государственное бюджетное образовательное учреждение дополнительного профессионального образования (повышения квалификации) специалистов – центр повышения квалификации **«Кинельский Ресурсный центр»** Самарской области

ПРИКАЗ

№ 181 – ОД от 25 декабря 2015 г.

Об утверждении Положения
об организации работ по защите персональных данных

В целях обеспечения защиты прав и свобод человека и в соответствии с требованиями Федерального закона от 27. 07. 2006 № 152-ФЗ «О персональных данных», ПРИКАЗЫВАЮ:

1. Считать Положение «Об обработке и защите персональных данных» в ГБОУ ДПО ЦПК «Кинельский РЦ» (утвержденное приказом ГБОУ ДПО ЦПК «Кинельский РЦ» № 32/1-ОД от 07. 02 2014 г.) утратившим силу с момента издания настоящего приказа;
2. Утвердить в новой редакции Положение об организации работ по защите персональных данных;
3. Положение об организации работ по защите персональных данных ввести в действие с момента издания настоящего приказа;
4. Ответственным за защиту персональных данных в организации, ознакомить всех сотрудников с утвержденным Положением под роспись;
5. Контроль за исполнением данного приказа оставляю за собой.

Директор А. В. Гулина

С приказом ознакомлен(а): _____ «25» декабря 2015 г.

_____ «25» декабря 2015 г.

_____ «25» декабря 2015 г.

УТВЕРЖДЕНО
Приказом
директора ГБОУ ДПО ЦПК
«Кинельский РЦ»
А.В. Гулиной

«25» декабря № 181-ОД
2015 г.

Положение об организации работы по защите персональных данных в государственном бюджетном образовательном учреждении дополнительного профессионального образования (повышения квалификации) специалистов - центра повышения квалификации «Кинельский Ресурсный центр» Самарской области

принято
на Общем собрании трудового коллектива
протокол № 8 **от** 21 декабря 2015 г.

Раздел 1 Общие положения

1.1 Положение о защите персональных данных (далее - Положение) определяет порядок сбора, хранения, комбинирования, передачи и любого другого использования персональных данных в государственном образовательном учреждении дополнительного профессионального образования (повышения квалификации) специалистов - центра повышения квалификации «Кинельский Ресурсный центр» Самарской области (далее-учреждении) в соответствии с законодательством Российской Федерации.

1.2 Положение разработано в соответствии с Конституцией Российской Федерации, Гражданским кодексом Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным законом от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации", Федеральным законом от 27.07.2006 N 152-ФЗ "О персональных данных", иными нормативными актами, действующими на территории Российской Федерации.

1.3 Настоящее Положение принято на Общем собрании трудового коллектива.

1.4 Персональные данные - информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника, а также любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

1.5 К персональным данным относятся:

- сведения, содержащиеся в документах, удостоверяющих личность;
- информация, содержащаяся в трудовой книжке;
- информация, содержащаяся в страховом свидетельстве государственного пенсионного страхования;
- сведения об образовании, квалификации или наличии специальных знаний или подготовки;
- информация о состоянии здоровья в случаях, предусмотренных законодательством;
- сведения, содержащиеся в свидетельстве о постановке на учет физического лица в налоговом органе на территории Российской Федерации;
- сведения о семейном положении;
- информация о заработной плате;
- другая персональная информация.

1.6 К документам, содержащим информацию персонального характера, относятся:

- документы, удостоверяющие личность или содержащие информацию персонального характера;
- учетные документы по личному составу, а также вспомогательные регистрационно-учетные формы, содержащие сведения персонального характера;
- трудовые договоры с работниками, изменения к трудовым договорам, договоры о материальной ответственности с работниками;

- распорядительные документы по личному составу (подлинники и копии);
- документы по оценке деловых и профессиональных качеств работников при приеме на работу;
- документы, отражающие деятельность конкурсных и аттестационных комиссий;
- документы о результатах служебных расследований;
- подлинники и копии отчетных, аналитических и справочных материалов, передаваемых руководству предприятия, руководителям структурных подразделений и служб;
- копии отчетов, направляемых в государственные органы статистики, налоговые инспекции, вышестоящие органы управления и другие учреждения;
- документы бухгалтерского учета, содержащие информацию о расчетах с персоналом;
- медицинские документы, справки;
- др. документы, содержащие сведения персонального характера.

