УТВЕРЖДЕНО
приказом ГАУ ДПО ПК ИРО
от 27.10.2022 года № 238-А

ПОЛОЖЕНИЕ

об обработке и защите персональных данных в государственном автономном учреждении дополнительного профессионального образования «Приморский краевой институт развития образования»

1. Общие положения

1.1. Назначение и область действия документа.

Настоящее положение об обработке и защите персональных данных (далее – Положение) в государственном автономном учреждении дополнительного профессионального образования «Приморский краевой институт развития образования» (далее – Учреждение) определяет порядок сбора, хранения, передачи, использования, уничтожения и любых других видов обработки персональных данных субъектов персональных данных в Учреждении.

Настоящее Положение разработано в соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», 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 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Трудовым кодексом Российской Федерации.

Цель данного Положения – определение порядка обработки персональных данных субъектов персональных данных в Учреждении.

Юридические и физические лица, в соответствии со своими полномочиями владеющие, получающие и использующие информацию о субъектах персональных данных, несут гражданскую, уголовную, административную, дисциплинарную и иную, предусмотренную законодательством Российской Федерации, ответственность за нарушение правил обработки и защиты этой информации.

Настоящее положение вступает в силу с момента его утверждения ректором Учреждения и действует бессрочно до замены его новым Положением.

Все изменения в Положение вносятся приказом ректора Учреждения.

Все сотрудники Учреждения, имеющие доступ к персональным данным субъектов персональных данных, в обязательном порядке должны быть ознакомлены с настоящим Положением под роспись, для последующего его исполнения.

2. Основные понятия и состав персональных данных

2.1. Термины и определения.

Автоматизированная обработка персональных данных – обработка персональных данных с использованием средств вычислительной техники.

Безопасность – состояние защищённости жизненно важных интересов личности, общества и государства от внутренних и внешних угроз.

Безопасность информации – состояние защищённости информации, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность информации.

Блокирование информации – временное прекращение сбора, систематизации, накопления, использования, распространения информации, в том числе её передачи.

Доступ к информации – возможность получения информации и ее использования.

Жизненно важные интересы – совокупность потребностей, удовлетворение которых надежно обеспечивает существование и возможности прогрессивного развития личности, общества и государства.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

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

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

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Обладатель информации – лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.

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 лицу (субъекту персональных данных).

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

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

Средства вычислительной техники - совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

Уничтожение информации – действие, в результате которого невозможно восстановить содержание информации в информационной системе или в результате которого уничтожаются материальные носители информации.

Целостность информации – способность средства вычислительной техники или информационной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

2.2. Определение перечня персональных данных, обрабатываемых в ГАУ ДПО ПК ИРО.

В Учреждении обрабатываются персональные данные следующих категорий субъектов персональных данных.

2.2.1. Персональные данные II-й категории участников государственной итоговой аттестации (далее – участники ГИА).

Обработка персональных данных участников ГИА осуществляется в целях реализации проведения государственной итоговой аттестации по образовательным программам общего образования в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральным законом от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации» и других нормативно-правовых актов.

В Учреждении с помощью средств автоматизации обрабатываются следующие категории персональных данных лиц, проходящих тестирование:

- фамилия, имя, отчество;
- документ, удостоверяющий личность;
- пол;
- дата рождения;
- гражданство;
- СНИЛС;
- отметка об ограниченных возможностях здоровья;
- образовательная организация;
- класс;
- форма обучения;
- сведения о допуске ГИА;
- выбранные экзамены;
- профильные предметы;
- предметы, преподаваемые по сокращенной программе;
- назначения на экзамены ППЭ;
- сведения об апелляциях;
- результаты ГИА;
- сведения об экспертизе ГИА.

Срок хранения вышеуказанных персональных данных – 10 лет.

2.2.2. Персональные данные II-й категории лиц, проводящих верификацию результатов тестирования.

