Согласовано:
Председатель первичной
профсоюзной организации
ГБПОУ СК «СКУД»
_____ С.А. Продченко
«19» декабря 2016 г.

Утверждаю:
Директор ГБПОУ СК «СКУД»
_____ В.Н. Арзуманов
«19» декабря 2016 г.

Подписано цифровой подписью: Арзуманов Валерий Николаевич
DN: E=uc_fk@roskazna.ru, S=г. Москва, ИНН=007710568760, ОГРН=1047797019830, STREET="Большой Златоустинский переулок, д. 6, строение 1", L=Москва, C=RU, O=Федеральное казначейство, CN=Федеральное казначейство
Причина: Я утвердил этот документ
Дата: 11 Октябрь 2022 г. 0:02:24

ПОЛОЖЕНИЕ
об обработке и защите персональных данных работников государственного бюджетного профессионального образовательного учреждения «Ставропольское краевое училище дизайна» (техникум).

1. **Общие положения**

1.1. Настоящее Положение об обработке и защите персональных данных работников государственного бюджетного профессионального образовательного учреждения «Ставропольское краевое училище дизайна» (техникум) (далее – Положение) устанавливает порядок приема, учета, сбора, поиска, обработки, накопления и хранения документов, содержащих сведения, отнесенные к персональным данным сотрудников государственного бюджетного профессионального образовательного учреждения «Ставропольское краевое училище дизайна» (техникум) (далее – училище, работодатель).

1.2. Настоящее Положение разработано в соответствии с Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Кодексом РФ об административных правонарушениях № 195 – ФЗ от 30.12.2001 г.; Федеральным законом от 27.07.2006 № 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. Целью настоящего Положения является развитием комплекса мер, направленных на обеспечение защиты персональных данных, хранящихся у работодателя, посредством планомерных действий по совершенствованию организации труда.

1.4. Положение о защите персональных данных и изменения утверждаются директором ГБПОУ СК «СКУД».

2. Основные понятия

Для целей настоящего Положения используются следующие понятия:

2.1. Работник - физическое лицо, состоящее в трудовых отношениях с работодателем.

2.2. Работодатель – государственное бюджетное профессиональное образовательное учреждение Ставропольского края «Ставропольское краевое училище дизайна» (техникум).

2.3. Персональные данные - любая информация, необходимая работодателю в связи с трудовыми отношениями и относящаяся прямо или косвенно к конкретному работнику, в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

2.3.1. К персональным данным относятся:

№ по перечню	Персональные сведения
1	ФИО
2	паспортные данные
3	ИНН, страховое медицинское свидетельство обязательного пенсионного страхования

4	место рождения
5	все биографические сведения сотрудника
6	образование;
7	специальность, профессия
8	занимаемая должность, сведения о квалификации
9	наличие судимостей
10	адрес местожительства, домашний телефон
11	состав семьи
12	социальное положение
13	размер заработной платы;
14	содержание трудового договора
15	подлинники и копии приказов по личному составу, основания к приказам по личному составу
16	личные дела, личные карточки (форма Т2) и трудовые книжки сотрудников
17	дела, содержащие материалы по повышению квалификации и переподготовке сотрудников, их аттестации, служебным расследованиям
18	копии отчетов, направляемые в органы статистики
19	анкета
20	копии документов об образовании
21	результаты медицинского обследования на предмет годности к осуществлению трудовых обязанностей
22	дата рождения
23	фотографии и иные сведения, относящиеся к персональным данным сотрудника
24	лицевые счета работников
25	Иная информация необходимая работодателю в связи с трудовыми отношениями с соответствующим работником

2.4. 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;

2.5. Распространение персональных данных - действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

2.6. Использование персональных данных - действия (операции) с персональными данными, совершаемые работодателем 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.

2.7. Блокирование персональных данных - временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи.

2.8. Уничтожение персональных данных - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

2.9. Сотрудник - лицо, имеющие трудовые отношения с училищем.

2.10. К персональным данным относятся:

2.10.1. Сведения, содержащиеся в документе, удостоверяющем личность работника.

2.10.2. Информация, содержащаяся в трудовой книжке работника.

2.10.3. Информация, содержащаяся в страховом свидетельстве государственного пенсионного страхования;

2.10.4. Сведения, содержащиеся в документах воинского учета.

2.10.5. Сведения об образовании, квалификации или наличии специальных знаний или подготовки, в том числе основном и дополнительном образовании

2.10.6. Информация медицинского характера, в случаях, предусмотренных законодательством.

