доступа в такое помещение, а при его обнаружении немедленно сообщить об этом факте руководству Института.

Перечень помещений, в которых обрабатываются персональные данные субъектов, приведен в Приложении № 5 к настоящему положению.

5.3.3.4. Обеспечение сохранности и учета носителей персональных данных.

5.3.3.5. Утверждение ректором перечня лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных обязанностей.

5.3.3.6. Назначение приказом ректора должностного лица, ответственного за обеспечение безопасности персональных данных в информационной системе и утверждение должностного регламента такого лица (Приложение № 6).

5.3.3.7. Создание резервных копий персональных данных.

5.3.3.8. Издание нормативно-методических локальных актов, регулирующих защиту персональных данных.

6. Блокировка, обезличивание, уничтожение персональных данных

6.1. Порядок блокировки и разблокировки персональных данных:

6.1.1. Блокировка персональных данных субъектов осуществляется с письменного заявления субъекта персональных данных.

6.1.2. Блокировка персональных данных подразумевает:

6.1.2.1. Запрет редактирования персональных данных.

6.1.2.2. Запрет распространения персональных данных любыми средствами (e-mail, сотовая связь, материальные носители).

6.1.2.3. Запрет использования персональных данных в массовых рассылках (sms, e-mail, почта).

6.1.2.4. Запрет открытия банковских счетов.

6.1.2.5. Изъятие бумажных документов, относящихся к субъекту персональных данных и содержащих его персональные данные из внутреннего документооборота Института и запрет их использования.

6.1.3. Блокировка персональных данных субъекта может быть временно снята, если это требуется для соблюдения законодательства.

6.1.4. Разблокировка персональных данных субъекта осуществляется с его письменного согласия или заявления.

6.1.5. Повторное согласие субъекта персональных данных на обработку его данных влечет разблокирование его персональных данных.

6.2. Порядок обезличивания и уничтожения персональных данных:

6.2.1. Обезличивание персональных данных субъекта происходит по письменному заявлению субъекта персональных данных, при условии, что все договорные отношения завершены и от даты окончания последнего договора прошло не менее 5 лет, для слушателей и иных сторонних лиц по истечении 3 лет.

6.2.2. При обезличивании персональные данные в информационных системах заменяются набором символов, по которому невозможно определить принадлежность персональных данных к конкретному субъекту.

6.2.3. Бумажные носители документов при обезличивании персональных данных уничтожаются. В случае невозможности уничтожения бумажных носителей, содержащих персональные данные как обезличиваемого субъекта, так и других субъектов персональных данных, персональные данные уничтожаются путем стирания или замазывания.

6.2.4. Операция обезличивания персональных данных субъекта необратима.

6.2.5. Институт обязан обеспечить конфиденциальность в отношении персональных данных при необходимости проведения испытаний информационных систем на территории разработчика и произвести обезличивание персональных данных в передаваемых разработчику информационных системах.

6.2.6. Уничтожение персональных данных субъекта подразумевает прекращение какого-либо доступа к персональным данным субъекта.

6.2.7. При уничтожении персональных данных субъекта работники Института не могут получить доступ к персональным данным субъекта в информационных системах.

6.2.8. Бумажные носители документов при уничтожении персональных данных уничтожаются, персональные данные в информационных системах обезличиваются. Персональные данные восстановлению не подлежат.

6.2.9. Операция уничтожения персональных данных необратима.

7. Передача и хранение персональных данных

7.1. Передача персональных данных:

7.1.1. Под передачей персональных данных субъекта понимается распространение информации по каналам связи и на материальных носителях.

7.1.2. При передаче персональных данных работники Института должны соблюдать следующие требования:

7.1.2.1. Не сообщать персональные данные субъекта в коммерческих целях. Обработка персональных данных субъектов в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи не допускается.

7.1.2.2. Осуществлять передачу персональных данных субъектов в пределах Института в соответствии с настоящим Положением, нормативно-технологической документацией и должностными инструкциями.

