Положение

об организации обработки, защиты и обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных Государственного бюджетного учреждения культуры «Самарская государственная филармония»

Утверждено и введено в действие Приказом № ____

от _____2012 г.

Самара 2012

СОДЕРЖАНИЕ

1 ВВЕДЕНИЕ

1.1 Настоящее «Положение о порядке обработки, защиты и обеспечении безопасности персональных данных при их обработки в информационных системах персональных данных (далее – «Положение») определяет порядок обработки, защиты и обеспечении безопасности персональных данных субъектов персональных данных в Государственном бюджетном учреждении культуры «Самарская государственная филармония» (далее – Учреждение).

1.2 Настоящее Положение разработано в соответствии с:

– Федеральным законом Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных»;

– Федеральным законом Российской Федерации от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– Трудовым кодексом Российской Федерации;

– Гражданским кодексом Российской Федерации;

– «Положением об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», утверждено постановлением Правительства РФ № 781;

– -«Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» утверждено постановлением Правительства РФ № 687.

1.3 Целью принятия данного Положения является определение такого порядка обработки персональных данных в Учреждении, при котором обеспечиваются все законные права и интересы субъектов персональных данных.

1.4 Положение обязательно для исполнения всеми лицами, Учреждения. Нарушение порядка обработки персональных данных, определённого Положением, влечёт материальную, дисциплинарную, гражданскую, административную и уголовную ответственность.

1.5 Все сотрудники Учреждения, должны быть ознакомлены с настоящим Положением под роспись.

1.6 Настоящее Положение вступает в силу после его утверждения директором Учреждения (далее- Директор) на основании Приказа Директора о введении в действие. Все изменения в Положение, вносятся на основании приказов о внесении изменений Директора в установленном порядке.

1.7 Положение не распространяется на обработку обезличенных персональных данных, а также персональных данных, сделанных общедоступными субъектом персональных данных.

1.8 Все персональные данные в Учреждении, за исключением обезличенных и сделанными общедоступными субъектом персональных данных, признаются информацией ограниченного доступа. Необходимость соблюдения конфиденциальности такой информации определена требованиями Федерального закона № 152-ФЗ «О персональных данных».

1.9 Защита и обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных Учреждения, а так же извлеченных из неё организуется в соответствии с требованиями Федеральных законов в этой сфере.

2 ОСНОВНЫЕ ПОНЯТИЯ

1.10 В настоящем Положении используются следующие основные понятия и определения:

Персональные данные (ПДн) - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту ПДн).

Оператор персональных данных - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку ПДн, а также определяющие цели обработки ПДн, состав ПДн, подлежащих обработке, действия (операции), совершаемые с ПДн.

Информационная система персональных данных (ИСПДн) - совокупность содержащихся в базах данных ПДн и обеспечивающих их обработку информационных технологий и технических средств.

Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с ПДн, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн.

Распространение персональных данных - действия, направленные на раскрытие ПДн неопределенному кругу лиц.

Предоставление персональных данных – действия, направленные на раскрытие ПДн определенному лицу или определенному кругу лиц.

Блокирование персональных данных – временное прекращение обработки ПДн (за исключением случаев, если обработка необходима для уточнения ПДн.

Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной

информации определить принадлежность ПДн конкретному субъекту ПДн.

Уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание ПДн в ИСПДн и (или) в результате которых уничтожаются материальные носители ПДн.

Трансграничная передача персональных данных - передача ПДн на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

Специальные категории персональных данных – ПДн, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни.

Биометрические персональные данные – сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность.

Персональные данные, сделанные общедоступными субъектом – персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом либо по его просьбе.

Автоматизированная обработка персональных данных – обработка ПДн с помощью средств вычислительной техники.

Неавтоматизированная обработка персональных данных (обработка ПД без использования средств автоматизации) – обработка ПДн, при которой такие действия с персональными данными, как использование, уточнение, распространение, уничтожение ПДн в отношении каждого субъекта ПДн осуществляются при непосредственном участии человека. Обработка ПДн не может

быть признана осуществляемой с использованием средств автоматизации только на том основании, что ПДн содержатся в ИСПДн, либо были извлечены из нее.