2.10.7. Сведения, содержащиеся в свидетельстве о постановке на учет физического лица в налоговом органе на территории Российской Федерации.

2.10.8. Сведения о семейном положении работника.

2.10.9. Сведения, содержащиеся в анкетных данных, автобиографии работника, личном листке по учету кадров.

3. Состав персональных данных

3.1. Субъектом персональных данных (собственником информационных ресурсов) – является субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения этими ресурсами. Это любой гражданин, к личности которого относятся соответствующие персональные данные, и который вступил (стал сотрудником) или изъявил желание вступить в трудовые отношения с работодателем. Субъект персональных данных самостоятельно решает вопрос передачи работодателю своих персональных данных.

3.2. Держателем персональных данных является работодатель, которому сотрудник добровольно передает во владение свои персональные данные. Работодатель выполняет функцию владения этими данными и обладает полномочиями распоряжения ими в пределах, установленных законодательством.

3.3. Права и обязанности работодателя в трудовых отношениях осуществляются физическим лицом, уполномоченным работодателем. Указанные права и обязанности он может делегировать нижестоящим руководителям – своим заместителям, руководителям структурных подразделений, работа которых требует знания персональных данных работников или связана с обработкой этих данных.

3.4. Потребителями (пользователями) персональных данных являются юридические и физические лица, обращающиеся к собственнику или держателю персональных данных за получением необходимых сведений и пользующиеся ими без права передачи и разглашения.

4. Принципы обработки персональных данных

4.1. Обработка персональных данных включает в себя действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных, получение, хранение, комбинирование, передачу, а также актуализацию, блокирование, защиту, уничтожение.

Получение, хранение, комбинирование, передача или любое другое использование персональных данных сотрудника может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности сотрудников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

4.2. Все персональные данные сотрудника получаются у него самого. Если персональные данные сотрудника возможно получить только у третьей стороны, то сотрудник должен быть уведомлен об этом заранее, и от него должно быть получено письменное согласие. Работодатель должен сообщить сотруднику о целях,

предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа сотрудника дать письменное согласие на их получение.

При принятии решений относительно сотрудника на основании его персональных данных не допускается использование данных, полученных исключительно в результате их автоматизированной обработки или электронного получения.

4.3. Хранение персональных и учетных данных работников осуществляется кадровой службой, бухгалтерией, учебной частью на бумажных и электронных носителях, которые обеспечивают их защиту от несанкционированного доступа и копирования.

В кадровой службе персональные данные хранятся на бумажных носителях в личных карточках по форме N Т-2 и личных делах, которые также могут содержать документы, содержащие персональные данные сотрудника, в порядке, отражающем процесс приема на работу. Для этого используются специально оборудованные шкафы или сейфы, которые запираются. Личное дело пополняется на протяжении всей трудовой деятельности сотрудника в училище. Изменения, вносимые в карточку Т-2, должны быть подтверждены соответствующими документами (например, копия свидетельства о браке).

Кадровая служба, вправе передавать персональные данные работника в бухгалтерию, учебную часть, руководителям структурных подразделений в случаях, установленных законодательством, необходимых для исполнения должностных обязанностей работников, в случае если указанные службы наделены соответствующими полномочиями директором училища.

Сотрудник отдела кадров, ответственный за документационное обеспечение кадровой деятельности, принимает от принимаемого на работу сотрудника документы, проверяет полноту их заполнения и правильность указываемых сведений в соответствии с предъявленными документами.

После увольнения документы по личному составу передаются на архивное хранение.

4.4. Уничтожение персональных данных.

4.4.1. Персональные данные работников хранятся не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

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

4.4.3. При обработке персональных данных сотрудников работодатель в лице директора вправе определять способы обработки, документирования, хранения и защиты персональных данных сотрудников училища на базе современных информационных технологий.

Работник обязан:

- передавать работодателю или его представителю комплекс достоверных, документированных персональных данных, состав которых установлен Трудовым кодексом РФ;

- своевременно сообщать работодателю об изменении своих персональных данных.

Работник имеет 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 сотрудника, за исключением случаев, предусмотренных законодательством РФ;

- определение своих представителей для защиты своих персональных данных;

- требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований.

