

**МИНИСТЕРСТВО ОБРАЗОВАНИЯ, НАУКИ И МОЛОДЕЖНОЙ ПОЛИТИКИ
КРАСНОДАРСКОГО КРАЯ
ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ КРАСНОДАРСКОГО КРАЯ
«УСПЕНСКИЙ ТЕХНИКУМ МЕХАНИЗАЦИИ И ПРОФЕССИОНАЛЬНЫХ
ТЕХНОЛОГИЙ»**

УТВЕРЖДЕНО
приказом от 01.11.2017 г. №450-ПР

ПОЛОЖЕНИЕ

Об обработке и защите персональных данных в государственном бюджетном профессиональном образовательном учреждении Краснодарского края «Успенский техникум механизации и профессиональных технологий»

1. Общие положения

1.1. Положение об обработке и защите персональных данных определяет порядок приема, учета, обработки, хранения и защиты персональных данных работников и обучающихся образовательной организации. Настоящее положение (далее – Положение) разработано в соответствии с Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным законом от 27 июля 2006 года №152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 17 ноября 2007 г. №781 «Об утверждении Положения об обеспечении безопасности 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» и уставом образовательной организации.

1.2. Положение закрепляет и регулирует комплекс мер, направленных на обеспечение защиты персональных данных, хранящихся в образовательной организации.

2. Понятие и состав персональных данных

2.1. Под персональными данными работников и обучающихся понимается информация, необходимая руководству образовательной организации в связи с трудовыми отношениями и отношениями, возникающими в связи с предоставлением образовательных услуг и касающиеся конкретного работника и обучающегося.

Персональные данные являются конфиденциальной информацией, охраняемой в установленном законом порядке.

2.2. К персональным данным относятся:

2.2.1. все биографические и анкетные данные работника или обучающегося (ФИО, дата и место рождения, пол и т.д.);

2.2.2. специальность, квалификация, профессиональная подготовка, сведения о повышении квалификации;

2.2.3. занимаемая должность;

2.2.4. факты биографии и предыдущей трудовой деятельности (место работы, размер заработка, наличие судимости, сведения о трудовом стаже, отношение к воинской обязанности);

2.2.5. адрес регистрации и местожительства;

2.2.6. номер телефона;

2.2.7. семейное положение, состав семьи;

2.2.8. место работы или учебы членов семьи и родственников;

2.2.9. размер заработной платы или стипендии;

2.2.10. содержание трудового договора;

2.2.11. содержание договора на обучение по основным программам профессионального обучения;

2.2.12. деловые и иные личные качества;

2.2.13. результаты медицинского обследования на предмет годности к осуществлению трудовых обязанностей, либо к обучению.

2.3. Документы, содержащие сведения, составляющие персональные данные:

2.3.1. Документы работников образовательной организации:

- документы, предъявляемые при заключении трудового договора: паспорт или документ, удостоверяющий личность; трудовая книжка; страховое свидетельство государственного пенсионного страхования; документы об образовании; документы воинского учета.

- документы о составе семьи, необходимые для предоставления гарантий, связанных с выполнением семейных обязанностей: свидетельство о заключении брака, свидетельство о рождении ребенка.

- документы о состоянии здоровья детей и других близких родственников, когда с наличием таких документов связано предоставление работнику каких-либо гарантий и компенсаций: справка об инвалидности и др.

2.3.2. Документы обучающихся в образовательной организации:

- документы, предъявляемые в приемную комиссию при заполнении заявления о приеме в образовательную организацию: паспорт или документ, удостоверяющий личность; документы об образовании; документы воинского учета.

- Документы, подтверждающие право на дополнительные гарантии и компенсации по определенным основаниям: об инвалидности и др.

- медицинская справка формы 086-У и др.

2.4. Собственником персональных данных является субъект, в полном объеме реализующий полномочия владения, пользования и распоряжения этими ресурсами. Это любой гражданин, к личности которого относятся соответствующие персональные данные и которые вступили или изъявил желание вступить в отношения с образовательной организацией. Собственник самостоятельно решает вопрос передачи образовательной организации своих персональных данных.

2.5. Держателем персональных данных является образовательная организация, которой работник или обучающийся добровольно передает во владение свои персональные данные. Права и обязанности образовательной организации в трудовых отношениях и в отношениях, связанных с предоставлением образовательных услуг осуществляются директором образовательной организации.