Обработка персональных данных лиц, проводящих верификацию результатов тестирования, осуществляется в целях реализации проведения государственной итоговой аттестации по образовательным программам общего образования в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральным законом от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации» и других нормативно-правовых актов.

В Учреждении обрабатываются следующие категории персональных данных лиц, проводящих верификацию результатов тестирования:

- фамилия, имя, отчество;
- документ, удостоверяющий личность;
- пол;
- дата рождения;
- гражданство;
- СНИЛС;
- место работы;
- уровень образования
- квалификация;
- должность;
- стаж работы;
- предметная специализация;
- сведения о планировании ГИА.

Срок хранения вышеуказанных персональных данных – 10 лет.

2.2.3. Персональные данные II-категории работников Учреждения.

Обработка персональных данных работников осуществляется в целях:

- организации кадрового учета, обеспечения соблюдения законов и иных нормативно-правовых актов;

- ведения делопроизводства, исполнения требований налогового законодательства в связи с исчислением и уплатой налога на доходы физических лиц, а также единого социального налога, пенсионного законодательства при формировании и представлении персонифицированных данных о каждом получателе доходов, учитываемых при начислении страховых взносов на обязательное пенсионное страхование и обеспечение, заполнения первичной статистической документации в соответствии с Трудовым кодексом Российской Федерации, Налоговым кодексом Российской Федерации, федеральными законами, в частности: «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования», «О персональных данных» и других нормативно-правовых актов.

В Учреждении обрабатываются следующие категории персональных данных работников:

– фамилия, имя, отчество;

– пол;

– дата и место рождения;

– гражданство;

– реквизиты документа, удостоверяющего личность (серия и номер документа, удостоверяющего личность, сведения о дате выдачи указанного документа и выдавшем его органе);

– страховой номер индивидуального лицевого счёта (СНИЛС);

– индивидуальный номер налогоплательщика (ИНН);

– сведения об образовании (вид образования, название учебного заведения, наименование документа об образовании, серия и номер бланка документа об образовании, регистрационный номер документа об образовании, год окончания, форма обучения, направление обучения или специальность, присвоенная квалификация или отметка о праве заниматься соответствующей деятельностью);

– сведения о присвоении ученого звания;

– сведения о присвоении ученой степени;

– сведения о повышении квалификации или профессиональной переподготовке;

– сведения о состоянии в браке;

– сведения о наличии детей;

– сведения о перемене фамилии, имени отчества;

– сведения о предыдущей трудовой деятельности (наименование организации, занимаемая должность, квалификационная категория, период работы, общий стаж работы, педагогический стаж, контактная информация организации);

– сведения о трудовой деятельности в ГАУ ДПО ПК ИРО (наименование структурного подразделения, должность, реквизиты приказа по личному составу, размер оклад, дополнительные начисления, условия труда, режим работы);

– профессия работника;

– сведения о начисленной и выплаченной заработной плате (иных выплат) работнику;

– сведения о налогах работника;

– сведения о временной нетрудоспособности работника;

– сведения об аттестации работника;

– сведения о наградах (поощрениях), почетных званиях;

– сведения об отпусках;

– сведения о социальных гарантиях;

– сведения о воинском учете;

– контактная информация: почтовый адрес, номер мобильного (домашнего, служебного) телефона, адрес электронной почты.

Срок хранения вышеуказанных персональных данных – 75 лет.

2.3. Общие принципы обработки.

Обработка персональных данных должна осуществляться на основе принципа соответствия объема и характера обрабатываемых персональных данных, а также способов обработки персональных данных заявленным целям обработки персональных данных.

Сбор, накопление, хранение, изменение, использование и распространение, а также другие действия, понимаемые под обработкой персональных данных, могут осуществляться только при условии письменного согласия физического лица, за исключением случаев, предусмотренных Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

Обработка персональных данных обрабатывается с помощью средств автоматизации.

Правила обработки персональных данных в государственной информационной системе (далее – ГИС) «РИС ГИА» установлены в «Инструкции администратора безопасности в ГИС «РИС ГИА» и «Инструкции пользователя ГИС «РИС ГИА».

