Рождества Пресвятой Богородицы Свято-Пафнутьев Боровский монастырь
Автономная некоммерческая организация профессионального образования
«Технический колледж»

РАССМОТРЕНО

На педагогическом Совете

Протокол № 1 от « 1» апреля 2025 г.

УТВЕРЖДАЮ

Директор АНО ПО «ТК»

А. М. Габидулин

Пр19 « 1 » апреля 2025 г.

Положение
о защите персональных данных

2025 г.

1. Общие положения

1.1. Положение о защите персональных данных (далее – Положение) определяет понятие и состав персональных данных, требования к обработке, хранению и защите персональных данных работника, необходимых в связи с трудовыми отношениями.

1.2. Положение основано на следующих нормативных документах:

– Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – ФЗ «О персональных данных»);

– Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ;

– Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– Устав АНО ПО «ТК» и иные локальные нормативные акты.

1.3. Положение вступает в силу с момента его утверждения руководителем АНО ПО «ТК» (далее – Организации) и действует до замены его новым Положением.

1.4. В Положении используются следующие основные понятия:

– персональные данные работника – любая информация, относящаяся к определенному или определяемому на основании такой информации работнику, в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация, необходимая работодателю в связи с трудовыми отношениями;

– персональные данные, разрешенные субъектом персональных данных для распространения, – персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном настоящим Федеральным законом;

– обработка персональных данных – сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передача), обезличивание, блокирование, уничтожение персональных данных работников Организации;

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

2. Состав и обработка персональных данных работников

2.1. В состав персональных данных работников Организации входят документы, содержащие информацию о паспортных данных, образовании, отношении к воинской обязанности, семейном положении, месте жительства, состоянии здоровья, а также о предыдущих местах их работы.

2.2. Комплекс документов, сопровождающий процесс оформления трудовых отношений работника в Организации при его приеме, переводе и увольнении:

2.2.1. Информация, представляемая работником при поступлении на работу в Организацию, должна иметь документальную форму. При заключении трудового договора в соответствии со ст. 65 Трудового кодекса Российской Федерации лицо, поступающее на работу, предъявляет работодателю:

– паспорт или иной документ, удостоверяющий личность;

– трудовую книжку, за исключением случаев, когда трудовой договор заключается впервые или работник поступает на работу на условиях совместительства, либо трудовая книжка у работника отсутствует в связи с ее утратой или по другим причинам;

– страховое свидетельство государственного пенсионного страхования;

– документы воинского учета – для военнообязанных и лиц, подлежащих воинскому учету;

– документ об образовании, о квалификации или наличии специальных знаний – при поступлении на работу, требующую специальных знаний или специальной подготовки;

– свидетельство о присвоении ИНН (при его наличии у работника).

2.2.2. При оформлении работника в Организацию работником отдела кадров заполняется унифицированная форма Т-2 «Личная карточка работника», в которой отражаются следующие анкетные и биографические данные работника:

– общие сведения (Ф.И.О. работника, дата рождения, место рождения, гражданство, образование, профессия, стаж работы, состояние в браке, паспортные данные);

– сведения о воинском учете;

– данные о приеме на работу;

В дальнейшем в личную карточку вносятся:

– сведения о переводах на другую работу;

– сведения об аттестации;

– сведения о повышении квалификации;

– сведения о профессиональной переподготовке;

– сведения о наградах (поощрениях), почетных званиях;

– сведения об отпусках;

– сведения о социальных гарантиях;

– сведения о месте жительства и контактных телефонах.

2.2.3. В отделе кадров Организации создаются и хранятся следующие группы документов, содержащие данные о работниках в единичном или сводном виде:

– документы, содержащие персональные данные работников (комплексы документов, сопровождающие процесс оформления трудовых отношений при приеме на работу, переводе, увольнении; комплекс материалов по анкетированию, тестированию; проведению собеседований с кандидатом на должность; подлинники и копии приказов по личному составу; личные дела и трудовые книжки работников; дела, содержащие основания к приказу по личному составу; дела, содержащие материалы аттестации работников; служебных расследований; справочно-информационный банк данных по персоналу (картотеки, журналы); подлинники и копии отчетных, аналитических и справочных материалов, передаваемых руководству Организации, руководителям структурных подразделений; копии отчетов, направляемых в государственные органы статистики, налоговые инспекции, вышестоящие органы управления и другие учреждения);

– документация по организации работы структурных подразделений (положения о структурных подразделениях, должностные инструкции работников, приказы, распоряжения, указания руководства Организации); документы по планированию, учету, анализу и отчетности в части работы с персоналом Организации.

2.3. Работодатель не имеет права получать и обрабатывать персональные данные работника о его расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, интимной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со ст. 24 Конституции РФ работодатель вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия.

Обработка указанных персональных данных работников работодателем возможна только с их согласия либо без их согласия в следующих случаях:

– персональные данные являются общедоступными;

– персональные данные относятся к состоянию здоровья работника и их обработка необходима для защиты его жизни, здоровья или иных жизненно важных интересов либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия работника невозможно;

– по требованию полномочных государственных органов в случаях, предусмотренных федеральным законом.