2.6. Пользователями (потребителями) персональных данных являются юридические и физические лица, обратившиеся к собственнику или держателю персональных данных за получением необходимых сведений и пользующиеся ими без права передачи и разглашения.

3. Обработка персональных данных

3.1. Обработка персональных данных включает в себя их получение, систематизацию, хранение, уточнение, изменение, передачу, а также блокирование, защиту и уничтожение.

3.2. Основными принципами обработки персональных данных в образовательной организации являются:

3.2.1. принцип законности целей и способов обработки персональных данных;

3.2.2. принцип соответствия объема и характера обрабатываемых персональных данных способам и целям их обработки;

3.2.3. принцип достоверности персональных данных, их достаточности для целей обработки;

3.2.4. принцип защиты персональных данных от неправомерного доступа и их использования или утраты.

3.3. При обработке персональных данных должны соблюдаться следующие общие требования:

3.3.1. обработка персональных данных работника может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов; содействия работникам в трудоустройстве, обучении и продвижении по карьерной лестнице, контроля качества выполняемой работы и обеспечения сохранности имущества;

3.3.2. все персональные данные работника следует получать от него самого. Если персональные данные работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее с указанием целей, источников и способов получения персональных данных и от него должно быть получено письменное согласие;

3.3.3. 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 трудовыми отношениями, работодатель вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия;

3.3.4. работодатель не имеет права получать и обрабатывать персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных Трудовым кодексом Российской Федерации;

3.3.5. защита персональных данных работника от неправомерного их использования или утраты должна быть обеспечена за счет средств работодателя, в порядке предусмотренном Трудовым кодексом Российской Федерации;

3.3.6. работники и их представители должны быть ознакомлены под роспись с документами работодателя, регламентирующими порядок обработки персональных данных;

3.3.7. работодатель, работники и их представители должны совместно выработать меры защиты персональных данных работников.

4. Работа с персональными данными

4.1. Персональные данные добровольно передаются работниками и обучающимися непосредственно держателю этих данных и потребителям внутри образовательной организации исключительно для обработки и использования в работе.

К числу массовых потребителей персональных данных вне образовательной организации относятся государственные и негосударственные учреждения и организации:

- налоговые инспекции;
- правоохранительные органы;
- органы статистики;
- страховые агентства;
- военкоматы;
- органы социального страхования;
- пенсионные фонды;
- подразделения органов местного самоуправления.

Передача информации, содержащей персональные данные возможна только с ведома и (или) по распоряжению директора образовательной организации. Экземпляры передаваемой информации дублируются и хранятся в образовательной организации на соответствующих носителях информации в течение трех лет.

Внутри образовательной организации к разряду потребителей персональных данных относятся работники структурных подразделений, которым эти данные необходимы для выполнения должностных обязанностей:

- специалист по кадрам;
- ведущий бухгалтер;
- экономист;
- секретарь руководителя;
- социальный педагог;
- педагог – психолог;
- руководители структурных подразделений.

4.2. Персональные данные работников содержатся в основном документе персонального учета работников – в личном деле, которое формируется специалистом по кадрам после издания приказа о приеме работника на работу. В случаях, непосредственно связанных с вопросами трудовых отношений, получение и обработка данных о частной жизни работника возможны только с его письменного согласия. Личное дело работника пополняется на протяжении всей трудовой деятельности в образовательной организации. После увольнения работника документы по личному составу передаются на хранение в архив образовательной организации.

4.3. Персональные данные обучающихся содержатся в основном документе персонального учета обучающихся – в личном деле, которое формируется учебной частью после издания приказа о зачислении на учебу и хранится в специально оборудованном шкафу.

4.4. Документы, содержащие информацию о персональных данных работников и обучающихся, хранятся на бумажных и электронных носителях в отделе кадров, бухгалтерии и в учебной части.

Доступ к такой информации без получения специального разрешения имеют директор образовательной организации, его заместители, главный бухгалтер, специалист по кадрам в соответствии со своими должностными обязанностями. Иные работники образовательной организации могут иметь доступ к персональным данным в случае получения разрешения директора в виде визы на служебной записке, обосновывающей

необходимость ознакомления и использования персональных данных конкретного работника или обучающегося.

4.5. При обработке персональных данных работников и обучающихся директор образовательной организации вправе определять способы обработки, документирования, хранения и защиты персональных данных работников и обучающихся на базе современных образовательных технологий.

5. Обеспечение безопасности персональных данных при их обработке в информационных системах

5.1. Под техническими средствами, позволяющими осуществлять обработку персональных данных, понимаются средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных и средства защиты информации, применяемые в информационных системах.