- при отказе работодателя или уполномоченного им лица исключить или исправить персональные данные работника - заявить в письменной форме о своем несогласии, представив соответствующее обоснование;

- требование об извещении работодателем всех лиц, которым ранее были сообщены неверные или неполные персональные данные сотрудника, обо всех произведенных в них исключениях, исправлениях или дополнениях;

- дополнить персональные данные оценочного характера заявлением, выражающим его собственную точку зрения;

- обжалование в суд любых неправомерных действий или бездействия работодателя при обработке и защите его персональных данных.

Для защиты персональных данных работников работодатель обязан:

- за свой счет обеспечить защиту персональных данных работника от неправомерного их использования или утраты в порядке, установленном законодательством РФ;

- ознакомить работника и его представителей с настоящим Положением и их правами в области защиты персональных данных под роспись;

- осуществлять передачу персональных данных работника только в соответствии с настоящим Положением и законодательством Российской Федерации;

- предоставлять персональные данные работника только уполномоченным лицам и только в той части, которая необходима им для выполнения их трудовых обязанностей в соответствии с настоящим Положением и законодательством Российской Федерации;

- обеспечить работнику свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей его персональные данные, за исключением случаев, предусмотренных законодательством;

- по требованию работника предоставить ему полную информацию о его персональных данных и обработке этих данных;

- работодатель не вправе обрабатывать персональные данные работника о его политических, религиозных, философских и иных убеждениях, состояния здоровья и интимной жизни жизни, за исключением случаев, предусмотренных частью 2 ст. 10 Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных".

В случаях, непосредственно связанных с вопросами трудовых отношений, работодатель вправе получать и обрабатывать персональные данные работника о его личной жизни только с письменного согласия работника;

5. Доступ к персональным данным

Персональные данные добровольно передаются сотрудником непосредственно держателю этих данных и потребителям внутри училища исключительно для обработки и использования в работе.

Внешний доступ. К числу массовых потребителей персональных данных вне училища можно отнести государственные и негосударственные функциональные структуры:

— налоговые инспекции;
— правоохранительные органы;
— органы статистики;
— органы медицинского страхования;
— военкоматы;
— органы социального страхования;
— пенсионные фонды;
— государственные и муниципальные органы управления.

Внутренний доступ. Внутри училища к разряду потребителей персональных данных относятся сотрудники функциональных структурных подразделений, которым эти данные необходимы для выполнения должностных обязанностей:

– директор;
– сотрудники бухгалтерии;
– начальники структурных подразделений.
– специалист по кадрам, юрисконсульт;
– секретарь руководителя, секретарь учебной части.

Право доступа к персональным данным других работников определяется приказом директора училища.

6. Передача персональных данных

6.1. При передаче персональных данных работника работодатель должен соблюдать следующие требования:

6.1.1. Передача внешнему потребителю:

– работодатель вправе передавать персональные данные работника третьим лицам и сторонним училищу организациям только при наличии письменного согласия работника. При отсутствии письменного согласия работника передача персональных данных производится исключительно в целях предупреждения угрозы жизни и здоровья работника, а также в других случаях, установленных законодательством.
– ответы на правомерные письменные запросы других фирм, учреждений и организаций даются с разрешения директора и только в письменной форме и в том объеме, который позволяет не разглашать излишний объем персональных сведений;
– по возможности персональные данные обезличиваются.
– при передаче персональных данных работника лица, получающие данную информацию, должны быть предупреждены представителем работодателя о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, от этих лиц должно быть получено письменное подтверждение соблюдения этого условия.

6.1.2. Передача внутреннему потребителю.

Работодатель вправе разрешать доступ к персональным данным сотрудников внутри училища. Право доступа к персональным данным других работников определяется приказом директора. Внутренние потребители персональных данных должны подписать обязательство о неразглашении персональных данных работников.

7. Защита персональных данных

Под угрозой или опасностью утраты персональных данных понимается единичное или комплексное, реальное или потенциальное, активное или пассивное проявление злоумышленных 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 действия, аварии технических средств и линий связи, другие объективные обстоятельства, а также заинтересованные и незаинтересованные в возникновении угрозы лица.

Защита персональных данных представляет собой регламентированный технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и, в конечном счете, обеспечивающий достаточно надежную безопасность информации в процессе управленческой и производственной деятельности училища.

Безопасность персональных данных, обрабатываемых училищем, обеспечивается реализацией правовых, организационных, технических и программных мер, необходимых

и достаточных для обеспечения требований законодательства в области защиты персональных данных.

