ВЕДОГОНЬ - ТЕАТР

Государственное бюджетное учреждение культуры города Москвы
«Ведогонь-театр»

г. Москва

«СОГЛАСОВАНО»
Председатель профкома

_____Ю.О. Буданова

«УТВЕРЖДАЮ»
Художественный руководитель

_____ П.В. Курочкин
«01» марта 2021 г.

ПОЛОЖЕНИЕ
о работе с персональными данными

Редакция № 2

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Целью данного Положения является защита персональных данных работников Государственного бюджетного учреждения культуры города Москвы «Ведогонь-театр» (далее – учреждение) от несанкционированного доступа, неправомерного их использования или утраты и установление правил работы с персональными данными работников учреждения.

1.2. Настоящее Положение разработано на основании статей Конституции РФ, Трудового кодекса РФ, Кодекса РФ об административных правонарушениях, Гражданского кодекса РФ, Уголовного кодекса РФ, Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», а также Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

1.3. Персональные данные относятся к категории конфиденциальной информации. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении 50 лет срока хранения, если иное не определено законом.

1.4. Настоящее Положение вступает в силу с момента его утверждения Художественным руководителем.

1.5. Все работники должны быть ознакомлены с настоящим Положением год роспись.

2. ПОНЯТИЕ И СОСТАВ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Под персональными данными сотрудников понимается информация,

необходимая учреждению 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. Состав персональных данных работника:

- анкетные данные, предоставленные при поступлении на работу, или в процессе работы (в т.ч. автобиография, сведения о семейном положении, перемене фамилии (имени), наличии детей и иждивенцев);
- владение иностранными языками и языками народов Российской Федерации;
- образование;
- специальность;
- сведения о трудовом и общем стаже;
- выполняемая работа с начала трудовой деятельности (включая военную службу, работу по совместительству, предпринимательскую деятельность и т.п.);
- сведения о составе семьи,
- сведения о личной и семейной жизни работника, включая личную и семейную тайны, ФИО близких и родственников, их даты рождения;
- идентификационный номер налогоплательщика;
- номер страхового свидетельства обязательного пенсионного страхования;
- Государственные и иные награды, знаки отличия (кем награжден и когда);
- паспортные данные, в т.ч. удостоверяющие личность гражданина Российской Федерации за пределами Российской Федерации;
- сведения о воинском учете;
- сведения о заработной плате сотрудника;
- сведения об особом социальном статусе работника (инвалидность, донор, беременность, член профсоюза и др.)
- сведения о социальных льготах;
- занимаемая должность;
- размер заработной платы;
- информация о наличии / отсутствии судимостей;
- адрес места жительства;
- домашний (контактный) телефон;
- содержание трудового договора и соглашений к нему;
- содержание декларации, подаваемой в налоговую инспекцию;
- подлинники и копии приказов по личному составу;
- личные дела, данные из личных карточек формы Т-2, трудовые книжки работников;
- основания к приказам по личному составу;
- дела, содержащие материалы по повышению квалификации и переподготовке работников, их аттестации, служебным расследованиям;
- копии отчётов, направляемые в органы статистики и другие государственные органы Российской Федерации;
- копии документов об образовании;
- сведения о состоянии здоровья работника, результаты медицинского обследования на предмет годности к осуществлению трудовых обязанностей, результаты психиатрического освидетельствования;

- фотографии и иные сведения, относящиеся к персональным данным работника;

- рекомендации, характеристики и т.п.

2.3. Под персональными данными физических лиц, состоящих в договорных и иных гражданско-правовых отношениях с учреждением, понимается информация, необходимая учреждению для оформления договорных и иных гражданско-правовых отношений и касающаяся конкретного физического лица, а также сведения о фактах, событиях и обстоятельствах жизни данного лица, позволяющие идентифицировать его личность.

2.4. Состав персональных данных физического лица, состоящего в договорных и иных гражданско-правовых отношениях с учреждением:

- паспортные данные;
- адрес места жительства;
- домашний телефон;
- содержание договора;
- номера ИНН и пенсионного свидетельства;
- копии отчётов, направляемые в органы статистики.

2.5. Указанные в п.2.2 и п.2.4. сведения являются конфиденциальными и не подлежат разглашению иначе как по основаниям, предусмотренным законодательством РФ.

3. СОЗДАНИЕ, ОБРАБОТКА, ХРАНЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Создание персональных данных работника.

Документы, содержащие персональные данные работника, создаются путём:

а) перенесения сведений из удостоверения личности, документа об образовании, пенсионного свидетельства, документов воинского учета в учётные формы (на бумажных и электронных носителях). Работодатель не принимает и не хранит копии личных документов работников, документы, которые работник предъявляет работодателю для хранения в оригинале (справки, медицинские заключения и т.д.) хранятся в личном деле работника в течение 50 лет после расторжения с работником трудового договора;

б) получения (приема) необходимых документов (трудовая книжка, личный листок по учёту кадров, автобиография, в необходимых случаях – результаты медицинского осмотра или медицинского заключения).

