ПРИЛОЖЕНИЕ № 3

к приказу ГБУК ИЛМ «А.П. Чехов и Сахалин»

от 27.07.2022 г. №229

**ПРАВИЛА**

**осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и локальными актами ГБУК ИЛМ «А.П. Чехов и Сахалин»**

1. Настоящие Правила определяют процедуры в ГБУК ИЛМ «А.П. Чехов и Сахалин» (далее – музей), направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, основания, порядок, методы проведения внутреннего контроля соответствия обработки персональных данных субъектов персональных данных требованиям к защите персональных данных в музее.
2. В целях осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных музей осуществляет проведение плановых и внеплановых проверок условий обработки персональных данных (далее - проверки) на предмет соответствия Федеральному закону от 27.07.2006 № 152-ФЗ «О персональных данных» (далее - Федеральный закон № 152-ФЗ).
3. Проверки проводятся в музее на основании ежегодного плана или на основании поступившей музею информации о нарушении правил обработки персональных данных (внеплановые проверки). Ежегодный план проверок разрабатывается и утверждается комиссией музея по осуществлению внутреннего контроля соответствия обработки персональных данных требованиям, предусмотренным Федеральным законом № 152-ФЗ (далее - Комиссия).
4. В ежегодном плане проверок по каждой проверке устанавливается объект внутреннего контроля, проверяемый период, срок проведения проверки, ответственные исполнители.
5. Проверки проводятся Комиссией. В проведении проверки не может участвовать работник музея, прямо или косвенно заинтересованный в ее результатах.
6. Основанием для проведения внеплановой проверки является поступившее в музей письменное обращение субъекта персональных данных или его представителя о нарушении правил обработки персональных данных данного субъекта персональных данных.
7. Проведение внеплановой проверки организуется Комиссией в течение пяти рабочих дней со дня поступления обращения.
8. Срок проведения проверки не может превышать тридцати календарных дней со дня принятия решения о ее проведении.
9. Члены Комиссии, получившие доступ к персональным данным субъектов персональных данных в ходе проведения проверки, обеспечивают конфиденциальность персональных данных субъектов персональных данных, не раскрывают третьим лицам и не распространяют персональные данные без согласия субъекта персональных данных.
10. Проверки условий обработки персональных данных осуществляются непосредственно на месте обработки персональных данных путем опроса либо, при необходимости, путем осмотра служебных мест работников музея, участвующих в процессе обработки персональных данных.
11. При проведении проверки условий обработки персональных данных должны быть полностью, объективно и всесторонне установлены:
    1. Порядок и условия применения организационных и технических мер, необходимых для выполнения требований к защите персональных данных;
    2. Порядок и условия соблюдения парольной защиты;
    3. Порядок и условия соблюдения антивирусной защиты;
    4. Порядок и условия обеспечения резервного копирования;
    5. Эффективность принимаемых мер по обеспечению безопасности персональных данных до их ввода в информационную систему персональных данных;
    6. Условия соблюдения режима защиты при подключении к сетям общего пользования и (или) международного обмена;
    7. Порядок и условия обновления программного обеспечения и единообразия применяемого программного обеспечения на всех элементах информационной системы персональных данных;
    8. Порядок и условия применения средств защиты информации;
    9. Состояние учета носителей персональных данных;
    10. Соблюдение правил доступа к персональным данным;
    11. Соблюдение порядка доступа в помещения, в которых ведется обработка персональных данных;
    12. Наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер;
    13. Мероприятия по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.
12. По результатам каждой проверки Комиссией проводится заседание. Решения, принятые на заседаниях Комиссии, оформляются протоколом и предоставляется директору музея с указанием мер, необходимых для устранения выявленных нарушений.
13. По существу, поставленных в обращении (жалобе) вопросов, Комиссия в течение пяти рабочих дней со дня окончания проверки дает письменный ответ заявителю.