СОГЛАСОВАНО
Председатель первичной профсоюзной организации ГБУК «ГАВРНХ им. П.М. Милославова»
_____ Е.Ю. Каплина
01.09.2023г.

УТВЕРЖДАЮ
Директор ГБУК «ГАВРНХ им. П.М. Милославова»
_____В.Н. Натаров
01.09.2023 г.

ПОЛОЖЕНИЕ
о защите персональных данных государственного бюджетного учреждения культуры «Государственный академический Волжский русский народный хор им. П.М. Милославова»

1. Общие положения

1.1.Настоящее Положение о защите персональных данных (далее - Положение) государственного бюджетного учреждения культуры «Государственный академический Волжский русский народный хор им. П.М. Милославова» (далее – Учреждение, ГБУК «ГАВРНХ им. П.М. Милославова») разработано в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Трудовым кодексом Российской Федерации, Политикой Учреждения в отношении обработки персональных данных и иными нормативно-правовыми актами в области защиты персональных данных, действующими на территории Российской Федерации.

1.2.Цель настоящего Положения – защита персональных данных работников ГБУК «ГАВРНХ им. П.М. Милославова» от несанкционированного доступа и разглашения, предотвращение и выявление нарушений законодательства РФ. Персональные данные работников Учреждения являются конфиденциальной, строго охраняемой информацией, в соответствии с действующим законодательством Российской Федерации.

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 защищенности ПД понимается комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию

определенных угроз безопасности ПД при их обработке в информационной системе.

1.4. Настоящее Положение и изменения к нему утверждаются директором «ГБУК «ГАВРНХ им. П.М. Милославова» и вводятся приказом. Все работники должны быть ознакомлены под подпись с данным Положением и изменениями к нему.

2. Перечень документов и сведений, содержащих персональные данные работника

2.1.В соответствии с Трудовым кодексом Российской Федерации лицо, поступающее на работу в Учреждение, предъявляет работодателю следующие документы, содержащие его персональные данные:

- паспорт или другой документ, удостоверяющий личность, который содержит сведения о его паспортных данных, месте регистрации (месте жительства), семейном положении;
- трудовую книжку или справку СТД-Р (СТД-СФР), которая содержит сведения о трудовой деятельности работника;
- страховое свидетельство государственного пенсионного страхования, которое содержит сведения о номере и серии страхового свидетельства;
- документ об образовании, квалификации или наличии специальных знаний, содержащий сведения об образовании, профессии;
- документы воинского учета, которые содержат сведения о воинском учете военнообязанных и лиц, подлежащих призыву на военную службу.

2.2.В перечень документов и сведений, содержащих персональные данные, включаются:

- трудовой договор;
- сведения о состоянии здоровья (медицинское заключение);
- сведения о заработной плате.

3. Общие требования при обработке персональных данных и гарантии их защиты

3.1.Обработка персональных данных работника осуществляется исключительно в целях обеспечения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучения и продвижения по службе, обеспечения личной безопасности работника, сохранности имущества, контроля количества и качества выполняемой работы.

3.2.Все персональные данные передаются им лично. Если персональные данные работника 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.

3.3.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 вопросами трудовых отношений, в соответствии со ст. 24 Конституции Российской Федерации Работодатель вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия.

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 федеральным законом.

3.5.При принятии решений, затрагивающих интересы работника, Работодатель не имеет права основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронного получения.

4. Передача и защита персональных данных

4.1.Защита персональных данных – комплекс мероприятий технического, организационного и организационно-технического характера, направленных на защиту сведений, относящихся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных).

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

При передаче персональных данных работника работодатель должен соблюдать следующие требования:

• не сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в других случаях, предусмотренных Трудовым Кодексом Российской Федерации или иными федеральными законами;

• не сообщать персональные данные работника в коммерческих целях без его письменного согласия;

• предупредить лиц, получающих персональные данные работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено.

Лица, получающие персональные данные работника, обязаны соблюдать конфиденциальность. Данное положение не распространяется на обмен персональными данными работников в порядке, установленном федеральными законами.

• разрешать доступ к персональным данным работников только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций;

• не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции;

• передавать персональные данные работника представителям работников в порядке, установленном Трудовым Кодексом Российской Федерации и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.

4.3.В целях обеспечения сохранности и конфиденциальности персональных данных работников Учреждения все операции по оформлению, формированию, ведению и хранению персональных данных должны выполняться только ответственными работниками, осуществляющими данную работу в соответствии со своими служебными обязанностями, зафиксированными в их должностных инструкциях.

4.4.Ответы на письменные запросы других организаций и учреждений в пределах их компетенции и предоставленных полномочий даются в письменной форме на бланке Учреждения и в том объеме, который позволяет не разглашать излишний объем персональных сведений о работниках Учреждения.

4.5.Передача информации, содержащей сведения о персональных данных работников Учреждения, по телефону/факсу, электронной почте и другими электронными носителями без письменного согласия работника запрещается.

4.6.Личные дела и документы, содержащие персональные данные работников, хранятся в запирающихся шкафах (сейфах), обеспечивающих защиту от несанкционированного доступа.

4.7.Персональные компьютеры, в которых содержатся персональные данные, должны быть защищены паролями доступа, а также специальными антивирусными программами.