Раздел 2 Частная модель угроз

2.1 Под актуальными угрозами безопасности персональных данных понимается 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.

2.2 Угрозы 1-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе.

2.3 Угрозы 2-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе.

2.4 Угрозы 3-го типа актуальны для информационной системы, если для нее актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

2.5 Определение типа угроз безопасности персональных данных, актуальных для информационной системы, производится комиссией с учетом оценки возможного вреда, проведенной во исполнение пункта 5 части 1 статьи 18 Федерального закона "О персональных данных", и в соответствии с нормативными правовыми актами, принятыми во исполнение части 5 статьи 19 Федерального закона "О персональных данных".

Раздел 3 Категорирование информационной системы обработки персональных данных

3.1 При обработке персональных данных в информационных системах устанавливаются 4 уровня защищенности персональных данных.

3.1.1 Необходимость обеспечения 1-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

- для информационной системы актуальны угрозы 1-го типа и информационная система обрабатывает либо специальные категории персональных данных, либо биометрические персональные данные, либо иные категории персональных данных;
- для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает специальные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

3.1.1.1 Для обеспечения 1-го уровня защищенности персональных данных при их обработке в информационных системах помимо требований, необходимо выполнение следующих требований:

- автоматическая регистрация в электронном журнале безопасности изменения полномочий сотрудника оператора по доступу к персональным данным, содержащимся в информационной системе;
- создание структурного подразделения, ответственного за обеспечение безопасности персональных данных в информационной системе, либо возложение на одно из структурных подразделений функций по обеспечению такой безопасности.

3.1.1.2 Указанный контроль проводится не реже 1 раза в 3 года в сроки, определяемые оператором (уполномоченным лицом).

3.1.2 Необходимость обеспечения 2-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

- для информационной системы актуальны угрозы 1-го типа и информационная система обрабатывает общедоступные персональные данные;
- для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает специальные категории персональных данных сотрудников оператора или специальные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;
- для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает биометрические персональные данные;
- для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные персональные данные более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;
- для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;
- для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории персональных данных более чем

100000 субъектов персональных данных, не являющихся сотрудниками оператора.

3.1.2.1 Для обеспечения 2-го уровня защищенности персональных данных при их обработке в информационных системах помимо выполнения требований, необходимо, чтобы доступ к содержанию электронного журнала сообщений был возможен исключительно для должностных лиц (работников) оператора или уполномоченного лица, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей.

3.1.3 Необходимость обеспечения 3-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

- для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные персональные данные сотрудников оператора или общедоступные персональные данные менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;
- для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории персональных данных сотрудников оператора или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;
- для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории персональных данных сотрудников оператора или специальные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;
- для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает биометрические персональные данные;
- для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

3.1.3.1 Для обеспечения 3-го уровня защищенности персональных данных при их обработке в информационных системах помимо выполнения требований, необходимо, чтобы было назначено должностное лицо (работник), ответственный за обеспечение безопасности персональных данных в информационной системе.

3.1.4. Необходимость обеспечения 4-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

- для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает общедоступные персональные данные;
- для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории персональных данных сотрудников оператора или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

3.1.4.1 Для обеспечения 4-го уровня защищенности персональных данных при их обработке в информационных системах необходимо выполнение следующих требований:

- организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности

неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;
- обеспечение сохранности носителей персональных данных;
- утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;
- использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.

Раздел 4 Администратор информационной безопасности

4.1 Администратор информационной безопасности несет ответственность за организацию работ по обеспечению безопасности информации, обрабатываемой, передаваемой и хранимой при помощи средств вычислительной техники (СВТ) на объектах вычислительной техники (ОВТ), а также правильность использования и нормального функционирования средств защиты информации (СЗИ);

4.2 Администратор информационной безопасности обязан осуществлять настройку и сопровождение системы защиты от НСД на ОВТ, при этом:

– реализует полномочия доступа для каждого пользователя к элементам защищаемых информационных систем на основе утвержденного руководством списка сотрудников, допущенных к работе на ОВТ;

– вводит описание пользователей ОВТ в информационную базу системы защиты от НСД;

– назначает пароли к информационным ресурсам и вводит в базу данных системы защиты описание полномочий доступа пользователей к защищаемым ресурсам;

– своевременно удаляет описание пользователя из базы данных при увольнении или перемещении сотрудника;

– периодически производит смену паролей пользователями для доступа в систему обработки информации ОВТ;

– настройку и сопровождение подсистемы регистрации и учета:

– проводит регулярный анализ системного журнала для выявления попыток несанкционированного доступа к защищаемым ресурсам;

– своевременно информирует руководство о несанкционированных действиях персонала и организует расследование попыток НСД.