7.1.2.3. Разрешать доступ к персональным данным только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы для выполнения должностных обязанностей.

7.1.2.4. Передавать персональные данные субъекта представителям субъекта в порядке, установленном законодательством и нормативно-технологической документацией и ограничивать эту информацию только теми персональными данными субъекта, которые необходимы для выполнения указанными представителями их функции.

7.2. Хранение и использование персональных данных:

7.2.1. Под хранением персональных данных понимается существование записей в информационных системах и на материальных носителях.

7.2.2. Персональные данные субъектов обрабатываются и хранятся в информационных системах, а также на бумажных носителях в Институте.

7.2.3. Хранение персональных данных субъектов осуществляется отделом кадров, бухгалтерией, Отделами Института: Отделом организации и обеспечения деятельности, Отделом печатных, электронных и информационных ресурсов, профкомом, кафедрами Института: Общего образования, Дошкольного, дополнительного, специального и инклюзивного образования, Центрами Института: Центром технического образования, Профессионального развития педагогических кадров и профессионального образования, Научно-методического сопровождения программ и проектов в области образования, Сопровождения специального, инклюзивного образования и комплексной безопасности детей, Развития общего образования, социализации и воспитания личности, Информационных технологий в образовании, Аттестации педагогических работников, Республиканским методическим центром по развитию национальной системы квалификаций в Республике Коми, Региональным центром выявления и поддержки одаренных детей в области искусства, спорта и науки в Республике Коми, Лабораториями Института: Развития этнокультурного образования, Национальных проблем дошкольного образования, помощником ректора в части выполнения должностных обязанностей по ведению и учету текущей документации, содержащей персональные данные, а также подготовке к хранению данной информации на бумажных и электронных носителях с ограниченным доступом.

7.2.4 Личные дела хранятся в бумажном виде в папках, прошитые и пронумерованные по страницам. Личные дела хранятся в специально

отведенной секции сейфа, обеспечивающего защиту от несанкционированного доступа.

7.2.5. Структурные подразделения, хранящие персональные данные на бумажных носителях, обеспечивают их защиту от несанкционированного доступа и копирования согласно «Положению об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утвержденному постановлением правительства РФ 15 сентября 2008 г. № 687.

7.2.6. Срок хранения персональных данных субъекта определяется на основе соответствующих федеральных законов и внутренних нормативных документов Института.

8. Доступ к персональным данным

8.1. Право доступа к персональным данным субъектов имеют работники Института, входящие в перечень лиц, осуществляющих обработку персональных данных (Приложение № 7). Должностное лицо Института, имеющее доступ к обработке персональных данных фиксируется в журнале о допуске к персональным данным (Приложение № 8).

8.2. Работники Института, получившие доступ к персональным данным субъекта, обязаны использовать их лишь в целях, для которых сообщены персональные данные и обязаны соблюдать режим секретности (конфиденциальности) обработки и использования полученной информации (персональных данных субъектов).

8.3. К числу массовых потребителей персональных данных вне Института относятся государственные и негосударственные функциональные структуры: налоговые инспекции; правоохранительные органы; органы статистики; страховые агентства; военкоматы; органы социального страхования; пенсионные фонды; подразделения федеральных, республиканских и муниципальных органов управления. Надзорно-контрольные органы имеют доступ к информации только в сфере своей компетенции.

8.4. Организации, в которые субъект может осуществлять перечисления денежных средств (страховые Общества, негосударственные пенсионные фонды, благотворительные организации, кредитные учреждения) могут получить доступ к персональным данным субъекта только в случае его письменного разрешения.

8.3. Субъект может получить доступ к своим персональным данным на основании письменного запроса или при обращении, включая право на безвозмездное получение копий любой записи, содержащей персональные данные субъекта.