Правила обработки персональных данных в Учреждении:

1.11 Обработка ПДн осуществляется на основании принципов достаточности для достижения конкретных, заранее определенных и законных целей. Не допускается обработка ПДн, несовместимая с целями сбора ПДн.

1.12 Содержание и объем обрабатываемых ПДн должны соответствовать заявленным целям обработки. Перечень ПДн, обрабатываемых в Учреждении, категорий субъектов ПДн, цели их обработки определяются внутренним документом Учреждения.

1.13 Перечень ИСПДн, в которых осуществляется обработка ПДн, определяются внутренним документом Учреждения.

1.14 В Учреждении не допускается объединение баз данных, содержащих ПДн, обработка которых осуществляется в целях, несовместимых между собой.

1.15 В Учреждении отдельным приказом назначается лицо, ответственное за организацию обработки и обеспечение безопасности ПДн (далее – Ответственное лицо), в функции которого входят обязанности по:

– осуществлению внутреннего контроля за соблюдением Учреждением и его сотрудниками законодательства Российской Федерации о ПДн, в том числе требований к защите ПДн;

– определению перечня лиц, допущенных к обработке ПДн, помещений, в которых осуществляется обработка ПДн, перечня прав доступа пользователей к ИСПДн;

– доведению до сведения сотрудников Учреждения законодательства Российской Федерации о ПДн, локальных актов по вопросам обработки ПДн, требований к защите персональных данных;

– приему и обработке обращений и запросов субъектов ПДн или их представителей и (или) осуществлению контроля за приемом и обработкой таких обращений и запросов, а также по организации обучения указанных сотрудников;

– оценке соответствия содержания и объема обрабатываемых ПДн целям обработки ПДн;

– разработке документов, определяющих политику Учреждения в отношении обработки ПДн, локальных актов по вопросам обработки ПДн, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;

– организации и проведению мероприятий по внутреннему контролю и (или) аудиту соответствия обработки ПДн требованиям Федерального закона «О персональных данных» и принятым в соответствии с ним нормативным правовым актам;

– оценке вреда, который может быть причинен субъектам ПДн в случае нарушения требований Федерального закона «О персональных данных», соотношение указанного вреда и принимаемых Учреждением мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных»;

– определению угроз безопасности ПДн при их обработке в ИСПДн;

– оценке эффективности принимаемых Учреждением мер по обеспечению безопасности ПДн до ввода в эксплуатацию ИСПДн;

– установлению правил доступа сотрудников Учреждения к ПДн, обрабатываемым в ИСПДн;

– взаимодействию с уполномоченным органом по защите прав субъектов ПДн.

1.16 Ответственное лицо может формировать рабочую группу, состоящую из сотрудников Учреждения, на которых возлагается ответственность за реализацию решений Ответственного лица в области обработки, защиты и обеспечения безопасности ПДн. В состав рабочей группы должны входить представители подразделений, в которых обрабатываются ПДн, а также ответственный сотрудник цеха компьютерного обслуживания, на которого возложены обязанности по учету машинных носителей ПДн.

1.17 Решения об инициации новых процессов обработки ПДн или внесении изменений в существующие процессы обработки ПДн согласовываются Ответственным лицом.

1.18 Хранение ПДн в Учреждении осуществляется в форме, позволяющей определить субъекта, не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект. По достижении целей обработки или в случае утраты необходимости в достижении этих целей ПДн подлежат уничтожению либо обезличиванию, если иное не предусмотрено федеральным законом.

1.19 В Учреждении не обрабатываются специальные категории ПДн и биометрические ПДн. При возникновении необходимости их обработки должны выполняться требования, предусмотренные Федеральным законом №152-ФЗ «О персональных данных» для указанных категорий ПДн.

1.20 Обработка ПДн, признанных сотрудниками Учреждения общедоступными, осуществляется с их письменного согласия в целях подготовки служебного телефонного справочника, изготовления визиток, размещения на официальном сайте Учреждения, изготовления афиш (буклетов, иных рекламных материалов), магнитных пластиковых карт, предназначенных для установления личности субъекта и доступа на территорию юридического лица и исполнения возложенных функций на Учреждение. Форма согласия приводится в Приложении №1.