2.4. Порядок сбора и хранения персональных данных.

При сборе персональных данных Учреждение обязано предоставить физическому лицу (субъекту персональных данных) по его запросу информацию о целях, способах обработки персональных данных, сведения о лицах, имеющих доступ к персональным данным, перечень обрабатываемых персональных данных и источник их получения, сведения о сроках обработки и хранения персональных данных.

Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных не дольше, чем этого требуют цели их обработки.

2.5. Передача персональных данных третьим лицам.

Передача персональных данных третьей стороне без письменного согласия субъекта персональных данных, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта персональных данных, а также в случаях, установленных Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», не допускается. Данное ограничение не распространяется на обмен персональными данными субъектов в порядке, установленном федеральными законами.

Передача персональных данных субъекта в коммерческих целях без его письменного согласия исключается. Обработка персональных данных субъекта в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи допускается только с его предварительного согласия.

Лица, получившие доступ к персональным данным субъекта, должны быть предупреждены о том, что эти данные могут быть использованы лишь в целях, для которых

они переданы, и обязаны соблюдать это правило. Лица, получившие персональные данные, обязаны соблюдать режим конфиденциальности.

2.6. Трансграничная передача персональных данных.

Трансграничная передача персональных данных Учреждением не осуществляется.

Все технические средства обработки персональных данных (рабочие станции и сервера) находятся в пределах Российской Федерации.

2.7. Порядок уничтожения и блокирования персональных данных.

Учреждение обязано прекратить обработку персональных данных и уничтожить их после достижения цели обработки или в случае отзыва субъектом персональных данных согласия на обработку, за исключением случаев, когда уничтожение противоречит федеральному законодательству, а также уведомить о своих действиях субъекта персональных данных и (или) уполномоченный орган. Во всех случаях предусмотрен срок уничтожения персональных данных – три рабочих дня.

Персональные данные, обрабатываемые в государственной информационной системе, удаляются путем стирания записи в базах данных администратором безопасности Учреждения по запросу субъекта или при достижении целей обработки персональных данных.

Временное прекращение операций по обработке персональных данных (блокирование) должно возникать по требованию субъекта персональных данных при выявлении им недостоверности обрабатываемых сведений или неправомерных действий в отношении его данных.

2.8. Защита персональных данных.

При обработке персональных данных Учреждение принимает организационные и технические меры для защиты персональных данных от неправомерных действий в соответствии с требованиями, устанавливаемыми Правительством Российской Федерации.

Защита персональных данных при их обработке в ГИС персональных данных регламентирована «Инструкцией администратора безопасности в ГИС «РИС ГИА», «Инструкцией пользователя ГИС «РИС ГИА» и другими внутренними документами Учреждения по защите информации.

Приказом ректора Учреждения «О назначении группы реагирования на инциденты информационной безопасности и о правилах регистрации инцидентов информационной безопасности и реагирования на них в ГИС «РИС ГИА» назначена группа реагирования на инциденты информационной безопасности.

В Учреждении разработана «Модель угроз безопасности ГИС «РИС ГИА», включающая в себя также модель нарушителя. Проведена классификации ГИС и персональных данных, обрабатываемых в ГИС. Для ГИС сформировано «Техническое задание на создание системы защиты информации в ГИС «РИС ГИА» и эскизный проект

«Создание системы защиты информации в ГИС «РИС ГИА», в которых описаны все организационные и технические меры, которые необходимо осуществить для нейтрализации актуальных угроз и выполнения требований действующего законодательства по защите конфиденциальной информации установленного класса защищенности.

2.9. Согласие на обработку персональных данных.

Со всех субъектов персональных данных собирается согласие на обработку их персональных данных в соответствии с законодательством Российской Федерации.

3. Доступ к персональным данным

3.1. Организация доступа работников к персональным данным субъектов.