8.4. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с оператором (номер договора, дата заключения

договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных оператором, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

8.5. Обращение субъекта или поступивший запрос рассматривается должностным лицом Института, ответственным за обеспечение безопасности персональных данных в информационной системе.

8.6. В случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или персональных данных субъекту персональных данных или его представителю при их обращении либо при получении запроса субъекта персональных данных или его представителя ответственный за обеспечение безопасности персональных данных в информационной системе готовит в письменной форме мотивированный ответ, содержащий ссылку на положение 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.

8.7. Институт предоставляет безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных.

8.8. В срок, не более семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, Институт вносит в них необходимые изменения.

С этой целью ответственный за обеспечение безопасности персональных данных дает поручение должностному лицу Института, входящему в Перечень лиц, осуществляющих обработку персональных данных, внести изменения в персональные данные субъекта.

8.9. В срок, не более 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, Институт уничтожает такие персональные данные и уведомляет субъекта персональных данных или его представителя о внесенных изменениях и предпринятых.

8.10. Институт сообщает в уполномоченный орган по защите прав субъектов персональных данных по запросу этого органа необходимую информацию в течение тридцати дней с даты получения такого запроса.

9. Права оператора персональных данных

Институт вправе:

9.1. Отстаивать свои интересы в суде.

9.2. Предоставлять персональные данные субъектов третьим лицам, если это предусмотрено действующим законодательством (налоговые, правоохранительные органы и др.).

9.3. Отказать в предоставлении персональных данных в случаях предусмотренных законом.

9.4. Использовать персональные данные субъекта без его согласия, в случаях предусмотренных законом.

9.5. Осуществлять внутренний контроль за соблюдением настоящего Положения согласно должностному регламенту специалиста по обеспечению безопасности персональных данных.

9.6. Проводить расследование инцидентов безопасности персональных данных на основании принятого в организации Регламента реагирования на инциденты информационной безопасности.

10. Права субъекта персональных данных

Субъект персональных данных имеет право:

10.1. Требовать уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав;

10.2. Требовать перечень обрабатываемых персональных данных, имеющихся в Институт и источник их получения.

10.3. Получать информацию о сроках обработки персональных данных, в том числе о сроках их хранения.

10.4. Требовать извещения всех лиц, которым ранее были сообщены неверные или неполные его персональные данные, обо всех произведенных в них исключениях, исправлениях или дополнениях.

10.5. Обжаловать в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке неправомерные действия или бездействия при обработке его персональных данных.

11. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных

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

11.2. Работники Института, осуществляющие обработку персональных данных, обязаны подписать соглашение о неразглашении персональных данных. Форма соглашения о неразглашении персональных данных представлена в приложении № 9 настоящего положения.

11.3. Работники, виновные в нарушении норм, регулирующих обработку персональных данных, несут административную ответственность по ст.ст. 13.11, 13.14 Кодекса об административных правонарушениях РФ.

11.4. Предоставление персональных данных посторонним лицам, в том числе, работникам Института, не имеющим права их обрабатывать, распространение персональных данных, утрата материальных носителей информации, содержащих персональные данные субъекта, а также иные нарушения обязанностей по обработке персональных данных, установленных настоящим Положением, локальными нормативными актами Института, влечет наложение на работника, имеющего доступ к персональным данным, дисциплинарного взыскания: замечания, выговора или увольнения.

11.5. Работник, имеющий доступ к персональным данным субъектов и совершивший указанный дисциплинарный проступок, несет полную материальную ответственность в случае причинения его действиями ущерба Институту (п. 7 ст. 243 Трудового кодекса РФ).

11.6. Работники, имеющие доступ к персональным данным субъектов, виновные в незаконном сборе или передаче персональных данных, а также осуществившие неправомерный доступ к охраняемой законом компьютерной информации, несут уголовную ответственность в соответствии со ст.ст. 137, 272 Уголовного кодекса РФ.

12. Заключительные положения

Настоящее Положение вступает в силу после его утверждения ректором. Все изменения в Положение вносятся на основании решения ректора в установленном порядке.