ГБПОУ СК «СКУД» предпринимает необходимые организационные и технические меры для обеспечения безопасности персональных данных от случайного или несанкционированного доступа, уничтожения, изменения, блокирования доступа и других несанкционированных действий, в том числе:

- назначение должностных лиц, ответственных за организацию обработки и защиты персональных данных;
- ограничение и регламентация состава работников, имеющих доступ к персональным данным;
- ознакомление работников с требованиями федерального законодательства и локальных нормативных документов по обработке и защите персональных данных;
- обеспечение учёта и хранения материальных носителей информации и их обращения, исключающего хищение, подмену, несанкционированное копирование и уничтожение; - определение угроз безопасности персональных данных при их обработке, формирование на их основе моделей угроз;
- разработка на основе модели угроз системы защиты персональных данных для соответствующего класса информационных систем;
- проверка готовности и эффективности использования средств защиты информации;
- реализация разрешительной системы доступа пользователей к информационным ресурсам, программно-аппаратным средствам обработки и защиты информации; - регистрация и учёт действий пользователей информационных систем персональных данных;
- парольная защита доступа пользователей к информационной системе персональных данных;
- применение средств контроля доступа к коммуникационным портам, устройствам ввода-вывода информации, съёмным машинным носителям и внешним накопителям информации;
- применение в необходимых случаях средств криптографической защиты информации для обеспечения безопасности персональных данных при передаче по открытым каналам связи и хранении на съемных машинных носителях информации; осуществление антивирусного контроля, предотвращение внедрения в корпоративную сеть вредоносных программ (программ-вирусов) и программных закладок; применение в необходимых случаях средств межсетевого экранирования; применение в необходимых случаях средств обнаружения вторжений в корпоративную сеть, нарушающих или создающих предпосылки к нарушению установленных требований по обеспечению безопасности персональных данных;
- применение в необходимых случаях централизованного управления системой защиты персональных данных;
- резервное копирование информации;
- обучение работников, использующих средства защиты информации, применяемые в информационных системах персональных данных, правилам работы с ними; - учёт применяемых средств защиты информации, эксплуатационной и технической документации к ним; - использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия;
- проведение мониторинга действий пользователей, проведение разбирательств по фактам нарушения требований безопасности персональных данных;
- размещение технических средств обработки персональных данных, в пределах охраняемой территории;
- организация пропускного режима;

- поддержание технических средств охраны, сигнализации помещений в состоянии постоянной готовности.

7.1. «Внутренняя защита»

Основным виновником несанкционированного доступа к персональным данным является, как правило, персонал, работающий с документами и базами данных. Регламентация доступа персонала к конфиденциальным сведениям, документами и базами данных входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий руководителями и специалистами училища. Для защиты персональных данных сотрудников необходимо соблюдать ряд мер:

– ограничение и регламентация состава сотрудников, функциональные обязанности которых требуют конфиденциальных знаний;
– строгое избирательное и обоснованное распределение документов и информации между сотрудниками;
– рациональное размещение рабочих мест сотрудников, при котором исключалось бы бесконтрольное использование защищаемой информации;
– знание сотрудниками требований нормативно – методических документов по защите информации и сохранении тайны;
– наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;
– организация порядка уничтожения информации;
– своевременное выявление нарушения требований разрешительной системы доступа сотрудниками подразделения;
– воспитательная и разъяснительная работа с сотрудниками по предупреждению утраты ценных сведений при работе с конфиденциальными документами;
– не допускается выдача личных дел сотрудников на рабочие места руководителей. Личные дела могут выдаваться на рабочие места только директору, и в исключительных случаях, по письменному разрешению директора, руководителю структурного подразделения;
– персональные компьютеры, в которых содержатся персональные данные, должны быть защищены паролями доступа.

7.2. «Внешняя защита»

Для защиты конфиденциальной информации создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лиц, пытающихся совершить несанкционированный доступ и овладение информацией. Целью и результатом несанкционированного доступа к информационным ресурсам может быть не только овладение ценными сведениями и их использование, но и их видоизменение, уничтожение, внесение вируса, подмена, фальсификация содержания реквизитов документа и др.

Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности училища, посетители, сотрудники других организационных структур.

Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов в кадровой службе.

Для защиты персональных данных сотрудников необходимо соблюдать ряд мер:

– порядок приема, учета и контроля деятельности посетителей;
– пропускной режим;
– порядок охраны территории, зданий, помещений, транспортных средств.

8. Ответственность за разглашение конфиденциальной информации, связанной с персональными данными

Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Трудовым кодексом РФ и иными федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.