4.8.Внешние электронные накопители (флешки, карты памяти, жесткие диски и др.) хранятся в запираемых шкафах (сейфах).

4.9.Помещения, в которых находятся сейфы, шкафы, персональные компьютеры, указанные выше, имеют дверь с запирающимся на ключ замком.

4.10.Учреждение должно определять тип угроз безопасности и уровней защищенности ПД, которые хранятся в информационных системах.

4.11. Угрозы защищенности персональных данных.

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

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

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

4.12.Уровни защищенности персональных данных.

4.12.1.Первый уровень защищенности. 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.

4.12.2.Второй уровень защищенности. 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.

4.12.3.Третий уровень защищенности. 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.

4.12.4.Четвертый уровень защищенности. Если при третьем типе угрозы работодатель обрабатывает только общие ПД работников или менее чем 100 тыс. физических лиц.

4.13.При четвертом 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.

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

4.15.При втором уровне защищенности 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.

4.16.При первом уровне защищенности ПД дополнительно к мерам, перечисленным в пунктах 4.13—4.15 настоящего Положения, работодатель:

- обеспечивает автоматическую регистрацию в электронном журнале безопасности изменения полномочий работников по допуску к ПД в системе.

5. Доступ к персональным данным

5.1. Работники, допущенные к ПД работников, подписывают обязательства о неразглашении персональных данных. В противном случае до обработки ПД работников не допускаются.

5.2.Внутренний доступ (доступ внутри Учреждения).

Право доступа к персональным данным работника имеют:

- директор ГБУК «ГАВРНХ им. П.М. Милославова»;
- заместитель директора по развитию;
- художественный руководитель;
- секретарь руководителя;
- специалист по кадрам;
- инспекторы творческого коллектива (к тем данным, которые необходимы для выполнения конкретных функций);
- главный бухгалтер
- сотрудники бухгалтерии (к тем данным, которые необходимы для выполнения конкретных функций);
- менеджер по рекламе, специалист по связям с общественностью (к тем данным, которые необходимы для выполнения конкретных функций);
- старший администратор (к тем данным, которые необходимы для выполнения конкретных функций);
- юрисконсульт, ведущий (к тем данным, которые необходимы для выполнения конкретных функций);
- непосредственные руководители работников, предоставивших Учреждению свои персональные данные;
- сам работник, носитель данных.

5.3.Работники Учреждения, имеющие доступ к персональным данным работников, имеют право получать только те персональные данные работника, которые необходимы им для выполнения конкретных функций (внутренний ограниченный доступ к ПД).

5.4.В целях выполнения порученного задания доступ к персональным данным работника может быть предоставлен иному работнику, должность которого не включена в перечень должностей работников, имеющих доступ к персональным данным работников на основании предоставленного письменного согласия работника на обработку его персональных данных и согласованного распорядительного документа директора Учреждения.

5.5.Внешний доступ.

Учреждение вправе осуществлять передачу персональных данных работника третьим лицам, в том числе в коммерческих целях, только с его предварительного письменного согласия, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в других случаях, предусмотренных действующим законодательством Российской Федерации.

Перед передачей персональных данных Учреждение должно предупредить третье лицо о том, что они могут быть использованы только в целях, для которых были сообщены. При этом у третьего лица необходимо получить подтверждение того, что такое требование будет им соблюдено.

Не требуется согласие работника на передачу персональных данных:

- третьим лицам в целях предупреждения угрозы жизни и здоровью работника;
- в Социальный фонд России в объеме, предусмотренном действующим

законодательством Российской Федерации;

- в налоговые органы;
- в военные комиссариаты;
- по запросу профессиональных союзов в целях контроля за соблюдением трудового законодательства работодателем;
- по мотивированному запросу прокуратуры;
- по мотивированному требованию правоохранительных органов и органов безопасности;
- по запросу от государственных инспекторов труда при осуществлении ими надзорно-контрольной деятельности;
- по запросу судов;
- в органы и организации, которые должны быть уведомлены о тяжелом несчастном случае, в том числе со смертельным исходом;
- в случаях, связанных с исполнением работником должностных обязанностей;
- в кредитную организацию, обслуживающую платежные карты работников.

5.6.Другие организации:

- сведения о работнике (в том числе уволенном) могут быть предоставлены другой организации только с письменного запроса на бланке организации с приложением копии заявления работника.

5.7.Родственники и члены семей:

- персональные данные работника могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого работника.

6. Права работника в целях обеспечения защиты персональных данных хранящихся у Работодателя

6.1.В целях обеспечения защиты персональных данных, хранящихся у работодателя, работники имеют право на:

• полную информацию об их персональных данных и обработке этих данных;

• свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные работника, за исключением случаев, предусмотренных федеральным законом;

• требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований Трудового Кодекса Российской Федерации и настоящего Положения. 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;

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

• определение своих представителей для защиты своих персональных данных;

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

7. Гарантии конфиденциальности персональных данных

7.1. Все работники организации, осуществляющие обработку ПД, обязаны хранить тайну о сведениях, содержащих ПД, в соответствии с Положением, требованиями законодательства РФ.

7.2. Работник 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 персональных данных работников, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством Российской Федерации.