3.2. Обработка персональных данных работника - получение, хранение, комбинирование персональных данных работника. Обработка персональных данных работников осуществляется с их письменного согласия.

3.2.1. При обработке персональных данных работника в целях их защиты и обеспечения прав и свобод человека и гражданина, а также при определении объёма и содержания обрабатываемых персональных данных должны строго учитываться положения Конституции Российской Федерации, Трудового кодекса Российской Федерации и иных федеральных законов.

3.2.2. Обработка персональных данных работника осуществляется исключительно в целях:

а) обеспечения соблюдения законов и иных нормативных правовых актов;

б) содействия работникам в трудоустройстве;

в) обеспечения личной безопасности работников;

г) контроля количества и качества выполняемой работы;

д) обеспечения сохранности имущества работника и учреждения.

3.2.3. Все персональные данные работника следует получать у него самого, за исключением случаев, если их получение возможно только у третьей стороны.

3.2.4. Получение персональных данных работника у третьих лиц возможно только при уведомлении работника об этом заранее и с его письменного согласия.

В уведомлении работника о получении его персональных данных у третьих лиц должна содержаться следующая информация:

а) о целях получения персональных данных;

б) о предполагаемых источниках и способах получения персональных данных;

в) о характере подлежащих получению персональных данных;

г) о последствиях отказа работника дать письменное согласие на их получение.

3.2.5. Учреждение не имеет права получать и обрабатывать персональные данные работника о его политических, религиозных и иных убеждениях и частной жизни, равно как и персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом.

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

3.2.7. Работники и их представители должны быть ознакомлены под расписку с документами учреждения, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области.

3.3. Сведения, содержащие персональные данные работника, включаются в его личное дело, карточку формы № Т-2, а также содержатся на электронных носителях информации, доступ к которым разрешен лицам, непосредственно использующим персональные данные работника в служебных целях.

3.4. Хранение персональных данных в бухгалтерии:

а) персональные данные, содержащиеся на бумажных носителях, хранятся в запираемом шкафу, установленном на рабочем месте главного бухгалтера;

б) персональные данные, содержащиеся на электронных носителях информации, хранятся в ПК главного бухгалтера.

3.4.1. Персональные данные, включенные в состав личных дел, хранятся в запираемом шкафу, установленном на рабочем месте начальника отдела кадров. Персональные данные, содержащиеся на электронных носителях информации, хранятся в ПК начальника отдела кадров.

3.4.2. Трудовые книжки, документы по ведению воинского учета, карточки формы № Т-2 хранятся в запертом металлическом сейфе.

3.4.3. Доступ к персональным данным в соответствующем объеме строго

ограничен кругом лиц, определенных в пунктах 4.1, 4.1.1. настоящего Положения.

После истечения срока нормативного хранения документов, которые содержат персональные данные работника, документы подлежат уничтожению. В ходе проведения экспертизы отбираются материалы с истекшими сроками хранения и по итогам отбора составляется акт о выделении к уничтожению материалов, не подлежащих хранению. После чего документы измельчаются в шредере. Персональные данные работников в электронном виде стираются с информационных носителей.

4. ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ

4.1. Внутренний доступ (доступ внутри учреждения).

В рамках ГБУК г. Москвы «Ведогонь-театр» каждый работник имеет доступ к персональным данным коллег в следующем объеме: ФИО, должность, номер телефона и электронная почта коллег.

4.1.1. Право доступа к персональным данным работника в большем объеме имеют:

- художественный руководитель и первый заместитель художественного руководителя;
- руководители структурных подразделений по направлению деятельности (доступ к личным данным только работников своего подразделения);
- при переводе из одного структурного подразделения в другое доступ к персональным данным работника становится доступным руководителю нового подразделения;
- сам работник, носитель данных;
- другие работники учреждения при выполнении ими своих служебных обязанностей: секретарь руководителя, работники отдела кадров, работники финансово-экономического отдела, ведущий юрисконсульт, инженер-электроник, курьер;
- начальник отдела кадров является ответственным за обработку персональных данных на бумажных носителях;
- инженер-электроник является ответственным за обеспечение безопасности персональных данных в информационной системе.

4.1.2. Перечень должностных лиц, имеющих доступ к персональным данным работников в соответствующем объеме, определяется пунктами 4.1. и 4.1.1. данного Положения и может быть изменен или дополнен приказом художественного руководителя.

4.2. Внешний доступ.

4.2.1. К числу массовых потребителей персональных данных вне учреждения 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.

4.2.2. Надзорно-контрольные органы имеют доступ к информации только в сфере своей компетенции.

4.2.3. Организации, в которые работник может осуществлять перечисление денежных средств (страховые компании, негосударственные пенсионные фонды, благотворительные организации, кредитные учреждения), могут получить доступ к персональным данным работника только в случае его письменного разрешения.

4.2.4. Другие организации.

Сведения о работающем работнике или уже уволенном могут быть предоставлены другой организации только с письменного запроса на бланке организации, с приложением копии нотариально заверенного заявления работника.