Должностные лица Учреждения должны иметь доступ только к тем персональным данным, которые необходимы им для выполнения своих функциональных обязанностей.

В учреждении разработана и утверждена разрешительная система допуска к персональным данным («Положение о разграничении прав доступа в ГИС «РИС ГИА»). Круг лиц, допущенных к обработке персональных данных, определяет руководство Учреждения на основании данных, представленных руководителями подразделений, в которых ведется обработка персональных данных. Данный перечень утверждается ректором Учреждения.

Работники Учреждения допускаются к обработке персональных данных после ознакомления с настоящим Положением, «Инструкцией пользователя ГИС «РИС ГИА», а также с иной организационно-распорядительной документацией по защите персональных данных.

Работники учреждения перед началом обработки персональных данных подписывают «Соглашение о неразглашении персональных данных».

Запрещается получать согласие на обработку персональных данных путем бездействия субъекта. Согласие субъекта должно быть явным.

Доступ работников к обработке персональных данных осуществляется в соответствии с «Положение о разграничении прав доступа в ГИС «РИС ГИА».

В случае обнаружения нарушений правил обработки персональных данных руководство учреждения и/или администратор безопасности и/или ответственный за организацию обработки персональных данных обязаны приостановить предоставление персональных данных пользователям до выявления и устранения причин нарушений.

Лица, не имеющие доступа к персональным данным в соответствии с «Положением о разграничении прав доступа в ГИС «РИС ГИА», могут быть допущены к ним на основании приказа, подписанного ректором либо руководителем подразделения данного лица.

3.2. Организация доступа субъекта персональных данных к его персональным данным.

Учреждение, обрабатывающее персональные данные, должно обеспечивать бесплатный доступ субъекта к персональным данным, ему соответствующим, за исключением случаев получения персональных данных в результате оперативно-розыскной деятельности, а также других случаев, предусмотренных федеральным законодательством.

Для получения доступа к своим персональным данным субъекту необходимо направить в Учреждение запрос, содержащий паспортные данные субъекта персональных данных, в бумажной или электронной форме, подписанные собственноручно или электронной цифровой подписью.

Работники Учреждения должны предоставить персональные данные субъекту в доступной форме, в них не должны содержаться персональные данные, относящиеся к другим субъектам.

В случае если персональные данные субъекта являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, Учреждение обязано удовлетворить требование субъекта по устранению нарушений обработки персональных данных.

С целью организации своевременной обработки запросов и обращений субъектов персональных данных разработан и утвержден документ «Журнал учета обращений граждан-субъектов персональных данных о выполнении их законных прав».

4. Права и обязанности ГАУ ДПО ПК ИРО

4.1. Права и обязанности Учреждения.

В случае выявления недостоверных персональных данных или неправомерных действий с ними Учреждение при обращении или по запросу субъекта персональных данных или его законного представителя либо уполномоченного органа по защите прав субъектов персональных данных, обязано осуществить устранение допущенных нарушений или, в случае невозможности устранения, уничтожить персональные данные, а также уведомить о своих действиях субъекта персональных данных или уполномоченный орган.

Должностные лица, в обязанность которых входит обработка запросов и обращений субъектов персональных данных, обязаны обеспечить каждому субъекту возможность ознакомления с документами и материалами, содержащими их персональные данные, если иное не предусмотрено законом.

В случае предоставлении субъектом фактов о неполных, устаревших, недостоверных или незаконно полученных персональных данных Учреждение обязано

внести необходимые изменения, уничтожить или блокировать их, а также уведомить о своих действиях субъекта персональных данных.

Учреждение обязуется не принимать на основании исключительно автоматизированной обработки решения, порождающие юридические последствия в отношении субъектов персональных данных или иным образом затрагивающие их права и законные интересы.

По запросу уполномоченного органа по защите прав субъектов персональных данных Учреждение обязано предоставить ему необходимую информацию.

Сроки реагирования на запросы субъекта персональных данных – 10 рабочих дней, с возможностью продления ещё на 5 рабочих дней.

