Приложение № 15

Утверждено

приказом государственной

инспекции по охране объектов

культурного наследия

Новосибирской области

от \_\_\_\_\_\_\_\_ 2023 г. № \_\_\_

Правила

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

1. Настоящими Правилами определяются процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных; основания, порядок, формы и методы проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.

2. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям в государственной инспекции по охране объектов культурного наследия Новосибирской области (далее – ГИО ОКН НСО) проводятся периодические проверки условий обработки персональных данных.

3. Проверки осуществляются лицом, ответственным за организацию обработки персональных данных в ГИО ОКН НСО.

4. Проверки соответствия обработки персональных данных установленным требованиям проводятся на основании утвержденного руководством ГИО ОКН НСО ежегодного плана осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям или на основании поступившего в ГИО ОКН НСО письменного заявления о нарушениях правил обработки персональных данных (внеплановые проверки).

Проведение внеплановой проверки организуется в течение трех рабочих дней с момента поступления соответствующего заявления.

5. При проведении проверки соответствия порядка обработки персональных данных установленным требованиям должны быть полностью, объективно и всесторонне установлены:

1) порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке;

2) порядок и условия применения средств защиты информации;

3) эффективность принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

4) состояние учета машинных носителей;

5) соблюдение правил обработки персональных данных в ГИО ОКН НСО;

6) наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых 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;

7) мероприятия по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

8) осуществление мероприятий по обеспечению целостности персональных данных.

9) соответствие информационной системы, обрабатывающей персональные данные, эксплуатационной, проектной и аттестационной документации.

6. Лицо, ответственное за организацию обработки персональных данных в ГИО ОКН НСО при проведении проверки соответствия обработки персональных данных имеет право:

1) запрашивать у работников ГИО ОКН НСО информацию, необходимую для реализации полномочий;

2) требовать от уполномоченных на обработку персональных данных лиц уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;

3) принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства Российской Федерации;

4) вносить руководству ГИО ОКН НСО предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке;

5) вносить руководству ГИО ОКН НСО предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в отношении обработки персональных данных.

7. В отношении персональных данных, ставших известными лицу, ответственному за организацию обработки персональных данных при проведении проверки соответствия обработки персональных данных в ходе проведения мероприятий внутреннего контроля, должна обеспечиваться конфиденциальность.

8. Своевременность и правильность проведения проверки контролируется ответственным за организацию обработки персональных данных.

9. Проверка должна быть завершена не позднее чем через 30 календарных дней со дня принятия решения о её проведении.

О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, руководству ГИО ОКН НСО докладывает ответственный за организацию обработки персональных данных в форме письменного заключения (докладной записки).