Министерство культуры Российской Федерации
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Академия хорового искусства имени В.С. Попова»

Принято

на заседании Учёного совета
Академии хорового искусства
имени В.С. Попова
24.02.2025, протокол № 1

Утверждаю

И.о. ректора
Академии хорового искусства
имени В.С. Попова
_____ А.В. Соловьёв
«24» февраля 2025 года

ПОЛОЖЕНИЕ
о защите персональных данных

Москва 2025

1. Общие положения

1.1. Положение о защите персональных данных федерального государственного бюджетного образовательного учреждения высшего образования «Академия хорового искусства имени В.С. Попова» (далее – Академия) разработано в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», ~~и~~ иными нормативными правовыми актами в области защиты персональных данных, локальными правовыми актами и организационно-распорядительными документами Академии

1.2. Цель настоящего Положения – защита персональных данных работников, обучающихся и поступающих в Академию от несанкционированного доступа и разглашения, предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений.

1.3. В целях настоящего Положения:

- под персональными данными (далее – ПД) понимается любая информация, прямо или косвенно относящаяся к субъекту персональных данных;
- под угрозами безопасности ПД понимается совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных;
- под уровнем защищённости ПД понимается комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определённых угроз безопасности ПД при их обработке в информационной системе.

1.4. Настоящее Положение и изменения к нему утверждаются Работодателем и вводятся в действие приказом. Все работники должны быть ознакомлены под роспись с данным Положением и изменениями к нему.

2. Защита персональных данных

2.1. Работодатель принимает следующие меры по защите ПД:

2.1.1. Назначение лица, ответственного за обработку ПД, которое осуществляет организацию обработки ПД, обучение и инструктаж, внутренний контроль за соблюдением работниками требований к защите ПД.

2.1.2. Разработка политики в отношении обработки ПД.

2.1.3. Установление правил доступа к ПД, обеспечение регистрации и учёта всех действий, совершаемых с ПД.

2.1.4. Установление индивидуальных паролей доступа сотрудников в информационную систему в соответствии с их должностными обязанностями.

2.1.5. Применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации.

2.1.6. Сертифицированное антивирусное программное обеспечение с регулярно обновляемыми базами.

2.1.7. Соблюдение условий, обеспечивающих сохранность ПД и исключающих несанкционированный к ним доступ.

2.1.8. Обнаружение фактов несанкционированного доступа к ПД.

2.1.9. Восстановление ПД, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

2.1.10. Обучение работников, непосредственно осуществляющих обработку ПД, положениям законодательства РФ о персональных данных, в том числе требованиям к защите персональных данных, документам, определяющим политику Работодателя в отношении обработки ПД, локальным актам по вопросам обработки персональных данных.

2.1.11. Осуществление внутреннего контроля

2.1.12. Определение типа угроз безопасности и уровней защищенности ПД, которые хранятся в информационных системах.

2.2. Угрозы защищенности персональных данных.

2.2.1. Угрозы первого типа. В программном обеспечении информационной системы есть функциональные возможности, которые не указаны в описании к нему либо не отвечают характеристикам, которые заявил производитель. Это потенциально может привести к неправомерному использованию персональных данных.

2.2.2. Угрозы второго типа. Потенциальные проблемы с прикладным программным обеспечением — внешними программами, которые установлены на компьютерах работников.

2.2.3. Угрозы третьего типа. Потенциальной опасности ни от системного, ни от программного обеспечения нет.

2.3. Уровни защищённости персональных данных.

2.3.1. Первый уровень защищённости. Если работодатель отнес информационную систему к первому типу угрозы или если тип угрозы второй, но работодатель обрабатывает специальные категории ПД более 100 тыс. физических лиц без учета работников.