2.4. Чтобы обрабатывать персональные данные сотрудников, работодатель получает от каждого сотрудника согласие на обработку его персональных данных. Такое согласие работодатель получает, если закон не предоставляет работодателю права обрабатывать персональные данные без согласия сотрудников.

2.5. Согласие работника не требуется в следующих случаях:

– обработка персональных данных осуществляется на основании Трудового кодекса РФ или иного федерального закона, устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия работодателя;

– обработка персональных данных осуществляется в целях исполнения трудового договора;

– обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;

– обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов работника, если получение его согласия невозможно.

3. Доступ к персональным данным работников

3.1. Допуск к персональным данным работника разрешен только специально уполномоченным лицам согласно перечню должностей.

3.2. Перечень лиц, имеющих доступ к персональным данным работников Организации с указанием целей обработки персональных данных, устанавливается приказом руководителя Организации, при этом указанные лица имеют право получать только те персональные данные, которые необходимы для выполнения конкретной функции.

3.3. От лиц, ответственных за хранение персональных данных, а также лиц, владеющих персональными данными в силу своих должностных обязанностей, берутся обязательства о неразглашении персональных данных работников.

3.4. Лицам, допущенным к обработке персональных данных, запрещается:

– передавать третьим лицам и работникам, не допущенным к обработке персональных данных, сведения, ставшие им известными при исполнении должностных обязанностей без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом;

– оставлять документы, содержащие персональные данные, в открытом доступе;

– оставлять кабинеты без присмотра и не запертыми при отсутствии в нем других работников;

– оставлять посторонних лиц в кабинете без присмотра и в отсутствии других работников.

3.5. Передача информации, содержащей сведения о персональных данных работников, по телефону в связи с невозможностью идентификации лица, запрашивающего информацию, запрещается.

4. Хранение и защита персональных данных работников

4.1. Документы, содержащие персональные данные работников Организации, хранятся на бумажных носителях в специально предназначенных для этого помещениях/в специально отведенном шкафу, обеспечивающем защиту от несанкционированного доступа. Срок хранения документов определяется утвержденной номенклатурой дел.

По истечении сроков хранения документы по решению Экспертной комиссии (создается в целях организации и проведения методической и практической работы по экспертизе ценности документов, образовавшихся в деятельности Организации) подлежат уничтожению в установленном порядке.

4.2. Персональные данные работников могут также храниться в электронном виде в локальной компьютерной сети.

4.3. Обеспечение безопасности персональных данных достигается, в частности:

2.4. Чтобы обрабатывать персональные данные сотрудников, работодатель получает от каждого сотрудника согласие на обработку его персональных данных. Такое согласие работодатель получает, если закон не предоставляет работодателю права обрабатывать персональные данные без согласия сотрудников.

2.5. Согласие работника не требуется в следующих случаях:

– обработка персональных данных осуществляется на основании Трудового кодекса РФ или иного федерального закона, устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия работодателя;

– обработка персональных данных осуществляется в целях исполнения трудового договора;

– обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;

– обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов работника, если получение его согласия невозможно.

3. Доступ к персональным данным работников

3.1. Допуск к персональным данным работника разрешен только специально уполномоченным лицам согласно перечню должностей.

3.2. Перечень лиц, имеющих доступ к персональным данным работников Организации с указанием целей обработки персональных данных, устанавливается приказом руководителя Организации, при этом указанные лица имеют право получать только те персональные данные, которые необходимы для выполнения конкретной функции.

3.3. От лиц, ответственных за хранение персональных данных, а также лиц, владеющих персональными данными в силу своих должностных обязанностей, берутся обязательства о неразглашении персональных данных работников.

3.4. Лицам, допущенным к обработке персональных данных, запрещается:

– передавать третьим лицам и работникам, не допущенным к обработке персональных данных, сведения, ставшие им известными при исполнении должностных обязанностей без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом;

– оставлять документы, содержащие персональные данные, в открытом доступе;

– оставлять кабинеты без присмотра и не запертыми при отсутствии в нем других работников;

– оставлять посторонних лиц в кабинете без присмотра и в отсутствии других работников.

3.5. Передача информации, содержащей сведения о персональных данных работников, по телефону в связи с невозможностью идентификации лица, запрашивающего информацию, запрещается.

4. Хранение и защита персональных данных работников

4.1. Документы, содержащие персональные данные работников Организации, хранятся на бумажных носителях в специально предназначенных для этого помещениях/в специально отведенном шкафу, обеспечивающем защиту от несанкционированного доступа. Срок хранения документов определяется утвержденной номенклатурой дел.

По истечении сроков хранения документы по решению Экспертной комиссии (создается в целях организации и проведения методической и практической работы по экспертизе ценности документов, образовавшихся в деятельности Организации) подлежат уничтожению в установленном порядке.

4.2. Персональные данные работников могут также храниться в электронном виде в локальной компьютерной сети.