Учреждение не может отказать субъекту персональных данных в предоставлении информации, если он отказался предоставлять свои биометрические данные.

Учреждение не в праве ограничивать свободу и права субъекта персональных данных.

5. Права и обязанности работников ГАУ ДПО ПК ИРО

5.1. Общие положения.

Работники обязаны ознакомиться с документами, которые устанавливают порядок обработки персональных данных, и подписать лист ознакомления с ними, а также подписать соглашение о неразглашении персональных данных, полученных в ходе исполнения своих должностных обязанностей.

5.2. Права работника.

В целях защиты персональных данных, хранящихся в Учреждении, работник, осуществляющий обработку персональных данных, имеет право:

- получать и вводить информацию в соответствии с его полномочиями;

- требовать оповещения Учреждением субъекта персональных данных обо всех произведенных в них исключениях, исправлениях или дополнениях.

5.3. Обязанности работника.

5.3.1. В части обработки персональных данных субъекта:

- соблюдать режим конфиденциальности;

- не сообщать персональные данные субъекта персональных данных в коммерческих целях без его письменного согласия;

- не сообщать персональные данные субъекта третьей стороне без письменного согласия, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта, а также в случаях, установленных федеральным законом;

- разрешать доступ к персональным данным субъектов только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те

персональные данные работника, которые необходимы для выполнения конкретных функций;

- не запрашивать дополнительную информацию, содержащую персональные данные, за исключением тех сведений, которые необходимы для выполнения работником трудовых обязанностей.

6. Права субъектов персональных данных

6.1. Получение сведений об Учреждении.

Субъект персональных данных имеет право на получение сведений об Учреждении, о месте ее нахождения, наличии персональных данных, относящихся к нему, а также на ознакомление с такими персональными данными. Субъект персональных данных вправе требовать от Учреждения 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.

6.2. Доступ к своим персональным данным.

Доступ к своим персональным данным предоставляется субъекту персональных данных или его законному представителю Учреждения при обращении либо при получении запроса субъекта персональных данных или его законного представителя.

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

- подтверждение факта обработки персональных данных Учреждением, а также цель такой обработки;

- способы обработки персональных данных, применяемые Учреждением;

- сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;

- перечень обрабатываемых персональных данных и источник их получения;

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

- сведения о том, какие юридические последствия для субъекта персональных данных может повлечь за собой обработка его персональных данных.

Если субъект персональных данных считает, что Учреждение осуществляет обработку его персональных данных с нарушением требований федерального законодательства или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие Учреждения в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

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.

6.3. Ограничение прав субъектов персональных данных.

Право субъекта персональных данных на доступ к своим персональным данным ограничивается в случае, если:

- обработка персональных данных, в том числе персональных данных, полученных в результате оперативно-розыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;

- предоставление персональных данных нарушает конституционные права и свободы других лиц.

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

7.1. Общие положения.

Юридические и физические лица в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность за нарушение режима защиты, обработки и порядка использования этой информации.

Неправомерность деятельности органов государственной власти и организаций по сбору персональных данных может быть установлена в судебном порядке по требованию субъекта персональных данных, действующего на основании законодательства о персональных данных.

7.2. Персональная ответственность работников ГАУ ДПО ПК ИРО.

Должностные лица Учреждения, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, несут дисциплинарную административную, гражданско-правовую или уголовную ответственность, предусмотренную федеральным законодательством.

Руководитель подразделения, разрешивший доступ сотруднику к персональным данным, несет персональную ответственность за данное решение.

Работники Учреждения, получающие доступ к персональным данным, несут персональную ответственность за обеспечение конфиденциальности предоставленной им информации. Кроме того, работники Учреждения, получающие для работы документы, содержащие персональные данные, несут персональную ответственность за их сохранность.

В случае, когда нарушение конфиденциальности, целостности или доступности персональных данных повлекло за собой какие-либо финансовые потери для Учреждения, виновные работники обязаны возместить причиненный ущерб.