2.3.2. Второй уровень защищённости. Если тип угрозы второй и работодатель обрабатывает специальные категории ПД работников вне зависимости от их количества или специальные категории ПД менее чем 100 тыс. физических лиц, или любые другие категории ПД более чем 100 тыс. физических лиц, или при третьем типе угрозы работодатель обрабатывает специальные категории данных более чем 100 тыс. физических лиц.

2.3.3. Третий уровень защищённости. Если при втором типе угрозы работодатель обрабатывает общие ПД работников или менее чем 100 тыс. физических лиц, или при третьем типе угрозы работодатель обрабатывает

специальные категории ПД работников или менее чем 100 тыс. физических лиц, или при третьем типе угрозы работодатель обрабатывает биометрические ПД, или при третьем типе угрозы работодатель обрабатывает общие ПД более чем 100 тыс. физических лиц.

2.3.4. Четвёртый уровень защищенности. Если при третьем типе угрозы работодатель обрабатывает только общие ПД работников, обучающихся и поступающих или менее чем 100 тыс. физических лиц.

2.4. При четвёртом уровне защищенности персональных данных работодатель:

- обеспечивает режим безопасности помещений, в которых размещаете информационную систему;
- обеспечивает сохранность носителей информации;
- утверждает перечень работников, допущенных до ПД;
- использует средства защиты информации, которые прошли оценку соответствия требованиям закона в области обеспечения безопасности информации.

2.5. При третьем уровне защищённости ПД дополнительно к мерам, перечисленным в пункте 2.4 настоящего Положения, работодатель назначает ответственного за обеспечение безопасности ПД в информационной системе.

2.6. При втором уровне защищённости ПД дополнительно к мерам, перечисленным в пунктах 2.4, 2.5 настоящего Положения, работодатель ограничивает доступ к электронному журналу сообщений, за исключением работников, которым такие сведения необходимы для работы.

2.7. При первом уровне защищенности ПД дополнительно к мерам, перечисленным в пунктах 2.4—2.6 настоящего Положения, работодатель:

- обеспечивает автоматическую регистрацию в электронном журнале безопасности изменения полномочий работников по допуску к ПД в системе;
- создает отдел, ответственный за безопасность ПД в системе, либо возлагает такую обязанность на один из существующих отделов работодателя.

2.8. В целях защиты ПД на бумажных носителях работодатель:

- приказом назначает ответственного за обработку ПД;
- ограничивает допуск в помещения, где хранятся документы, которые содержат ПД работников, обучающихся и поступающих;
- хранит документы, содержащие ПД работников и обучающихся в шкафах, запирающихся на ключ;
- хранит трудовые книжки работников в сейфе в отделе обеспечения основной деятельности.

2.9. В целях обеспечения конфиденциальности документы, содержащие ПД работников, обучающихся и поступающих оформляются, ведутся и хранятся только специалистами, назначенными приказом Работодателя.

2.10. Работники Академии, допущенные к ПД работников, обучающихся и поступающих подписывают обязательства о неразглашении персональных

данных. В противном случае до обработки ПД работников обучающихся и поступающих не допускаются.

2.11. Допуск к документам, содержащим ПД работников, обучающихся и поступающих осуществляется в Академии на основании письменного разрешения ректора или проректоров.

2.12. Передача ПД по запросам третьих лиц, если такая передача прямо не предусмотрена законодательством Российской Федерации, допускается исключительно с согласия работника, обучающегося или поступающего на обработку его персональных данных в части их предоставления или согласия на распространение персональных данных.

2.13. Передача информации, содержащей сведения о ПД работников, обучающихся и поступающих, по телефону запрещается в связи с невозможностью идентификации лица, запрашивающего информацию.

3. Гарантии конфиденциальности персональных данных

3.1. Все работники Академии, осуществляющие обработку ПД, обязаны хранить тайну о сведениях, содержащих ПД, в соответствии с Положением, требованиями законодательства Российской Федерации.

3.2. Работник, обучающийся или поступающий вправе требовать полную информацию о своих персональных данных, об их обработке, использовании и хранении.

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