3 ПОРЯДОК ПРЕДОСТАВЛЕНИЯ ДОСТУПА СОТРУДНИКОВ К ПЕРСОНАЛЬНЫМ ДАННЫМ

4 ПОРЯДОК ВЗАИМОДЕЙСТВИЯ С ТРЕТЬИМИ ЛИЦАМИ ПРИ ПОЛУЧЕНИИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ПОРУЧЕНИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ И ПЕРЕДАЧЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ГОСУДАРСТВЕННЫМ ОРГАНАМ И ОРГАНИЗАЦИЯМ

1.21 Учреждение вправе обрабатывать ПДн, полученные не от самого субъекта. В этом случае Учреждение до начала обработки таких ПДн обязано предоставить этому субъекту ПДн следующую информацию:

- наименование и адрес оператора;
- цель обработки ПДн и ее правовое основание;
- предполагаемые пользователи ПДн;
- права субъекта ПДн, установленные Федеральным законом «О персональных данных»;
- источник получения ПДн.

1.22 Перечень третьих лиц, от которых Учреждение получает ПДн, перечень третьих лиц, которым Учреждение поручает обработку ПДн, а также перечень государственных органов и организаций, которым Учреждение передает (предоставляет) ПДн, утверждаются внутренним актом (документом) Учреждения.

1.23 Учреждение вправе не предоставлять субъекту ПДн информацию, указанную в п.4.1 Положения, если:

- Учреждению представлено подтверждение того, что субъект ПДн уведомлен об осуществлении обработки его ПДн Учреждением;
- ПДн получены Учреждением на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн;

– ПДн сделаны общедоступными субъектом или получены из общедоступного источника;

– Учреждение осуществляет обработку ПДн для статистических или иных исследовательских целей, для осуществления профессиональной деятельности журналиста либо научной, литературной или иной творческой деятельности, если при этом не нарушаются права и законные интересы субъекта ПДн;

– предоставление субъекту ПДн информации, указанной в п.4.1 Положения, нарушает права и законные интересы третьих лиц.

1.24 Учреждение на основании договора, государственного или муниципального контракта вправе поручить обработку ПДн сторонней организации (третьему лицу) с согласия субъекта ПДн, если иное не предусмотрено федеральным законом. При этом сторонняя организация обязана соблюдать принципы и правила обработки ПДн, предусмотренные Федеральным законом №152-ФЗ «О персональных данных».

1.25 В договоре (государственном или муниципальном контракте), на основании которого Учреждение поручает обработку ПДн сторонней организации (третьему лицу), должны быть определены:

1) перечень действий (операций) с ПДн, которые будут совершаться сторонней организацией,

2) цели обработки ПДн,

3) обязанность соблюдения конфиденциальности ПДн и обеспечения безопасности ПДн при их обработке,

4) требования к защите обрабатываемых ПДн в соответствии со статьей 19 Федерального закона «О персональных данных»,

5) положения, определяющие ответственность сторонней организации перед Учреждением.

1.26 При поручении обработки ПДн сторонней организации Учреждение обязуется выполнять предусмотренные Федеральным законом № 152-ФЗ «О персональных данных» условия обработки ПДн.

1.27 При выявлении Учреждением необходимости уточнения, блокирования и уничтожения ПДн, обработка которых поручена

сторонней организации, Ответственное лицо в течение 5 дней направляет в стороннюю организацию письменное требование совершить соответствующее действие с ПДн.

1.28 При поручении обработки ПДн сторонней организации, ответственность перед субъектами ПДн за действия указанной сторонней организации несет Учреждение.

1.29 Учреждение не вправе сообщать ПДн работников третьей стороне без их письменного согласия, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в других случаях, предусмотренных Трудовым кодексом РФ или иными федеральными законами. Передача (предоставление) ПДн государственным органам и организациям осуществляется в соответствии с требованиями нормативных правовых актов, устанавливающих обязанность такой передачи (предоставления).