5.2. Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

5.3. Обмен персональными данными при их обработке в информационных системах осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и путем применения технических средств.

5.4. При обработке персональных данных в информационной системе должно быть обеспечено:

5.4.1. проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным;

5.4.2. своевременное обнаружение фактов несанкционированного доступа к персональным данным;

5.4.3. возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

5.4.4. постоянный контроль за обеспечением уровня защищенности персональных данных.

5.5. Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах включают в себя:

5.5.1. определение угроз безопасности персональных данных при их обработке;

5.5.2. установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;

5.5.3. обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними.

5.5.4. учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных.

5.5.5. контроль за соблюдением условий использования средств защиты информации.

5.5.6. описание системы защиты персональных данных.

6. Передача персональных данных

6.1. При передаче персональных данных работников и лиц обучающихся руководство образовательной организации должно соблюдать следующие требования:

- передача персональных данных от держателя или его представителя внешнему потребителю допускается в минимальных объемах и только в целях выполнения задач, соответствующих объективной причине сбора этих данных;

- при передаче персональных данных работника или обучающегося потребителям за пределы образовательной организации работодатель не должен сообщать эти данные без письменного согласия работника или обучающегося, за исключением случаев когда это необходимо в целях предупреждения угрозы жизни и здоровья или в случаях, установленных федеральным законом.

- ответы на правомерные запросы других учреждений и организаций даются с разрешения директора образовательной организации в письменной форме и в объеме, который позволяет не разглашать излишний объем персональных данных.

- не допускается отвечать на вопросы, связанные с передачей персональных данных по телефону или факсу.

- по возможности персональные данные обезличиваются.

7. Защита персональных данных

7.1. Защита персональных данных представляет собой регламентированные процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и, обеспечивающий достаточно надежную безопасность информации в процессе управленческой и образовательной деятельности образовательной организации.

7.2. Под угрозой или опасностью утраты персональных данных понимается единичное или комплексное, реальное или потенциальное, активное или пассивное проявление возможностей внешних или внутренних источников угрозы создавать неблагоприятные события, оказывать дестабилизирующее воздействие на защищаемую информацию.

Риск угрозы любым информационным ресурсам создают стихийные бедствия, экстремальные ситуации, террористические акты, аварии технических средств и линий связи, другие объективные обстоятельства, а также заинтересованные и незаинтересованные в возникновении угрозы лица.

7.3. Внутренняя защита – регламентация доступа к конфиденциальным сведениям, документам и базам данных.

Для защиты персональных данных необходимо соблюдать ряд мер:

- ограничивать и регламентировать состав работников, функциональные обязанности которых требуют владения конфиденциальной информацией;

- избирательно и обоснованно распределять документы и информацию между работниками;

- знакомить работников с требованиями нормативно – методических документов по защите информации и сохранении тайны;

- создавать необходимые условия в помещении для работы с персональными данными;

- определять и регламентировать состав работников, имеющих право доступа в помещение, в котором находятся документы, содержащие персональные данные;

- проводить разъяснительную работу с работниками образовательной организации по предупреждению утраты сведений при работе с персональными данными;

7.4. Внешняя защита – комплекс мер, направленных на создание неблагоприятных условий и труднопреодолимых препятствий для лиц, пытающихся получить несанкционированный доступ (в целях видоизменения, уничтожения, подмены и фальсификации) к документам, содержащим персональные данные.

Для защиты персональных данных образовательная организация соблюдает следующие меры:

- 7.4.1. установление порядка приема, учета и контроль деятельности посетителей;
- 7.4.2. пропускной режим;
- 7.4.3. охрана территории, зданий, помещений и транспортных средств.

8. Ответственность за разглашение конфиденциальной информации, содержащей персональные данные.

8.1. Персональная ответственность является обязательным условием обеспечения эффективности защиты системы персональных данных.

8.2. Каждый работник образовательной организации, получающий для работы документ, содержащий персональные данные, несет персональную ответственность за сохранность носителя и конфиденциальность информации.

8.3. Нарушение установленного действующим законодательством порядка сбора, хранения, использования или распространения информации о работниках и обучающихся влечет дисциплинарную, административную, гражданско-правовую или уголовную ответственность граждан и юридических лиц в соответствии с действующим законодательством.

СОГЛАСОВАНО

Юрисконсульт

Специалист по кадрам

Н.Л.Страшко

В.С.Петрова