Рег. № 3

УТВЕРЖДАЮ
Директор ФГБПОУ
«Медицинский колледж»
_____ В.А. Шаронова
«20» марта 2018г.

# ПОЛОЖЕНИЕ
## о защите персональных данных работников федерального государственного бюджетного профессионального образовательного учреждения «Медицинский колледж» Управления делами Президента Российской Федерации

## 1. Общие положения

1.1. Настоящее Положение о защите персональных данных работников регулирует порядок приема, учета, сбора, поиска, обработки, накопления и хранения документов, содержащих сведения, отнесенные к персональным данным всех работников федерального государственного бюджетного профессионального образовательного учреждения «Медицинский колледж» Управления делами Президента Российской Федерации (далее по тексту - «Колледж»).

1.2. В тексте данного Положения используются следующие понятия:

- Работодатель - федерального государственного бюджетного профессионального образовательного учреждения «Медицинский колледж» Управления делами Президента Российской Федерации
- Работники - лица, состоящие в трудовых отношениях с Работодателем.

1.3. Настоящее Положение составлено с целью развития комплекса мер, направленных на обеспечение защиты персональных данных,

хранящихся у Работодателя, посредством планомерных действий по совершенствованию организации труда в Колледже.

1.4. Положение о защите персональных данных работников утверждается директором Колледжа и вводится в действие приказом по Колледжу. Все работники Колледжа должны быть ознакомлены с настоящим Положением под роспись.

## 2. Понятие и состав персональных данных

2.1. Под персональными данными работников понимается информация, необходимая Работодателю в связи с трудовыми отношениями и касающаяся конкретного работника, а также сведения о фактах, событиях и обстоятельствах жизни работника, позволяющие идентифицировать его личность.

2.2. Персональные данные всегда являются конфиденциальной, строго охраняемой информацией.

2.3. К персональным данным работника относятся:

- все биографические сведения;
- образование;
- специальность;
- занимаемая должность;
- наличие судимостей;
- адрес места жительства;
- домашний телефон;
- состав семьи;
- место работы или учебы членов семьи и родственников;
- характер взаимоотношений в семье;
- размер заработной платы;
- содержание трудового договора;
- состав декларируемых сведений о наличии материальных ценностей;
- содержание декларации, подаваемой в налоговую инспекцию;

- подлинники и копии приказов по личному составу;
- личные дела, личные карточки (форма *12)* и трудовые книжки работников;
- основания к приказам по личному составу;
- дела, содержащие материалы по повышению квалификации и переподготовке работников, их аттестации, служебным расследованиям;
- копии отчетов, направляемые в органы статистики;
- анкета;
- копии документов об образовании;
- результаты медицинского обследования на предмет годности к осуществлению трудовых обязанностей;
- фотографии и т.п.

2.4. Документы, указанные в п. 2.3. настоящего Положения, являются конфиденциальными, однако, учитывая их массовость и единое место обработки и хранения - соответствующий гриф ограничения на них не ставится.

2.5. Режим конфиденциальности персональных данных снимается по истечении 75 лет срока хранения, если иное не определено законом.

2.6. Собственником информационных ресурсов (персональных данных) -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 работником) или изъявил желание вступить в трудовые отношения с Работодателем.

2.7. Субъект персональных данных самостоятельно решает вопрос передачи Работодателю своих персональных данных.

2.8. Держателем персональных данных является Работодатель, которому работник добровольно передает во владение свои персональные данные. Работодатель выполняет функцию владения этими данными и

обладает полномочиями распоряжения ими в пределах, установленных законодательством Российской Федерации.

2.9. Права и обязанности Работодателя в трудовых отношениях осуществляются физическим лицом, уполномоченным Работодателем. Сведения о персональных данных работников он может делегировать руководителям структурных подразделений, работа которых требует знания персональных данных работников или связана с обработкой этих данных.

2.10. Потребителями (пользователями) персональных данных работников являются юридические и физические лица, обращающиеся к Работодателю или кадровому работнику за получением необходимых сведений и пользующиеся ими без права передачи, разглашения.

## 3. Принципы обработки персональных данных

3.1. Обработка персональных данных работников включает в себя их получение, хранение, комбинирование, передачу, а также актуализацию, блокирование, защиту, уничтожение.

3.2. Получение, хранение, комбинирование, передача или любое другое использование персональных данных работника 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 работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

3.3. Все персональные данные работника получаются у него самого. Если персональные данные 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.

3.4. Не допускается получение и обработка персональных данных работника о его политических, религиозных и иных убеждениях и частной жизни, а также о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных законодательством Российской Федерации.

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

3.6. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со ст. 24 Конституции РФ возможно получение и обработка данных о частной жизни сотрудника только с его письменного согласия.

3.7. Защита персональных данных работников от неправомерного их использования или утраты обеспечивается Работодателем за счет его средств.

3.8. Пакет характеризующих материалов (далее пакет) работника формируется после издания приказа о его приеме на работу.

3.9. Пакет обязательно содержит личную карточку формы Т2, а также может содержать документы, содержащие персональные данные работника, в порядке, отражающем процесс приема на работу - это: заявление сотрудника о приеме на работу; характеристика-рекомендация; результат медицинского обследования на предмет годности к осуществлению трудовых обязанностей; копия приказа о приеме на работу; расписка работника об ознакомлении с документами организации, устанавливающими порядок обработки персональных данных работников, а также об его правах и обязанностях в этой области.