1.30 Процедура ответа на письменные запросы других организаций и учреждений описана в «Регламенте обмена информацией, содержащей персональные данные, с третьими лицами и неопределенным кругом лиц».

1.31 Ответственность за соблюдение установленного в данном разделе Положения порядка взаимодействия с третьими лицами несут руководители (начальники) структурных подразделений, осуществляющих такое взаимодействие.

1.32 Процедуры обмена ПДн с третьими лицами и неопределенным кругом лиц, описаны в «Регламенте обмена информацией, содержащей персональные данные, с третьими лицами и неопределенным кругом лиц».

1.33 Процедура отправки документов, содержащих персональные данные, через организацию федеральной почтовой связи, описана в «Регламенте обмена информацией, содержащей персональные данные, с третьими лицами и неопределенным кругом лиц» и «Регламенте взаимодействия с субъектами ПДн».

5 ПОРЯДОК СБОРА, ХРАНЕНИЯ И УТОЧНЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

6 ПОРЯДОК ВЗАИМОДЕЙСТВИЯ С СУБЪЕКТАМИ ПЕРСОНАЛЬНЫХ ДАННЫХ

7 ПОРЯДОК УНИЧТОЖЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

1.34 Уничтожение ПДн осуществляется:

– по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом - в течение 30 дней;

– при предоставлении субъектом ПДн сведений, подтверждающих, что ПДн являются незаконно полученными или не являются необходимыми для заявленной цели обработки – в течение 7 дней;

– если невозможно обеспечить правомерность обработки ПДн – в течение 10 дней;

– в случае отзыва субъектом ПДн согласия на обработку ПДн, если сохранение персональных данных более не требуется для целей обработки ПДн – в течение 30 дней.

1.35 При невозможности уничтожения ПДн в сроки, определенные Федеральным законом №152-ФЗ «О персональных данных» для случаев, когда невозможно обеспечить правомерность обработки ПДн, при достижении целей обработки ПДн, а также при отзыве субъектом согласия на обработку ПДн, если сохранение ПДн более не требуется для целей обработки ПДн, Учреждение осуществляет блокирование ПДн и уничтожает ПДн в течение 6 месяцев, если иной срок не установлен федеральными законами.

1.36 Уничтожение ПДн должно производиться способом, исключающим возможность восстановления этих ПДн на носителе. Способ уничтожения персональных данных в ИСПДн должен быть реализован с помощью штатных средств.

1.37 Уничтожение носителей ПДн должно производиться комиссией, состав которой определяется руководителем Учреждения. Факт уничтожения носителя ПДн подтверждается «Актом об уничтожении персональных данных» (Приложение 2).

8 ОРГАНИЗАЦИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

9 ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ НОРМ, РЕГУЛИРУЮЩИХ ОБРАБОТКУ И ЗАЩИТУ ПЕРСОНАЛЬНЫХ ДАННЫХ СУБЪЕКТА

1.38 Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту ПДн, несут административную ответственность по ст.ст. 13.11, 13.14 Кодекса об административных правонарушениях РФ.

1.39 Предоставление ПДн посторонним лицам, в том числе, работникам Учреждения, не имеющим к ним доступа, распространение ПДн, утрата документов и иных материальных носителей, содержащих ПДн субъекта, а также нарушения, установленные настоящим Положением, внутренними нормативными актами (приказами, распоряжениями) Учреждения, влечет наложение на сотрудника, дисциплинарного взыскания: замечания, выговора или увольнения.

1.40 Сотрудник Учреждения, совершивший указанный дисциплинарный проступок, несет полную материальную ответственность в случае причинения его действиями ущерба Учреждению (п.7 ст. 243 Трудового кодекса РФ).

1.41 Сотрудники Учреждения, виновные в незаконном собирании или распространении ПДн, осуществившие неправомерный доступ к охраняемой законом компьютерной информации, несут уголовную ответственность в соответствии со ст.ст. 137, 272 Уголовного кодекса РФ.

1.42 Сотрудники Учреждения, виновные в незаконном собирании или распространении ПДн на бумажных носителях, несут уголовную ответственность в соответствии со ст.ст. 137, Уголовного кодекса РФ.