

ДЕПАРТАМЕНТ КУЛЬТУРЫ ГОРОДА МОСКВЫ

Государственное бюджетное учреждение культуры города Москвы
«Государственный музей Владимира Высоцкого»

П Р И К А З

9 декабря 2022 г.

№ 153

**О создании комиссии по внутреннему контролю соответствия
обработки персональных данных требованиям к защите персональных
данных**

В целях осуществления внутреннего контроля соответствия обработки персональных данных в Государственном бюджетном учреждении культуры города Москвы "Государственный музей Владимира Высоцкого" требованиям, установленным Федеральным законом от 27 июля 2006 г. №152-ФЗ "О персональных данных", и принятым в соответствии с ним нормативным правовым актам Российской Федерации, города Москвы и локальным нормативным актам **приказываю:**

1. Создать комиссию по внутреннему контролю соответствия обработки персональных данных требованиям к защите персональных данных, утвердив ее состав согласно Приложению 1 к настоящему приказу.

2. Утвердить Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных согласно Приложению 2 к настоящему приказу.

3. Контроль за исполнением настоящего приказа оставляю за собой.

Директор



Высоцкий Н.В.

С приказом ознакомлены:



Приложение 1
к приказу ГБУК г. Москвы
"Государственный музей Владимира
Высоцкого"
от 9 декабря 2022 г. № 153

СОСТАВ КОМИССИИ

**по внутреннему контролю соответствия обработки персональных
данных требованиям к защите персональных данных**

Председатель Комиссии:	заместитель директора Лапунова Людмила Петровна
Заместитель председателя Комиссии:	заместитель директора Бакановский Максим Георгиевич
Члены Комиссии:	главный бухгалтер Селина Людмила Юрьевна
	начальник отдела кадров Островская Ирина Александровна
	контрактный управляющий Шинина Наталья Леонидовна

ПРАВИЛА

осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

1. Общие положения

1.1. Настоящие Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее – Правила) устанавливают основания, порядок и формы проведения внутреннего контроля соответствия обработки и защиты персональных данных требованиям, установленным Федеральным законом от 27 июля 2006 г. №152-ФЗ "О персональных данных", принятым в соответствии с ним нормативным, правовым актам Российской Федерации и города Москвы и локальным нормативным актам Государственного бюджетного учреждения культуры города Москвы "Государственный музей Владимира Высоцкого". Настоящие Правила разработаны в соответствии с законодательством Российской Федерации и города Москвы в области обработки и защиты персональных данных и иными правовыми актами, принимаемыми в соответствии с данным законодательством (далее – законодательство в сфере персональных данных).

1.2. Целями осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее – внутренний контроль) являются:

- оценка выполнения в Учреждении требований по обработке и защите персональных данных, установленных законодательством Российской Федерации, Правительства Москвы, а также локальными нормативными актами Учреждения;
- выявление и предотвращение в Учреждении нарушений законодательства Российской Федерации и города Москвы в сфере персональных данных.

1.3. Внутренний контроль проводится комиссией, назначаемой приказом Учреждения (далее – Комиссия).

1.4. В состав Комиссии могут входить работники Учреждения и внешние эксперты. В проведении внутреннего контроля не могут участвовать работники Учреждения, прямо или косвенно заинтересованные в его результатах.

1.5. Члены Комиссии, получившие доступ к персональным данным в ходе проведения внутреннего контроля, обеспечивают конфиденциальность персональных данных их субъектов.

1.6. В настоящих Правилах используются основные понятия, определенные в статье 3 Федерального закона от 27 июля 2006 г. №152-ФЗ "О персональных данных".

2. Порядок осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

2.1. Внутренний контроль осуществляется Учреждением путем проведения проверок соблюдения требований законодательства в сфере персональных данных и внутренних документов Учреждения по обработке и защите персональных данных (далее – проверки).

2.2. Проверки проводятся непосредственно на месте обработки персональных данных путем:

- опроса либо (при необходимости) осмотра рабочих мест работников, участвующих в процессе обработки персональных данных;
- проверки документов, относящихся к деятельности структурного подразделения в части обработки и (или) защиты персональных данных;
- проведения (при необходимости) инструментальных проверок защищенности информационных систем персональных данных.

2.3. Проверки в Учреждении разделяются на:

- плановые;
- внеплановые.

2.4. Плановые проверки проводятся не реже одного раза в год в соответствии с Планом проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее – План внутреннего контроля).

План внутреннего контроля разрабатывается лицом, назначенным ответственным за организацию обработки персональных данных, либо по его поручению. Разработанный План разрабатывается и утверждается ежегодно. План внутреннего контроля утверждается в порядке, установленном в Учреждении.

2.5. Количество плановых проверок зависит от:

- результатов проведения предыдущих проверок;
- критичности объекта (структурного подразделения, осуществляющего обработку и (или) защиту персональных данных, или процесса обработки персональных данных), по которому планируется проведение проверки;
- предложений руководства и специалистов структурных подразделений Учреждения.

2.6. Внеплановые внутренние проверки могут проводиться в следующих случаях:

- по результатам расследования выявленных нарушений требований законодательства в сфере персональных данных;
- по результатам внешних контрольных мероприятий, проводимых уполномоченным органом по защите прав субъектов персональных данных;
- при существенных изменениях процессов или процедур обработки и защиты персональных данных;
- при выявлении большого числа нарушений требований законодательства в сфере персональных данных или повторяемости одних и тех же нарушений от проверки к проверке;
- по указанию руководства Учреждения.

2.7. Руководители проверяемых структурных подразделений к началу проведения проверок должны обеспечить доступность:

- необходимых для проведения проверок работников;
- необходимых для проведения проверок материалов;
- помещений, относящиеся к области проведения проверок.

2.8. Результат проведения внутреннего контроля фиксируется в Отчете по результатам проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее по тексту – Отчет).

2.9. В Отчете должны быть указаны:

- основание проверки;
- вид проверки (плановая/внеплановая);

- цель проведения проверки;
- выявленные нарушения.

2.10. Отчет подписывают члены Комиссии и председатель.

2.11. По результатам проведения внутреннего контроля Комиссией проводится анализ выявленных нарушений и разрабатывается план действий по устранению выявленных нарушений.

2.12. Результаты проведения внутреннего контроля и план действий по устранению выявленных нарушений доводятся до сведения руководства Учреждения для принятия решений о необходимости проведения работ по устранению выявленных нарушений.

2.13. Решения о необходимости проведения работ по устранению выявленных нарушений подлежат реализации в порядке, установленном в Учреждении.

2.14. В целях контроля устранения выявленных нарушений Комиссия может проводить повторные проверки.

3. Права Комиссии

3.1. Для реализации своих полномочий Комиссия имеет право:

- привлекать к проведению проверок работников Учреждения;
- запрашивать у работников Учреждения необходимую информацию;
- принимать меры по устранению выявленных нарушений;
- вносить предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке;
- вносить предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в сфере персональных данных.

3.2. К проведению проверок могут привлекаться третьи лица на договорной основе в соответствии с действующим законодательством.