4.3. Обеспечение безопасности персональных данных достигается, в частности:

– определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных (п. 4.4 настоящего Положения);

– применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных (п. 4.6 настоящего Положения);

– применением прошедших в установленном порядке процедур оценки соответствия средств защиты информации;

– оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

– учетом машинных носителей персональных данных;

– обнаружением фактов несанкционированного доступа к персональным данным и принятием мер, в том числе мер по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные системы персональных данных и по реагированию на компьютерные инциденты в них;

– восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

– установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

– контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

4.4. 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.

4.4.1. 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.

4.4.2. 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.

4.4.3. 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.

4.5. С целью защиты персональных данных в Организации принимаются следующие меры:

– назначение лица, ответственного за обработку персональных данных, которое осуществляет организацию обработки персональных данных, обучение и инструктаж, внутренний контроль за соблюдением работниками требований к защите персональных данных;

– разработка политики в отношении обработки персональных данных;

– установление правил доступа к персональным данным, обеспечение регистрации и учета всех действий, совершаемых с персональными данными;

– установление индивидуальных паролей доступа сотрудников в информационную систему в соответствии с их производственными обязанностями;

– применение прошедших в установленном порядке процедур оценки соответствия средств защиты информации;

– сертифицированное антивирусное программное обеспечение с регулярно обновляемыми базами;

– соблюдение условий, обеспечивающих сохранность персональных данных и исключающих несанкционированный к ним доступ;

– обнаружение фактов несанкционированного доступа к персональным данным;

– восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

– обучение работников, непосредственно осуществляющих обработку персональных данных, положениям законодательства Российской Федерации о персональных данных, в том числе требованиям к защите персональных данных, документам, определяющим политику Организации в отношении обработки персональных данных, локальным актам по вопросам обработки персональных данных;

– осуществление внутреннего контроля и аудита;

– определение типа угроз безопасности и уровней защищенности персональных данных, которые хранятся в информационных системах.

4.6. Уровни защищенности персональных данных.

4.6.1. Первый уровень защищенности:

– 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 100 тысяч субъектов персональных данных, не являющихся сотрудниками Организации.

4.6.2. Второй уровень защищенности.

– 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 Организации или специальные категории персональных данных менее чем 100 тысяч субъектов персональных данных, не являющихся сотрудниками Организации;

– 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 100 тысяч субъектов персональных данных, не являющихся сотрудниками Организации;

– для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории персональных данных более чем 100 тысяч субъектов персональных данных, не являющихся сотрудниками Организации;

– для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории персональных данных более чем 100 тысяч субъектов персональных данных, не являющихся сотрудниками Организации.

4.6.3. Третий уровень защищенности.

– для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные персональные данные сотрудников Организации или общедоступные персональные данные менее чем 100 тысяч субъектов персональных данных, не являющихся сотрудниками Организации;

– для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории персональных данных сотрудников Организации или

иные категории персональных данных менее чем 100 тысяч субъектов персональных данных, не являющихся сотрудниками Организации;

– для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории персональных данных сотрудников Организации или специальные категории персональных данных менее чем 100 тысяч субъектов персональных данных, не являющихся сотрудниками Организации;

– 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 100 тысяч субъектов персональных данных, не являющихся сотрудниками Организации.

4.6.4. Четвертый уровень защищенности.

– 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 Организации или иные категории персональных данных менее чем 100 тысяч субъектов персональных данных, не являющихся сотрудниками Организации.

4.7. При четвертом уровне защищенности персональных данных работодатель:

– обеспечивает режим безопасности помещений, в которых размещаете информационную систему;

– обеспечивает сохранность носителей информации;

– утверждает распорядительным актом перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

– использует средства защиты информации, которые прошли процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.

4.8. При третьем уровне защищенности персональных данных дополнительно к мерам, перечисленным в пункте 4.6.3 настоящего Положения, работодатель назначает ответственного за обеспечение безопасности персональных данных в информационной системе.

4.9. При втором уровне защищенности персональных данных дополнительно к мерам, перечисленным в пункте 4.6.2 настоящего Положения, работодатель ограничивает доступ к электронному журналу сообщений, за исключением работников, которым такие сведения необходимы для работы.

4.10. При первом уровне защищенности персональных данных дополнительно к мерам, перечисленным в пункте 4.6.1 настоящего Положения, работодатель:

– обеспечивает автоматическую регистрацию в электронном журнале безопасности изменения полномочий работников по допуску к персональным данным в системе;

– создает отдел, ответственный за безопасность персональных данных в системе, либо возлагает такую обязанность на один из существующих отделов работодателя.

4.11. В целях защиты персональных данных на бумажных носителях работодатель:

приказом назначает ответственного за обработку персональных данных;

– ограничивает допуск в помещения, где хранятся документы, которые содержат персональные данные работников;

– хранит документы, содержащие персональные данные работников в шкафах, запирающихся на ключ;

– хранит трудовые книжки работников в сейфе в отделе кадров.

5. Гарантии конфиденциальности персональных данных

5.1. Все работники организации, осуществляющие обработку персональных данных, обязаны хранить тайну о сведениях, содержащих персональные данные, в соответствии с настоящим Положением, требованиями законодательства Российской Федерации.

5.2. Работник вправе требовать полную информацию о своих персональных данных, об их обработке, использовании и хранении.

5.3. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работников, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством.