



**ПЕРМСКИЙ
СТРОИТЕЛЬНЫЙ
КОЛЛЕДЖ**

УТВЕРЖДАЮ

Директор
КГАПОУ ПСК

 И.А. Коновалов

«20» февраля 2016 г.



ЛОКАЛЬНЫЙ НОРМАТИВНЫЙ АКТ №37
Положение о порядке обработки и обеспечения
безопасности персональных данных сотрудников
в краевом государственном автономном
профессиональном образовательном учреждении
«Пермский строительный колледж»
(КГАПОУ ПСК)

Пермь, 2016

1. Общие положения

1.1. Настоящее Положение о порядке обработки и обеспечении безопасности персональных данных сотрудников в красном государственном автономном профессиональном образовательном учреждении «Пермский строительный колледж» (далее – Положение) разработано в соответствии с: Федеральным законом от 27 июля 2006 г. №152-ФЗ «О персональных данных» (далее - Федеральным законом); 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 17 ноября 2007 г. №781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»; Приказ ФС по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) от 05.09.2013г. № 996 «Об утверждении требований и методов по обеспечению персональных данных», Постановления Правительства РФ от 01.11.2012г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13 февраля 2008 г. №55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных»; Конституции Российской Федерации; Трудового кодекса Российской Федерации и устанавливает единый порядок обработки персональных данных сотрудников в государственном бюджетном образовательном учреждении среднего профессионального образования «Пермский строительный колледж» (далее – Учреждение).

1.2. В настоящем Положении используются следующие термины и определения:

- персональные данные (далее ПДн) – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);
- предоставление ПДн – действия, направленные на раскрытие ПДн определенному лицу или определенному кругу лиц;
- использование персональных данных – действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц;
- 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;
- 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;
- автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники;
- информационная система персональных данных (далее ИСПДн) - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

- несанкционированный доступ – доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своим функциональному назначению и техническим характеристикам.

- обработка персональных данных без использования средств автоматизации (неавтоматизированная) – обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека;

- технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах;

- сотрудник Учреждения – под сотрудниками Учреждения подразумеваются лица, заключившие трудовой договор с Учреждением;

- типовая форма – под типовой формой понимается любая бухгалтерская и кадровая документация, содержащая ПДн сотрудника Учреждения.

1.3. Настоящее Положение устанавливает порядок получения, учета, обработки, накопления и хранения документов (типовых форм), содержащих сведения, отнесенные к ПДн сотрудников Учреждения.

1.4. Настоящее Положение разработано с целью – защиты ПДн сотрудников Учреждения.

1.5. Целью обработки ПДн сотрудников Учреждения является – проведение операций по учету кадров, по начислению и выплате заработной платы и премий, предоставление отчетности по субъектам ПДн в налоговые органы и пенсионный фонд РФ (другие государственные органы по запросу) сотрудников Учреждения.

1.6. Настоящее Положение и изменения к нему утверждаются Директором Учреждения и вводятся приказом по Учреждению. Положение в обязательном порядке доводится до сотрудников Учреждения допущенных к обработке ПДн под роспись.

2. ПДн сотрудников обрабатываемых в Учреждении

2.1. Перечень ПДн:

Таблица 1

№ п/п	Персональные данные сотрудников, обрабатываемые в ИСПДн
1	Фамилия, имя, отчество
2	Место и дата рождения
3	Адрес прописки (регистрации)
4	Паспортные данные
5	Контактная информация
6	Образование, профессия
7	Должность
8	Сведения о воинском учете

№ п/п	Персональные данные сотрудников, обрабатываемые в ИСПДн
9	Сведения об отпусках
10	Сведения о наградах (поощрениях), почетных званиях
11	Сведения о местах работы
12	Сведения о семейном положении, детях (фамилия, имя, отчество, дата рождения)
13	Сведения о постановке на налоговый учет
14	Сведения о регистрации в Пенсионном фонде
15	Сведения о доходах/зарплате
16	Выписки из больничных листов и листов нетрудоспособности
17	Гражданство

3. Основные условия проведения обработки ПДн в Учреждении

3.1. Обработка ПДн осуществляется:

- после получения согласия сотрудника Учреждения;
- после направления уведомления об обработке ПДн в Управление Федеральной службы по надзору в сфере связи и массовых коммуникаций по Пермскому краю;
- после принятия необходимых мер по защите ПДн в Учреждении.

3.2. В Учреждении приказом Директора назначается сотрудник, ответственный за защиту ПДн, и определяется перечень лиц, допущенных к обработке ПДн.

3.3. В Учреждении запрещается:

- обрабатывать ПДн в присутствии лиц, не допущенных к их обработке;
- осуществлять ввод ПДн под диктовку.

4. Порядок определения защищаемой информации в Учреждении

4.1. В Учреждении защищаемая информация, отнесенная к ПДн сотрудников определяется на основании следующих разработанных документов:

- Перечнем персональных данных обрабатываемых в информационной системе персональных данных «1С:Бухгалтерия», «1С: ЗИК», «1С: Колледж» в КГАПОУ ПСК;
- Актом классификации информационной системы персональных данных КГАПОУ ПСК;
- Моделью угроз безопасности персональных данных при их обработке в информационной системе персональных данных КГАПОУ ПСК;
- настоящим Положением.

5. Обязанности Учреждения

5.1. Директор колледжа (далее Работодатель) и его представители при обработке ПДн сотрудника должны соблюдать следующие требования:

5.1.1. Обработка ПДн сотрудника осуществляется с соблюдением законов и иных нормативных правовых актов, содействия сотрудникам в трудоустройстве, обучении и продвижении по службе, обеспечении личной безопасности сотрудников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

5.1.2. При определении объема и содержания, обрабатываемых ПДн сотрудника Работодатель и его представители должны руководствоваться законодательной базой РФ в области защиты информации, отнесенной к ПДн.

5.1.3. Все ПДн сотрудника следует получать у него самого. С оригиналов документов снять копии, которые в последствии хранятся в личном деле сотрудника. Если ПДн сотрудника, возможно, получить только у третьей стороны, то сотрудник должен быть уведомлен об этом заранее и от него должно быть получено согласие. Работодатель должен сообщить работнику о цели, предполагаемых источниках и способах получения ПДн, а также

о характере подлежащих получению ПДн и последствиях отказа сотрудника дать согласие на их получение.

5.1.4. Работодатель не имеет права получать и обрабатывать ПДн сотрудника, включающие в себя – политические взгляды, религиозные и философские убеждения, национальной принадлежности, состояния здоровья (за исключением больничных листов, и листов не трудоспособности), интимной жизни без письменного согласия сотрудника Учреждения.

5.1.5. При принятии решений, затрагивающих интересы сотрудника, Работодатель не имеет права основываться на ПДн сотрудника, полученных исключительно в результате их автоматизированной обработки или электронного получения.

5.1.6. Защита ПДн сотрудника от неправомерного их использования или утраты должна быть обеспечена Работодателем, в соответствии действующим Федеральным законом и другими нормативными руководящими документами уполномоченных органов исполнительной власти в области защиты информации, отнесенной к ПДн.

6. Обязанности сотрудника Учреждения

Сотрудник обязан:

6.1. Передать Работодателю или его представителю комплект достоверных документированных ПДн, перечень которых установлен трудовым кодексом РФ.

6.2. Своевременно в срок, не превышающий 5-ти дней, сообщить Работодателю (или его представителю) об изменении своих ПДн.

7. Права сотрудника Учреждения

Сотрудник имеет право:

7.1. Получать полную информацию, касающуюся обработки его ПДн, содержащую:

- подтверждение факта обработки ПДн оператором;
- цели и применяемые оператором способы обработки ПДн;
- обрабатываемые ПДн, источник их получения;
- сроки обработки ПДн, в том числе сроки их хранения;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению оператора, если обработка поручена или будет поручена такому лицу (относится к государственным и негосударственным структурам, а также к физическим лицам).

7.2. На свободный доступ к своим ПДн, включая право на получение копий любой записи, содержащей ПДн сотрудника, за исключением случаев, предусмотренных законодательством РФ.

7.3. Требовать от оператора (Работодателя) уточнения его ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

Запрашиваемые сведения (ПДн) должны быть представлены сотруднику Учреждения оператором в доступной форме, и в них не должны содержаться ПДн, относящиеся к другим сотрудникам Учреждения.

При отказе Работодателя исключить или исправить его ПДн, сотрудник имеет право заявить в письменной форме Работодателю о своем несогласии с соответствующим обоснованием такого несогласия.

7.4. Требовать об извещение Работодателем всех лиц, которым ранее были сообщены неверные или неполные его ПДн, обо всех произведенных в них изменениях, исправлениях или дополнениях.

7.5. Обжаловать в судебных инстанциях любые неправомерные действия или бездействие Работодателя при обработке и защите его ПДн.

8. Доступ к ПДн сотрудника Учреждения

8.1. Внутренний доступ.

Право доступа к ПДн работника имеют:

- Директор колледжа и его заместители;
- главный бухгалтер Учреждения, сотрудники бухгалтерии;
- сотрудники отдела кадров;
- учебные отделения;
- работник Учреждения, носитель ПДн.

8.2. Внешний доступ.

К числу потребителей ПДн вне Учреждения относятся государственные и негосударственные функциональные структуры, такие как:

- налоговые инспекции;
- правоохранительные органы;
- органы статистики;
- страховые агенты;
- военкоматы;
- органы социального страхования;
- пенсионные фонды;
- банковские структуры (при возникновении договорных отношений);
- подразделения муниципальных органов власти.

8.3. Другие организации.

Сведения о работающем сотруднике или уже уволенном могут быть представлены другой организации только с письменного запроса на бланке организации с приложением письменного разрешения (заявления) сотрудника, чьи ПДн подлежат запросу.

8.4. Родственники и члены семей.

ПДн сотрудника Учреждения могут быть представлены родственникам или членам семьи только с письменного разрешения самого сотрудника.

В случае развода бывшая супруга (супруг) имеют право на основании Трудового кодекса РФ обратиться в Учреждение с письменным запросом о размере заработной платы сотрудника без его согласия.

9. Сбор, обработка и хранение ПДн сотрудников Учреждения

9.1. После предоставления сотрудником достоверных сведений о себе, Работодатель обязан проверить их достоверность, сверяя данные, представленные сотрудником, с имеющимися у сотрудника документами. Представление сотрудником подложных документов или ложных сведений при поступлении на работу является основанием для расторжения трудового договора.

9.2. Все документы, содержащие ПДн сотрудников подшиваются в папки (отдельная папка для каждого сотрудника) с непрозрачной обложкой (личные дела) и хранятся в специально отведенных шкафах (сейфах).

9.3. Обработка ПДн в ИСПДн Учреждения с использованием средств автоматизации.

9.3.1. Не допускается обработка ПДн в ИСПДн с использованием средств автоматизации при отсутствии:

- утвержденных организационно-технических документов о порядке эксплуатации ИСПДн, включающих Акт классификации ИСПДн, инструкции пользователю по антивирусной защите, и других нормативно методических документов;

- настроенных средств защиты от несанкционированного доступа, средств антивирусной защиты, резервного копирования информации и других программных и технических средств в соответствии с требованиями безопасности информации в Учреждении;

9.4. Обработка ПДн без использования средств автоматизации.

9.4.1. Неавтоматизированная обработка ПДн осуществляется в Учреждении в виде документов на бумажных носителях к которым относятся: карточки формы Т2; материалы по учету рабочего времени; листки нетрудоспособности; журнал учета командировок; журнал учета трудовых книжек; трудовые книжки; копии паспортов; копии ИНН; копии пенсионных свидетельств; копии военных билетов; трудовые договора; документы о составе семьи; дополнительные соглашения с сотрудниками Учреждения; копии документов об образовании; документы о повышении квалификации сотрудниками Учреждения, а также документы на съемных носителях, к которым относятся: флешь память; магнитные дискеты и т.п.

9.4.1.1. При неавтоматизированной обработке ПДн в Учреждении на бумажных носителях должны соблюдаться следующие правила:

- не допускается фиксация на одном бумажном носителе ПДн, цели, обработки которых заведомо не совместимы;
- ПДн должны обособляться от иной информации, в частности путем фиксации их на отдельных бумажных носителях, в специальных разделах или на полях форм (бланков);
- документы, содержащие ПДн на бумажных носителях должны храниться в служебных помещениях Учреждения только в надежно запираемых и опечатываемых шкафах (сейфах).

9.4.1.2. При неавтоматизированной обработке ПДн в Учреждении на съемных носителях должны соблюдаться следующие правила:

- съемный носитель, содержащий ПДн должен иметь идентификационный (инвентарный) учетный номер;
- съемные носители учитываются в журнале учета съемных носителей (форма журнала Приложение №2);
- к каждому съемному носителю оформляется опись файлов, содержащихся на нем, с указанием цели обработки и категории ПДн;
- вышедшие из строя съемные носители уничтожаются в присутствии специально созданной комиссии с составлением Акта об уничтожения носителей ПДн (форма Акта уничтожения Приложение №3);
- учтенные съемные носители, содержащие ПДн, должны храниться в служебных помещениях Учреждения отдельно от других носителей только в надежно запираемых и опечатываемых шкафах (сейфах).