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

В случае развода бывшая супруга (супруг) имеет право обратиться в учреждение с письменным запросом о размере заработной платы работника без его согласия (ТК РФ).

5. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. 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.

5.2. 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 не заинтересованные в возникновении угрозы лица.

5.3. 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 компании.

5.4. Защита персональных данных работника от неправомерного их использования или утраты обеспечивается учреждением за счёт его средств в порядке, установленном федеральным законом.

5.5. Внутренняя защита.

5.5.1. Основным виновником несанкционированного доступа к персональным данным является, как правило, персонал, работающий с документами и базами данных. Регламентация доступа персонала к конфиденциальным сведениям, документам и базам данных входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий между руководителями и специалистами

организации.

5.5.2. Для обеспечения внутренней 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 работников, при котором исключалось бы бесконтрольное использование защищаемой информации;
- знание работником требований нормативно-методических документов по защите информации и сохранению 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 требований разрешительной системы доступа работниками подразделения;
- воспитательная и разъяснительная работа с работниками подразделения по предупреждению утраты ценных сведений при работе с конфиденциальными документами;
- не допускается выдача личных дел работников на рабочие места руководителей. Личные дела могут выдаваться на рабочие места только Художественному руководителю, сотрудникам отдела кадров и в исключительных случаях, по письменному разрешению Художественного руководителя - руководителю структурного подразделения (например, при подготовке материалов для аттестации работника).

5.5.3. Защита персональных данных работника на электронных носителях.

В состав мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных с учетом актуальных угроз безопасности персональных данных и применяемых информационных технологий, входят:

- антивирусная защита,
- обеспечение доступности персональных данных,
- управление конфигурацией информационной системы и системы защиты персональных данных;
- учреждение обеспечивает режим безопасности помещений, в которых размещается информационная система;
- учреждение обеспечивает сохранность носителей информации;
- учреждение использует средства защиты информации, которые прошли оценку соответствия требованиям закона в области обеспечения безопасности информации.

Все папки, содержащие персональные данные работника, должны быть защищены паролем, который сообщается начальнику отдела кадров и руководителю (специалисту) службы, отвечающей за функционирование внутренней сети учреждения.

5.6. Внешняя защита.

5.6.1. Для защиты конфиденциальной информации создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лица, пытающегося 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.

5.6.2. Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности учреждения, посетители, работники других организационных структур. Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов в отделе кадров.

5.6.3. Для обеспечения внешней защиты персональных данных работников необходимо соблюдать ряд мер:

- соблюдать порядок приёма, учёта и контроля деятельности посетителей;
- вести учёт и порядок выдачи ключей от помещений, в том числе электронных;
- использовать технические средства охраны, сигнализации;
- соблюдать порядок охраны территории, зданий, помещений, транспортных средств;
- следовать требованиям к защите информации при интервьюировании и собеседованиях.

5.7. Все лица, связанные с получением, обработкой и защитой персональных данных, обязаны подписать обязательство о неразглашении информации, содержащей персональные данные сотрудников.

5.8. Работник любого подразделения независимо от занимаемой должности, не имеет права разглашать персональные данные других работников, ставшие ему известными в связи с исполнением трудовых обязанностей либо случайно.

5.9. По возможности, персональные данные обезличиваются.

5.10. Кроме мер защиты персональных данных, установленных законодательством, учреждение, работники и их представители могут вырабатывать совместные меры защиты персональных данных работников.

6. ОТВЕТСТВЕННОСТЬ ЗА РАЗГЛАШЕНИЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ, СВЯЗАННОЙ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ

6.1. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, привлекаются к дисциплинарной ответственности. К данным лицам могут быть применены следующие дисциплинарные взыскания:

а) замечание;

б) выговор;

в) увольнение по соответствующим основаниям.

6.2. За каждый дисциплинарный проступок может быть применено только одно дисциплинарное взыскание.

6.3. Копия приказа о применении к сотруднику дисциплинарного взыскания с указанием оснований его применения вручается работнику под расписку в течение пяти дней со дня издания приказа.

6.4. Если в течение года со дня применения дисциплинарного взыскания работник не будет подвергнут новому дисциплинарному взысканию, то он считается не имеющим дисциплинарного взыскания. Учреждение до истечения года со дня издания приказа о применении дисциплинарного взыскания, имеет право снять его с работника по собственной инициативе, по письменному заявлению работника или по ходатайству его непосредственного руководителя.

6.5. Лица, нарушившие неприкосновенность частной жизни, допустившие разглашение личной и семейной тайны, могут быть привлечены к уголовной ответственности.

6.6. Моральный вред, причиненный работнику вследствие нарушения правил обработки его персональных данных, подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных работником убытков.

Вина конкретного работника организации должна быть доказана.

Прошито, пронумеровано и скреплено
всего 9 **листа (ов)**

Художественный руководитель
ГБУК г. Москвы «Ведогонь-театр»

Курочкин П.В