– сопровождает подсистемы обеспечения целостности рабочего программного обеспечения (ПО):

– проводит периодическое тестирование функций системы защиты от НСД при изменении программной среды и полномочий исполнителей ОВТ;

– осуществляет восстановление системы защиты от НСД при сбоях;

– проводит контроль соответствия общесистемной программной среды эталону;

– обеспечивает поддержание установленного порядка и соблюдение требований инструкции по антивирусной защите;

– участвует в анализе ситуаций, касающихся функционирования средств защиты информации и расследования фактов несанкционированного доступа;

– производит выдачу исполнителям паролей для средств защиты информации (СЗИ) от несанкционированного доступа (НСД) фиксируя в журнале учета системы защиты объекта вычислительной техники - автоматизированное рабочее место (Приложение №1), а также осуществляет оперативный контроль за действиями пользователей ОВТ;

– составляет технический паспорт информационных систем персональных данных (Приложение №2)

4.3. Администратор информационной безопасности имеет право:

– Контролировать работу пользователей на автоматизированных рабочих местах (АРМ).

– Требовать прекращения обработки информации как в целом, так и отдельных пользователей, в случае выявления нарушений установленного порядка работ или нарушения функционирования АРМ.

Раздел 5 Парольная защита персональных компьютеров

5.1 Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ЛС возлагается на администратора информационной безопасности.

Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями автоматизированной системы самостоятельно с учетом следующих требований:

- длина пароля должна быть не менее 8 символов;
- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 позициях;
- личный пароль пользователь не имеет права сообщать никому.

5.2 При наличии в случае возникновения нештатных ситуаций, форс-мажорных обстоятельств и т.п. технологической необходимости использования имен и паролей некоторых сотрудников (исполнителей) в их отсутствие, такие сотрудники обязаны сразу же после смены своих паролей их новые значения (вместе с именами соответствующих учетных записей) в запечатанном конверте или опечатанном пенале передавать на хранение ответственному за информационную безопасность подразделения (руководителю своего подразделения). Опечатанные конверты (пеналы) с паролями исполнителей должны храниться в сейфе. Для опечатывания конвертов (пеналов) должны применяться личные печати владельцев паролей (при их наличии у исполнителей).

5.3 Полная плановая смена паролей пользователей должна проводиться не реже одного раза в год.

5.4 Внеплановая смена личного пароля или удаление учетной записи пользователя автоматизированной системы в случае прекращения его полномочий (увольнение, переход на другую работу и т.п.) должна производиться администратором информационной безопасности.

5.5 Хранение сотрудником (исполнителем) значений своих паролей на бумажном носителе допускается только в личном столе.

Раздел 6 Антивирусная защита

6.1 В целях обеспечения антивирусной защиты на объектах вычислительной техники (далее – ОВТ) производится антивирусный контроль.

Ответственность за поддержание установленного в настоящей Инструкции порядка проведения антивирусного контроля возлагается на Администратора информационной безопасности.

6.2 К применению на ОВТ допускаются только лицензионные антивирусные средства.

6.3 На ОВТ запрещается установка программного обеспечения, не связанного с выполнением функций, предусмотренных технологическим процессом обработки информации на АРМ.

6.4 Пользователи ОВТ при работе с носителями информации обязаны перед началом работы осуществить проверку их на предмет отсутствия компьютерных вирусов.

6.5 Ярлык для запуска антивирусной программы должен быть вынесен на "Рабочий стол" операционной системы.

6.6 Обновление вирусных баз осуществляется еженедельно путем настройки в антивирусном средстве доступа к серверам обновлений разработчика антивирусного средства. В случае невозможности настроить доступ к серверам обновлений разработчика антивирусного средства, Администратор информационной безопасности один раз в неделю осуществляет установку пакетов обновлений вирусных баз, осуществляет контроль их подключения к антивирусному пакету и проверку жесткого диска и съемных носителей на наличие вирусов.

6.7 При обнаружении компьютерного вируса пользователи обязаны немедленно поставить в известность Администратора информационной безопасности и прекратить какие-либо действия на ОВТ.

6.8 Администратор информационной безопасности проводит расследование факта заражения ОВТ компьютерным вирусом. «Лечение» зараженных файлов осуществляется путем выбора соответствующего пункта меню антивирусной программы и после этого вновь проводится антивирусный контроль.

6.9 В случае обнаружения не поддающегося лечению вируса, Администратор информационной безопасности обязан удалить инфицированный файл в соответствующую папку антивирусного пакета, и проверить работоспособность ОВТ. В случае отказа ОВТ – произвести восстановление соответствующего программного обеспечения.

Раздел 7 Инструкции пользователям

7.1 Обработка персональных данных работника осуществляется исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

7.2 Требования к передаче персональных данных:

- не сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в других случаях, предусмотренных законодательством РФ;
- не сообщать персональные данные работника в коммерческих целях без его письменного согласия;
- предупредить лиц, получающих персональные данные работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено;
- осуществлять передачу персональных данных работника в пределах одной организации, у одного индивидуального предпринимателя в соответствии с локальным нормативным актом, с которым работник должен быть ознакомлен под роспись;
- разрешать доступ к персональным данным работников 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 информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции;
- передавать персональные данные работника представителям работников в порядке, установленном законодательством РФ, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.

7.3 Отделы, а также сотрудники учреждения, в ведение которых входит работа с персональными данными, обеспечивают защиту персональных данных от несанкционированного доступа и копирования.

7.4 Персональные данные работника предоставляются самим работником. Если персональные данные работника, возможно, получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Работодатель должен сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение.

7.5 Работник обязан предоставлять работодателю достоверную персональную информацию. При изменении персональных данных работник должен письменно уведомить об этом работодателя в срок, установленный законодательством.

7.6 Работодатель не имеет права получать и обрабатывать персональные данные работника о его политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со ст. 24 Конституции Российской Федерации работодатель вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия (Приложение №3).

7.7 Ответственные должностные лица организуют хранение и использование персональных данных работников в соответствии с законодательством РФ.

7.8 Хранение персональных данных работников осуществляется на электронных носителях, а также в бумажном варианте.

7.9 Доступ к программному обеспечению, а также к персональной информации, хранящейся на электронных носителях осуществляется при введении личного идентификатора и пароля пользователя.

7.10 Документы персонального характера хранятся в сейфах отделов, ответственных за ведение и хранение таких документов.

7.11 Документы, содержащие персональные данные, подлежат хранению и уничтожению в порядке, предусмотренном архивным законодательством Российской Федерации.

7.12 Права работника по обеспечению защиты своих персональных данных

7.13 Работники имеют право на:

- полную информацию о своих персональных данных и обработке этих данных;
- свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные работника, за исключением случаев, предусмотренных федеральным законом;
- определение своих представителей для защиты своих персональных данных;
- доступ к своим медицинским данным с помощью медицинского специалиста по своему выбору;
- требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением законодательства РФ;
- требование об извещении работодателем всех лиц, которым ранее были сообщены неверные или неполные персональные данные работника, обо всех произведенных в них исключениях, исправлениях или дополнениях;
- обжалование в суд любых неправомерных действий или бездействия работодателя при обработке и защите его персональных данных.

7.14 Нарушение требований законодательства о персональных данных влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

Срок действия Положения бессрочное.

Приложение № 1

ЖУРНАЛ

учета системы защиты объекта вычислительной техники - автоматизированное рабочее место

Ф.И.О.	Уровень полномочий	Содержание пароля	Дата выдачи	Подпись

Приложение №2

ТЕХНИЧЕСКИЙ ПАСПОРТ
Информационной системы персональных данных
«_____»

Составил_____
(Подпись администратора безопасности)

_____

(Год)

1. Общие сведения об ИСПДн.