Приложение №1
к положению об обработке
персональных данных в ГОУДПО «КРИРО»

Ректору ГОУДПО «КРИРО»
Г.В. Китайогородской

Заявление-согласие
субъекта на обработку его персональных данных

Я, _____,
(Ф.И.О. полностью)
паспорт серии _____, номер _____, выданный _____
_____ «___» _____ ____ г.,
зарегистрированный (ая) по адресу: _____,

в соответствии со ст. 9 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» даю согласие ГОУДПО «КРИРО», расположенному по адресу: 167982, г. Сыктывкар, ул. Орджоникидзе, 23 (далее – оператор), на автоматизированную, а также без использования средств автоматизации обработку моих персональных данных, а именно:

фамилия, имя, отчество; дата рождения; место рождения; адрес; семейное, социальное и имущественное положение; образование и специальность; профессия; должность; заработная плата (оклад, премии, надбавки); номера банковских расчетных счетов; сведения о социальных льготах; судимости и/или наличие обязательств по исполнительным листам; паспортные данные; ИНН; информация о воинской обязанности; данные страхового полиса обязательного медицинского страхования; данные страхового полиса обязательного пенсионного страхования;

трудовой и общий стаж; данные о предыдущих местах работы; фотография; адрес электронной почты; телефон (домашний, сотовый); фамилия, имя отчество, дата рождения детей.

для обработки с целью: соблюдения трудового законодательства РФ, законодательства РФ об охране труда и техники безопасности, законодательства РФ об охране здоровья, заключения и исполнение договоров, стороной которых являются субъекты персональных данных, организация пропуска на территорию, на которой находится оператор, зачисления заработной платы работников на банковские карты, выпуск визитных карточек, размещения контактных данных руководителей на сайте Организации.

Перечень действий с персональными данными, на совершение которых дается согласие:

- сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение.

Я утверждаю, что ознакомлен с документами организации, устанавливающими порядок обработки персональных данных, а также с моими правами и обязанностями в этой области.

Согласие вступает в силу со дня его подписания и действует в течение неопределенного срока. Согласие может быть отозвано мною в любое время на основании моего письменного заявления.

Об ответственности за достоверность представленных сведений предупрежден(а).

«___» _____ 20__ г. _____
(подпись)

Приложение № 2
к положению об обработке
персональных данных в ГОУДПО «КРИРО»
(к Заявлению на обучение)

Ректору ГОУДПО «КРИРО»
Г.В. Китайгородской

Я, _____,
(Ф.И.О. полностью)
_____
(должность и место работы)

Даю согласие на обработку своих персональных данных в соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»

«___» _____ 20__ г. _____
(подпись)

Приложение № 3
к положению об обработке
персональных данных в ГОУДПО «КРИРО»

Ректору ГОУДПО «КРИРО»
Г.В. Китайгородской.

Отзыв согласия на обработку персональных данных

Я, _____,
(Ф.И.О. полностью)

паспорт серии _____, номер _____, выданный _____ _____ «___» _____ ____ г., зарегистрированный (ая) по адресу: _____,

Прошу Вас прекратить обработку моих персональных данных в связи с
_____
(указать причину)

начиная с «___» _____ 20__ г.

«___» _____ 20__ г. _____
(подпись)

Приложение № 4
к положению об обработке
персональных данных в ГОУДПО «КРИРО»

Ректору ГОУДПО «КРИРО»
Г.В. Китайгородской

Заявление-согласие
субъекта на получение его персональных данных у третьей стороны

Я, _____,
(Ф.И.О. полностью)
паспорт серии _____, номер _____, выданный
_____
«___» _____ ____ г.,
в соответствии со ст.ст. 86-88 Трудового Кодекса Российской Федерации на получение, использование и хранение моих персональных данных, _____
(согласен/не согласен)
а именно:
_____
_____
(указать состав персональных данных (Ф.И.О, паспортные данные, адрес и т.д.)
для обработки в целях _____
_____
_____ ,
(указать цели обработки)
у следующих лиц _____
_____
_____
(указать Ф.И.О. физического лица или наименование организации, которым сообщаются данные)

Я также утверждаю, что ознакомлен с возможными последствиями моего отказа дать письменное согласие на их получение.

