Приложение 14  
к приказу  
(наименование организации)

от «\_\_\_»\_\_\_\_\_\_.20\_\_\_ №\_\_\_\_

**ПРАВИЛА**

**осуществления внутреннего контроля соответствия обработки персональных данных в подсистеме «Параграф» объектового уровня государственной информационной системы Санкт-Петербурга «Комплексная автоматизированная информационная система каталогизации ресурсов образования Санкт-Петербурга» требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных»**

Настоящими правилами осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее – Правила) определяются процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации при обработке персональных данных в подсистеме «Параграф» объектового уровня государственной информационной системы Санкт-Петербурга «Комплексная автоматизированная информационная система каталогизации ресурсов образования Санкт-Петербурга» (далее –КАИС КРО «Параграф»), основания, порядок, формы и методы проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в КАИС КРО «Параграф».

Настоящие правила разработаны в соответствии Федеральным законом 27.07.2006 № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации», Постановлением Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

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

В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям к защите персональных данных в КАИС КРО «Параграф» необходимо проводить периодические проверки условий обработки персональных данных.

Проверки осуществляются ответственным за организацию обработки персональных данных в КАИС КРО (наименование организации). В проведении проверки не может участвовать работник, прямо или косвенно заинтересованный в её результатах.

Проверки соответствия обработки персональных данных установленным требованиям к защите персональных данных в КАИС КРО «Параграф», проводятся на основании утвержденного ежегодного плана осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям к защите персональных данных или на основании поступившего в (наименование организации) письменного заявления о нарушениях правил обработки персональных данных (внеплановые проверки).

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

При проведении проверки соответствия обработки персональных данных установленным требованиям к защите персональных данных должны быть полностью, объективно и всесторонне установлены:

* порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленный уровень защищенности персональных данных КАИС КРО «Параграф»;
* порядок и условия применения средств защиты информации;
* эффективность принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
* состояние учета машинных носителей персональных данных;
* соблюдение правил доступа к персональным данным;
* наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер;
* мероприятия по восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
* осуществление мероприятий по обеспечению целостности персональных данных.

Ответственный за организацию обработки персональных данных в КАИС КРО или в (наименование организации) имеет право:

* запрашивать у сотрудников (наименование организации) информацию, необходимую для реализации полномочий;
* требовать от сотрудников (наименование организации), осуществляющих обработку персональных данных, уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;
* принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства Российской Федерации;
* вносить предложения директору (наименование организации) о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке;
* вносить предложения директору (наименование организации) о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в отношении обработки персональных данных.

В отношении персональных данных, ставших известными ответственному за организацию обработки персональных данных в КАИС КРО «Параграф» (или комиссии) в ходе проведения мероприятий внутреннего контроля, должна обеспечиваться конфиденциальность персональных данных.

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

О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, докладывает директору (наименование организации) ответственный за организацию обработки персональных данных, либо председатель комиссии в форме акта.

Контроль за своевременностью и правильностью проведения проверки возлагается на заместителя директора по информационной безопасности.