1.1. Наименование ИСПДн: «_____»

1.2. Физическое расположение ИСПДн:

1.3. Частная модель угроз безопасности ПДн в ИСПДн:_____

1.4. Класс ИСПДн: _____

1.5. Уровень защищенности персональных денных:_____

1.6. Перечень ПДн, обрабатываемых в ИСПДн:_____

Таблица 1

П Е Р Е Ч Е Н Ь
персональных данных, обрабатываемых в ИСПДн

№ п/п	Наименование персональных данных	Категория ПДн	Цель обработки ПДн в рамках ИСПДн
1.	Персональные данные работников		
1.1	Первичные учетные данные работников		Учет работников, осуществление процессов согласно трудовому законодательству РФ
1.2	Сведения о занимаемой должности		Поддержание иерархичности отношений между работниками, осуществление процессов согласно трудовому законодательству РФ
1.3	Финансовое состояние работника		Осуществление налоговых отчислений, осуществление процессов согласно трудовому законодательству РФ
1.4	Сведения о реквизитах работника		Осуществление процессов согласно трудовому законодательству РФ
1.5	Дополнительные сведения о работнике		Выплата льгот, осуществление процессов согласно трудовому законодательству РФ

2.Технологические процессы обработки ПДн, используемые в ИСПДн.

Таблица 2

П Е Р Е Ч Е Н Ь
технологических процессов обработки ПДн, используемых в ИСПДн

№ п/п	Наименование технологических процессов обработки ПДн
1.	
2.	
3.	

3. Состав оборудования информационной системы.

3.1 Состав основных технический средств и систем (ОТСС):

Таблица 3

П Е Р Е Ч Е Н Ь
основных технических средств и систем, входящих в состав ИСПДн

№ п/п	**Тип ОТСС**	**Программные и технические характеристики**	**Место установки**	**Кол-во, шт.**
1				
2				

3.2 Состав вспомогательных технических средств и систем (ВТСС) установленных в помещениях, где расположены ОТСС:

Таблица 4

П Е Р Е Ч Е Н Ь
вспомогательных технических средств, не участвующих в обработке персональных данных

№ п/п	**Наименование и тип ВТСС**	**Место установки**	**Кол-во, шт.**	**Примечание**

3.3 Состав средств защиты информации:

П Е Р Е Ч Е Н Ь
средств защиты информации, установленных
в ИСПДн « »

Таблица 5

№ п/п	Наименование и тип технического средства	Сведения о сертификате	Место установки

Приложение №3

СОГЛАСИЕ
на обработку персональных данных

г.Кинель
«___»_____20__г.

Я,_____
___,
(Ф.И.О.)
_____ серия_____№_____
выдан:
(вид документа, удостоверяющего личность)
_____
_____
_____
(когда и кем)
проживающий (ая) по
адресу:_____
_____
___
настоящим даю свое согласие на обработку
Государственное бюджетное образовательное учреждение дополнительного профессионального образования (повышения квалификации) специалистов – центр повышения квалификации «Кинельский Ресурсный центр» Самарской области (ГБОУ ДПО ЦПК «Кинельский РЦ»)
(наименование и адрес оператора (органа исполнительной власти Самарской области, областного государственного учреждения)
моих персональных данных и подтверждаю, что, давая такое согласие, я действую своей волей и в своих интересах.

Согласие дается мною для целей:
оформление трудовых и договорных отношений, представление персональных данных для награждения и профессиональной аттестации в вышестоящие структуры и органы
(цель обработки персональных данных)
и распространяется на следующую информацию: *фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы и другая информация, связанная с трудовой деятельностью.*
(перечень персональных данных)
Настоящее согласие предоставляется на осуществление любых действий в отношении моих персональных данных, которые необходимы или желаемы для достижения указанных выше целей, включая (без ограничения) сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передача), обезличивание, блокирование, уничтожение, трансграничную передачу персональных данных, а также осуществление любых иных действий с моими персональными данными с учетом федерального законодательства.

В случае неправомерного использования предоставленных мною персональных данных согласие отзывается моим письменным заявлением.

Данное согласие действует с «____»_____20___г.
до окончания трудовой деятельности в данном учреждении.

_____
(Ф.И.О., подпись лица, давшего согласие)