«___» _____ 20__ г. _____
(подпись)

Приложение № 5
к положению об обработке
персональных данных в ГОУДПО «КРИРО»

Перечень помещений,
в которых обрабатываются и хранятся персональные данные в ГОУДПО «КРИРО»

№ п /п	Наименование структурного подразделения	Расположение помещения (№ кабинета)
1	Приемная ректора	Административное здание, кабинеты №№ 201-202
2	Отдел кадров	Административное здание, кабинет № 210
3	Отдел финансово-экономической деятельности и бухгалтерского учета	Административное здание, кабинеты №№ 203, 205, 207, 208, 211
4	Отдела организации и обеспечения деятельности	Административное здание, кабинет № 212
5	Помещение серверной	Административное здание, кабинет №215
6	Архив Института	Административное здание, цокольный этаж (подвальное помещение)

Приложение № 6
к положению об обработке
персональных данных в ГОУДПО «КРИРО»

ДОЛЖНОСТНОЙ РЕГЛАМЕНТ
лица, ответственного за обеспечение безопасности персональных данных ГОУДПО «КРИРО»

1.Общие положения

1.1. Настоящий должностной регламент лица, ответственного за обеспечение безопасности персональных данных (далее – Регламент) определяет основные цели, функции и права лиц, ответственных за обеспечение безопасности персональных данных (далее – Специалист) в ГОУДПО «КРИРО» (далее – Институт).

1.2. Специалист назначается приказом ректора на основании Положения о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам, утвержденного постановлением Совета Министров – Правительства Российской Федерации от 15 сентября 1993 г. № 912-51, во исполнение Федерального Закона от 27.07.2006 г. № 152-ФЗ «О персональных данных»

1.3. Специалист проводит свою работу согласно нормативным методическим документам Федеральной службы по техническому и экспортному контролю России, Федеральной службы безопасности России и иных уполномоченных законодательством органов в области обеспечения безопасности персональных данных.

1.4. Непосредственное руководство работой специалиста осуществляет ректор. Назначение и освобождение от полномочий специалиста производится ректором Института.

1.5. Работа специалиста проводится в соответствии с планами работ, утверждаемыми ректором Института.

1.6. В своей работе специалист руководствуется законодательными и иными нормативными актами Российской Федерации в области обеспечения безопасности персональных данных, приказами и указаниям ректора и другими руководящими документами по обеспечению безопасности персональных данных.

2. Основные функции специалиста

2.1. Проведение единой политики, организация и координация работ по обеспечению безопасности персональных данных в Институте.

2.2. Проведение мероприятий по организации обеспечения безопасности персональных данных, включая классификацию информационных систем персональных данных.

2.3. Проведение мероприятий по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, в том числе:

– мероприятия по размещению, охране, организации режима допуска в помещения, где ведется обработка персональных данных;

– мероприятия по закрытию технических каналов утечки персональных данных при их обработке;

– мероприятия по защите от несанкционированного доступа к персональным данным

– мероприятия по выбору средств защиты персональных данных при их обработке.

2.4. Проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным или передачи их лицам, не имеющим права доступа к такой информации.

2.5. Своевременное обнаружение фактов несанкционированного доступа к персональным данным.

2.6. Недопущение воздействия на технические средства обработки персональных данных, в результате которого может быть нарушено их функционирование.

2.7. Обеспечение возможности восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

2.8. Постоянный контроль над обеспечением уровня защищенности персональных данных.

2.9. Участие в подготовке объектов соответствующей организации к аттестации по выполнению требований обеспечения безопасности персональных данных.

