Приложение 3

к Политике МКОУ ЗАТО
Знаменск Гимназия № 231 в отношении обработки
персональных данных

Правила
осуществления внутреннего контроля за соответствием обработки персональных данных требованиям к защите персональных данных в МКОУ ЗАТО Знаменск Гимназия № 231

I. Общие положения

1. Настоящие Правила осуществления внутреннего контроля за соответствием обработки персональных данных требованиям к защите персональных данных в МКОУ ЗАТО Знаменск Гимназия № 231 (далее – Правила) разработаны в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – № 152-ФЗ), 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».

2. Правила определяют процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в области персональных данных (далее – ПДн), основания, порядок, формы и методы проведения внутреннего контроля соответствия обработки ПДн требованиям к защите ПДн в МКОУ ЗАТО Знаменск Гимназия № 231 (далее – учреждение).

3. В Правилах используются основные понятия, определенные в статье 3 № 152-ФЗ.

II. Порядок проведения внутренних проверок

4. В соответствии с требованиями пп.4 п.1 ст. 18.1 № 152-ФЗ, а также в целях осуществления внутреннего контроля соответствия обработки ПДн требованиям к защите ПДн в учреждения проводятся периодические внутренние проверки условий обработки ПДн (далее – проверки).

5. Проверки проводятся в соответствии с приказом директора МКОУ ЗАТО Знаменск Гимназия № 231.

6. Проверки организуются лицом, ответственным за организацию обработки ПДн, и осуществляются комиссией по проведению внутренней проверки условий обработки ПДн в учреждения (далее – комиссия), состав которой утверждается приказом директора учреждения.

7. Проверки проводятся непосредственно на месте обработки ПДн путем опроса либо, при необходимости, путем осмотра рабочих мест сотрудников, участвующих в процессе обработки ПДн.

8. Лицо, ответственное за организацию обработки ПДн, и комиссия имеет право:

- запрашивать у сотрудников информацию, необходимую для реализации полномочий;
- требовать от сотрудников, осуществляющих обработку ПДн, уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем ПДн;
- вносить директору учреждения предложения о:

а) совершенствовании правового, технического и организационного обеспечения обработки ПДн;

б) приостановлении или прекращении обработки ПДн, осуществляемой с нарушением требований законодательства Российской Федерации;

в) привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в области ПДн.

9. Лицо, ответственное за организацию обработки ПДн, и члены комиссии обеспечивают конфиденциальность ПДн, ставших им известными в ходе проведения мероприятий внутреннего контроля.

10. Проверка должна быть завершена не позднее чем через тридцать календарных дней с даты издания приказа директора учреждения о создании комиссии.

11. По результатам проверки составляется акт проведения внутренней проверки условий обработки персональных данных в учреждении, согласно приложению к настоящим Правилам. Акт подписывается членами комиссии и утверждается директором учреждения.

12. При выявлении в ходе проверки нарушений в акте делается запись о мероприятиях по устранению нарушений и сроках исполнения.

III. Исследуемые вопросы в рамках проверки

13. В ходе проверки могут быть исследованы следующие вопросы:

1) Общие вопросы:

- соответствие нормативных правовых и иных актов учреждения, регламентирующих меры по обеспечению безопасности ПДн, требованиям законодательства Российской Федерации;
- опубликование документа, определяющего политику учреждения в отношении обработки ПДн, на официальном сайте МКОУ ЗАТО Знаменск Гимназия № 231 в информационно-телекоммуникационной сети «Интернет»;
- наличие согласий на обработку ПДн сотрудников учреждения;
- наличие обязательств сотрудников учреждения в случае расторжения с ними трудового договора (контракта) прекратить обработку ПДн, ставших известными им в связи с исполнением должностных обязанностей;
- ознакомление сотрудников учреждения с нормативными правовыми и иными актами учреждения, регламентирующими меры по обеспечению безопасности ПДн;
- отсутствие фактов несанкционированного доступа к ПДн.

2) Обработка ПДн с использованием средств автоматизации:

- соответствие полномочий пользователя информационных систем ПДн (далее – ИСПДн) учреждения правилам доступа;
- соблюдение пользователями ИСПДн учреждения парольной политики;
- соблюдение пользователями ИСПДн учреждения антивирусной политики;
- соблюдение пользователями ИСПДн учреждения правил работы со съемными носителями ПДн;
- соблюдение порядка доступа в помещения учреждения, в которых расположены элементы ИСПДн;
- соблюдение порядка резервирования баз данных и хранения резервных копий;
- соблюдение порядка работы со средствами защиты информации;
- знание пользователей ИСПДн о своих действиях во внештатных ситуациях.

3) Обработка ПДн без использования средств автоматизации:

- организация хранения бумажных носителей с ПДн;
- соблюдение порядка доступа к бумажным носителям с ПДн;
- соблюдение порядка доступа в помещения, в которых обрабатываются и хранятся бумажные носители с ПДн.

14. Вопросы, исследуемые в рамках проверки, приведенные в Правилах, могут изменяться и дополняться без необходимости внесения изменений в Правила.

Борзых Наталья Алексеевна

Подписан цифровой подписью: Борзых Наталья Алексеевна
DN: C=RU, OU=директор, O=МКОУ ЗАТО Знаменск Гимназия №231, CN=Борзых Наталья Алексеевна, E=gymn213@mail.ru
Основание: Я являюсь автором этого документа
Расположение: Российская Федерация,Астраханская область, г.Знаменск, ул.Волгоградская 12а
Дата: 2022.09.13 20:30:13 +04'00'