3.10. При заполнении личной карточки Т-2 используются следующие документы:

- паспорт;
- трудовая книжка;
- военный билет;
- документы об образовании;
- документы о присвоении ученой степени, ученого звания.

3.11. Пакет пополняется на протяжении всей трудовой деятельности работника в Колледже. Изменения, вносимые в карточку Т-2, должны быть подтверждены соответствующими документами (например, копия свидетельства о браке).

3.12. Ответственный за документационное обеспечение кадровой деятельности, принимает от принимаемого на работу работника документы, проверяет полноту их заполнения и правильность указываемых сведений в соответствии с предъявленными документами.

3.13. Под блокированием персональных данных понимается временное прекращение операций по их обработке по требованию субъекта персональных данных при выявлении им недостоверности обрабатываемых сведений или неправомерных действий в отношении его данных.

3.14. При обработке персональных данных работников Работодатель вправе определять способы обработки, документирования, хранения и защиты персональных данных работников Колледжа на базе современных информационных технологий.

## 4. Права и обязанности работника в целях обеспечения защиты персональных данных

4.1. Работник обязан:

- передавать Работодателю или его представителю комплекс достоверных, документированных персональных данных, состав которых установлен Трудовым кодексом Российской Федерации;
- своевременно сообщать Работодателю об изменении своих персональных данных.

4.2. В целях обеспечения защиты персональных данных, хранящихся у Работодателя, 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, за исключением случаев, предусмотренных законодательством Российской Федерации;
- определение своих представителей для защиты своих персональных данных;
- доступ к относящимся к ним медицинским данным;
- требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований. При отказе Работодателя исключить или исправить персональные данные работника он имеет право заявить в письменной форме Работодателю о своем несогласии с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера работник имеет право дополнить заявлением, выражающим его собственную точку зрения;
- 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;

- обжалование любых неправомерных действий или бездействия Работодателя при обработке и защите его персональных данных.

## 5. Доступ к персональным данным

5.1. Персональные данные добровольно передаются работником непосредственно работнику кадровой службы исключительно для обработки и использования в работе.

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

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

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

- все сотрудники отдела кадров;
- все сотрудники бухгалтерии;
- начальники структурных подразделений.

5.4. В отделе кадров хранятся личные карточки работников, работающих в настоящее время. Для этого используются специально

оборудованные шкафы или сейфы, которые запираются. Личные карточки располагаются в алфавитном порядке.

5.5. После увольнения документы по личному составу передаются на хранение.

## 6. Передача персональных данных

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

- передача персональных данных от держателя или его представителей внешнему потребителю может допускаться в минимальных объемах и только в целях выполнения задач, соответствующих объективной причине сбора этих данных;
- при передаче персональных данных работника потребителям (в том числе и в коммерческих целях) за пределы Колледжа Работодатель не должен сообщать эти данные третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника или в случаях, установленных федеральным законом;
- 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;
- не допускается отвечать на вопросы, связанные с передачей персональной информации по телефону или факсу;
- по возможности персональные данные обезличиваются;
- Работодатель вправе разрешать доступ к персональным данным работников только специально уполномоченным лицам.

## 7. Защита персональных данных

7.1. 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.

7.2. 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.

7.3. Защита персональных данных представляет собой жестко регламентированный и динамически 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.

7.4. Для защиты персональных данных работников необходимо соблюдать ряд мер:

- ограничение и регламентация состава работников, функциональные обязанности которых требуют конфиденциальных знаний;
- строгое избирательное и обоснованное распределение документов и информации между работниками;
- рациональное размещение рабочих мест, при котором исключалось бы бесконтрольное использование защищаемой информации;
- знание работниками требований нормативно - методических документов по защите информации и сохранении тайны;

- наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;
- определение и регламентация состава работников, имеющих право доступа (входа) в помещение, в котором находится вычислительная техника;
- организация порядка уничтожения информации;
- своевременное выявление нарушения работниками требований разрешительной системы доступа;
- воспитательная и разъяснительная работа с работниками по предупреждению утраты ценных сведений при работе с конфиденциальными документами;
- не допускается выдача личных дел работников на рабочие места. Личные дела могут выдаваться на рабочие места только директору и в исключительных случаях, по письменному разрешению директора руководителю структурного подразделения;
- персональные компьютеры, на которых содержатся персональные данные, должны быть защищены от несанкционированного доступа.

7.5. Для защиты конфиденциальной информации создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лица, пытающегося совершить несанкционированный доступ и овладение информацией.

7.6. 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.

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

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

7.9. Для защиты персональных данных работников также необходимо соблюдать: порядок приема, учета и контроля деятельности посетителей; пропускной режим в Колледже; порядок охраны территории, зданий, помещений, транспортных средств; требования к защите информации при интервьюировании и собеседованиях.

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

8.1. Персональная ответственность - одно из главных требований к организации функционирования системы защиты персональной информации и обязательное условие обеспечения эффективности этой системы.

8.2. Руководитель, разрешающий доступ работника к конфиденциальному документу, несет персональную ответственность за данное разрешение.

8.3. Каждый работник, получающий для работы конфиденциальный документ, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

8.4. 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 вплоть до увольнения по пп. «в» п.6 ст. 81 Трудового Кодекса РФ за разглашение

персональных данных другого работника, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.