2.10.Разработка организационных распорядительных документов по обеспечению безопасности персональных данных в соответствующей организации.

2.11.Организация в установленном порядке расследования причин и условий появления нарушений в безопасности персональных данных и разработка предложений по устранению недостатков и предупреждению подобного рода нарушений, а также осуществление контроля над устранением этих нарушений.

2.12.Разработка предложений, участие в проводимых работах по совершенствованию системы безопасности персональных данных в соответствующей организации.

2.13.Проведение периодического контроля эффективности мер защиты персональных данных в соответствующей организации. Учет и анализ результатов контроля.

2.14.Организация повышения осведомленности руководства и работников Института по вопросам обеспечения безопасности персональных данных, работников сторонних учреждений и организаций.

2.15.Подготовка отчетов о состоянии работ по обеспечения безопасности персональных данных.

2.16. Рассмотрение обращений субъекта персональных данных или его законного представителя и поступивших запросов, относящихся к субъектам персональных данных.

3. Права специалиста

3.1. Специалист имеет право:

- Запрашивать и получать необходимые материалы для Института и проведения работ по вопросам обеспечения безопасности персональных данных.
- Разрабатывать проекты организационных и распорядительных документов по обеспечению безопасности персональных данных.
- Готовить предложения о привлечении к проведению работ по защите информации на договорной основе организаций, имеющих лицензии на право проведения работ в области защиты информации.
- Контролировать деятельность структурных подразделений Института в части выполнения ими требований по обеспечению безопасности персональных данных.
- Вносить предложения ректору о приостановке работ в случае обнаружения несанкционированного доступа, утечки (или предпосылок для утечки) персональных данных.
- Привлекать в установленном порядке необходимых специалистов из числа работников Института для проведения исследований, разработки решений, мероприятий и организационно-распорядительных документов по вопросам обеспечения безопасности персональных данных.

4. Ответственность специалиста

4.1. Специалист несет персональную ответственность за:

- правильность и объективность принимаемых решений;
- правильное и своевременное выполнение приказов, распоряжений, указаний руководства Института по вопросам, входящим в возложенные на него функции;
- выполнение возложенных на него обязанностей, предусмотренных настоящим Регламентом;

соблюдение трудовой дисциплины, охраны труда;

- качество проводимых работ по обеспечению безопасности персональных данных в соответствии с функциональными обязанностями.
- согласно действующему законодательству Российской Федерации за разглашение сведений ограниченного распространения, ставших известными ему по роду работы.

Приложение № 7
к положению об обработке
персональных данных в ГОУДПО «КРИРО»

Соглашение о неразглашении
персональных данных субъекта

Я, _____,
(Ф.И.О. полностью)
паспорт серии _____, номер _____, выданный
_____ _____
«___» _____ ____ г.,

понимаю, что получаю доступ к персональным данным работников ГОУДПО «КРИРО» (далее – Институт) и членов их семей, а также иных физических лиц.

Я также понимаю, что во время исполнения своих обязанностей, мне приходится заниматься сбором, обработкой и хранением персональных данных.

Я понимаю, что разглашение такого рода информации может нанести ущерб субъектам персональных данных, как прямой, так и косвенный.

В связи с этим, даю обязательство, при работе (сбор, обработка и хранение) с персональными данными соблюдать все описанные в «Положении об обработке персональных данных» требования.

Я подтверждаю, что не имею права разглашать сведения, ставшие мне известными и перечисленные в п. 3.1 Положения об обработке персональных данных.

Я подтверждаю, что не имею права разглашать содержание документов, ставших мне известными и перечисленных в п. 3.2 Положения об обработке персональных данных.

Я предупрежден (а) о том, что в случае разглашения мной сведений, касающихся персональных данных или их утраты я несу ответственность в соответствии со ст. 24 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных».

«___» _____ 20__ г. _____
(подпись)