10. Передача ПДн сотрудников Учреждения

10.1. При передаче ПДн сотрудника Работодатель должен соблюдать следующие требования:

- не сообщать ПДн сотрудника третьей стороне без письменного согласия сотрудника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровья сотрудника, а также в случаях, установленных Федеральным законом;
- не сообщать ПДн сотрудника в коммерческих целях без его письменного согласия;
- предупредить лиц получающих ПДн сотрудника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от третьих лиц подтверждения того, что это правило соблюдено. Лица, получающие ПДн сотрудника, обязаны соблюдать конфиденциальность. Данное Положение не распространяется на обмен ПДн сотрудников в порядке, установленном Федеральными законами;

- разрешать доступ к ПДн сотрудников только специально уполномоченным лицам, при этом указанные лица должны иметь право получить только те ПДн сотрудника, которые необходимы для выполнения конкретных функций;

- не запрашивать информацию о состоянии здоровья сотрудника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения сотрудником трудовой функции;

- передавать ПДн сотрудника его представителям в порядке, установленном Трудовым кодексом РФ, и ограничивать эту информацию только теми ПДн сотрудника, которые необходимы для выполнения указанными представителями их функций.

11. Защита ПДн сотрудников Учреждения

11.1. Защита ПДн сотрудников в Учреждении организована в соответствии с разработанными и введенными организационными и техническими мерами защиты, которые доводятся до каждого сотрудника Учреждения под роспись. В дополнение к разработанным вышеперечисленным мерам в Учреждении введены следующие правила по защите ПДн сотрудников, а именно:

- в целях обеспечения сохранности и конфиденциальности ПДн сотрудников Учреждения все операции должны выполняться только сотрудниками: Директором, его заместителями, сотрудниками бухгалтерии, сотрудники отдела кадров (управления персоналом), сотрудниками отделений, осуществляющими данную обработку в соответствии со своими служебными обязанностями, зафиксированными в их должностных инструкциях;

- ответы на письменные запросы других Организаций и Учреждений в пределах их компетенции и предъявленных полномочий даются в письменной форме на бланке Организации и в том объеме, который позволяет не разглашать излишний объем ПДн о сотрудниках Учреждения;

- передача информации, содержащей сведения о ПДн сотрудников Учреждения, по телефону, факсу, электронной почте без письменного согласия сотрудника запрещается.

12. Ответственность за разглашение информации отнесенной к ПДн сотрудника Учреждения

12.1. Лица виновные в нарушении норм, регулирующих получение, обработку и защиту ПДн сотрудника, несут предусмотренную законодательством Российской Федерации ответственность.

**Приложение №1. Форма соглашения сотрудника Учреждения на обработку его
ПДн**

Я _____ (Ф.И.О.)

_____ (номер основного документа, удостоверяющего его личность, сведения о дате выдачи
указанного документа и выдавшие его органы)

даю согласие на обработку сведений, составляющих мои персональные данные, персональные данные членов моей семьи сотрудникам Учреждения, которым эти данные необходимы для выполнения должностных обязанностей в целях исполнения условий моего трудового договора, законодательства РФ.

Согласен на совершение Учреждением следующих действий: сбор, систематизацию, накопление, хранение, уточнение, обновление, изменение, использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных следующими способами: автоматизированная обработка, обработка без использования средств автоматизации.

О персональной ответственности за несанкционированную обработку персональных данных предупрежден.

Срок действия настоящего согласия - на период действия моего трудового договора. С правом отзыва настоящего согласия ознакомлен(а).

С юридическими последствиями обработки моих персональных данных ознакомлен(а). О конфиденциальности персональных данных сотрудников Учреждения предупрежден(а). « _____ » _____ 201__ г.

(подпись

расшифровка

подписи)

Приложение №3. Форма Акта уничтожения носителей ПДн

УТВЕРЖДАЮ

Директор КГАПОУ ПСК

И.А. Коновалов

«_____» _____ 2016 г.

А К Т № _____

об уничтожении носителей персональных данных

Комиссия, в составе:

Председатель: _____ / _____ /

Члены комиссии: _____ / _____ /

_____ / _____ /

провела отбор носителей персональных данных (бумажные носители, дискеты, компакт-диски, флешь и т.д.) и установила, что в соответствии с требованиями руководящих документов по защите информации отнесенной к персональным данным, информация, записанная на этих носителях, достигла цели своей обработки и подлежит дальнейшему уничтожению:

№ п/п	Дата	Тип носителя	Регистрационный номер носителя персональных данных	Примечание
1				
2				
3				

После утверждения акта персональные носители сверены с записями в акте и уничтожены путем

_____ (разрезание, сжигание, механическое уничтожение и т.п.)

Уничтоженные носители с журналов учета списаны.

Подписи членов комиссии:

Председатель: _____ / _____ /

Члены комиссии: _____ / _____ /

_____ / _____ /

