**Приложение №1**
к приказу №100 от 11.09.2026

**Правила, устанавливающие процедуры,
направленные на выявление и предотвращение нарушений законодательства
Российской Федерации в сфере персональных данных,
устранение последствий таких нарушений**

## 1. Общие положения

1.1. Настоящие правила, устанавливающие процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных (далее – Правила) разработаны на основании требований Трудового кодекса Российской Федерации, Федерального закона Российской Федерации от 27 июля 2006 №152-ФЗ «О персональных данных».

1.2. Целью Правил является определение процедур, направленных на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных в Государственном бюджетном учреждении Ивановской области «Ивановский государственный театральный комплекс» (далее – Организация, Оператор).

1.3. В настоящих Правилах используются основные понятия, определенные в статье 3 Федерального закона Российской Федерации от 27.07.2006 №152-ФЗ «О персональных данных».

## 2. Процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных

2.1. Обработка персональных данных должна осуществляться на законной и справедливой основе.

2.2. Организация устанавливает следующие процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных:

1) издание локальных актов Организации по вопросам обработки персональных данных;

2) назначение лица, ответственного за организацию обработки персональных данных;

3) определение лиц, уполномоченных на получение, обработку, хранение, передачу и любое другое использование персональных данных в Организации и несущих ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты этих персональных данных;

4) определение порядка доступа работников Организации в помещения, в которых ведется обработка персональных данных;

5) ознакомление работников Организации непосредственно осуществляющих обработку персональных данных под роспись до начала работы с положениями законодательства Российской Федерации о персональных данных, в том числе с требованиями к защите персональных данных, документами, определяющими политику Организации в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников;

6) получение персональных данных лично у субъекта персональных данных, в случае недееспособности субъекта персональных данных согласие на обработку его персональных данных дает законный представитель субъекта персональных данных, в случае возникновения необходимости получения персональных данных у третьей стороны Организация извещает об этом субъекта персональных данных заранее, получает его письменное согласие и сообщает ему о целях, предполагаемых источниках и способах получения персональных данных;

7) определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

8) применение правовых, организационных и технических мер по обеспечению безопасности персональных данных;

9) опубликование на официальном сайте Организации в информационно-телекоммуникационной сети Интернет документов, определяющих политику Организации в отношении обработки персональных данных, сведения о реализуемых требованиях к защите персональных данных;

10) при осуществлении сбора персональных данных с использованием информационно-телекоммуникационных сетей, опубликование в соответствующей информационно-телекоммуникационной сети, в том числе на страницах официального сайта Организации в информационно-телекоммуникационной сети Интернет, с использованием которой осуществляется сбор персональных данных, документа, определяющего политику Организации в отношении обработки персональных данных, и сведения о реализуемых требованиях к защите персональных данных, а также обеспечение возможности доступа к указанному документу с использованием средств соответствующей информационно-телекоммуникационной сети;

11) осуществление внутреннего контроля соответствия обработки персональных данных Федеральному закону Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных» и принятым в соответствии с ним локальным нормативным актам, требованиям к защите персональных данных, политике Оператора в отношении обработки персональных данных, локальным актам Организации;

12) оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных», соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных указанным Федеральным законом;

13) применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

14) оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

15) учет машинных носителей персональных данных;

16) обнаружение фактов несанкционированного доступа к персональным данным и принятием мер, в том числе мер по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные системы персональных данных и по реагированию на компьютерные инциденты в них;

17) установление правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

18) контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных;

19) обеспечение взаимодействия с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации;

20) обеспечение личной ответственности работников, осуществляющих обработку либо имеющих доступ к персональным данным;

21) организация рассмотрения запросов субъектов персональных данных или их представителей и ответов на такие запросы;

22) блокирование, внесение изменений и уничтожение персональных данных в предусмотренных действующим законодательством случаях;

23) оповещение субъектов персональных данных в предусмотренных действующим законодательством случаях;

24) разъяснение прав субъектам персональных данных в вопросах обработки и обеспечения безопасности персональных данных.

## 3. Процедуры, направленные на устранение последствий нарушений законодательства Российской Федерации в сфере персональных данных

3.1. Организация устанавливает следующие процедуры, направленные на устранение последствий нарушений законодательства Российской Федерации в сфере персональных данных:

1) прекращение неправомерной обработки персональных данных или обеспечение прекращения неправомерной обработки персональных данных лицом, действующим по поручению Организации, в случае выявления неправомерной обработки персональных данных, осуществляемой Организацией или лицом, действующим по поручению Организации, Организация, в срок, не превышающий трех рабочих дней с момента такого выявления;

2) в случае если обеспечить правомерность обработки персональных данных невозможно – уничтожение таких персональных данных или обеспечение их уничтожения, в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных;

3) уведомление субъекта персональных данных или его представителя об устранении допущенных нарушений или об уничтожении персональных данных, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанного органа;

4) в случае отсутствия возможности уничтожения персональных данных в течение установленного срока, Организация осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Организации) и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами;

5) уведомление о факте уничтожения субъекта персональных данных и, в случае если уничтожение произведено по запросу уполномоченного органа, указанного органа, после уничтожения персональных данных;

6) восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

7) информирование федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности, о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных;

8) уведомление уполномоченного органа по защите прав субъектов персональных данных в случае установления оператором, уполномоченным органом по защите прав субъектов персональных данных или иным заинтересованным лицом факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных:

- в течение двадцати четырех часов о произошедшем инциденте, о предполагаемых причинах, повлекших нарушение прав субъектов персональных данных, и предполагаемом вреде, нанесенном правам субъектов персональных данных, о принятых мерах по устранению последствий соответствующего инцидента, а также предоставить сведения о лице, уполномоченном оператором на взаимодействие с уполномоченным органом по защите прав субъектов персональных данных, по вопросам, связанным с выявленным инцидентом;

- в течение семидесяти двух часов о результатах внутреннего расследования выявленного инцидента, а также предоставить сведения о лицах, действия которых стали причиной выявленного инцидента (при наличии).

**4. Заключительные положения**

4.1. Настоящие Правила вступают в силу со дня их утверждения директором Организации.

4.2. В настоящие Правила могут вноситься изменения и дополнения, которые утверждаются и вводятся в действие приказом директора Организации.

4.3. В случае, если отдельные нормы настоящих Правил противоречат действующему законодательству Российской Федерации и/или Уставу Организации, они утрачивают силу и применяются соответствующие нормы законодательства Российской Федерации и/или Устава Организации. Недействительность отдельных норм настоящих Правил не влечет недействительности других норм и Правил в целом.

Ответственный за организацию
обработки персональных данных _____ / Чуркина С.Н.

«11» 09 20 26 года