ВЕДОГОНЬ - ТЕАТР

Государственное бюджетное учреждение культуры города Москвы
«Ведогонь-театр»

г. Москва

«СОГЛАСОВАНО»
Председатель профкома

_____Л.С. Гришина

«УТВЕРЖДАЮ»
Художественный руководитель

_____ П.В. Курочкин
«16» декабря 2022г.

ПОЛОЖЕНИЕ
о защите персональных данных

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 и обеспечения гарантии конфиденциальности сведений о работнике, предоставленных работодателю.

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» с учетом актуальных изменений.

1.3. Персональные данные являются конфиденциальной, строго охраняемой информацией. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении 50 лет срока хранения, если иное не определено законом.

В целях настоящего Положения под персональными данными понимается любая информация, прямо или косвенно относящаяся к субъекту персональных данных.

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

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

2. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. 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.

2.2. 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.

2.3. 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.

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

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

2.5. Внутренняя защита.

2.5.1. 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.

2.5.2. Для обеспечения внутренней защиты персональных данных работников в учреждении соблюдается 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).

2.5.3. 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, в учреждении входят:

- антивирусная защита,

- 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, защищены паролем, который известен начальнику отдела кадров и руководителю (специалисту) службы, отвечающей за функционирование внутренней сети учреждения.

2.6. Внешняя защита.

2.6.1. 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.

2.6.2. 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.

2.6.3. Для обеспечения внешней защиты персональных данных работников в учреждении принят ряд мер:

- соблюдается порядок приёма, учёта и контроля деятельности посетителей;

- ведется учёт и порядок выдачи ключей от помещений, в том числе электронных;

- используются технические средства охраны, сигнализации;
- соблюдается порядок охраны территории, зданий, помещений, транспортных средств;
- выполняются требования к защите информации при интервьюировании и собеседованиях.

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

2.8. 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.

2.9. По возможности, персональные данные обезличиваются.

2.10. В целях защиты персональных данных на бумажных носителях работодатель:

- приказом назначает ответственных за обработку персональных данных;
- ограничивает допуск в помещения, где хранятся документы, которые содержат персональные данные работников;
- хранит документы, содержащие персональные данные работников в шкафах, запирающихся на ключ;
- хранит трудовые книжки работников в сейфе в отделе кадров.

2.11. В целях обеспечения конфиденциальности документы, содержащие персональные данные работников, оформляются, ведутся и хранятся только работниками отдела кадров, бухгалтерии и службы охраны труда работодателя.

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

2.13. Передача информации, содержащей сведения о персональных данных работников, по телефону в связи с невозможностью идентификации лица, запрашивающего информацию, запрещается.

2.14. Все работники организации, осуществляющие обработку персональных данных, обязаны хранить тайну о сведениях, содержащих персональные данные, в соответствии с Положением, требованиями законодательства РФ.

2.15. Работник вправе требовать полную информацию о своих персональных данных, об их обработке, использовании и хранении.

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

3.1. 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.

Проверено, прошито, пронумеровано и скреплено
всего 4 **листа (ов)**

Художественный руководитель ГБУК г. Москвы «Ведогонь-театр»

_____ **Курочкин П.В.**