УТВЕРЖДАЮ
_____ М.Х. Исапаева
«03» 03 2020 г.

ПРАВИЛА
осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в МБУ ДО «ДДТ Ленинского района г.Грозного»

I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящие Правила разработаны в соответствии со ст.18 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных».

II. УСЛОВИЯ ОСУЩЕСТВЛЕНИЯ ВНУТРЕННЕГО КОНТРОЛЯ

2.1. В целях осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в МБУ ДО «ДДТ Ленинского района г.Грозного» организовывается проведение периодических проверок условий обработки персональных данных (далее - проверки).

2.2. Проверки осуществляются должностным лицом, ответственным за организацию обработки персональных данных в МБУ ДО «ДДТ Ленинского района г.Грозного» (далее - ответственный за организацию обработки персональных данных), либо комиссией, образуемой приказом по МБУ ДО «ДДТ Ленинского района г.Грозного».

2.3. В проведении проверки не может участвовать сотрудник МБУ ДО «ДДТ Ленинского района г.Грозного».

2.4. прямо или косвенно заинтересованный в её результатах.

2.5. Проверки проводятся на основании утвержденного в МБУ ДО «ДДТ Ленинского района г.Грозного». Плана осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям к защите персональных данных (плановые проверки) или на основании поступившего в МБУ ДО «ДДТ Ленинского района г.Грозного». письменного заявления о нарушениях правил обработки персональных данных (внеплановые проверки) (Приложение 1)

2.6. Плановые контрольные мероприятия проводятся постоянной комиссией периодически в соответствии с утвержденным Планом проведения контрольных мероприятий (далее – План, приложение 1) и направлены на постоянное совершенствование системы защиты персональных данных ИСПДн.

2.7. Плановые проверки проводятся не чаще чем один раз в полгода.

2.8. Проведение внеплановой проверки организуется в течение трех рабочих дней.

2.9. Внеплановые контрольные мероприятия проводятся на основании решения комиссии по информационной безопасности (создается на период проведения мероприятий). Решение о проведении плановых контрольных мероприятий может быть принято в следующих случаях

- по результатам расследования инцидента информационной безопасности;
- по результатам внешних контрольных мероприятий, проводимых регулирующими органами;
- по решению руководителя образовательного учреждения.

2.10. При проведении проверки должны быть полностью, объективно и всесторонне установлены:

2.10.1. 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 установленные уровни защищенности персональных данных;

2.10.2. порядок и условия применения средств защиты информации;

2.10.3. эффективность принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

2.10.4. состояние учета машинных носителей персональных данных;

2.10.5. соблюдение правил доступа к персональным данным;

2.10.6. наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер;

2.10.7. мероприятия по восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

2.10.8. осуществление мероприятий по обеспечению целостности персональных данных.

2.11. Ответственный за организацию обработки персональных данных в МБУ ДО «ДДТ Ленинского района г.Грозного» или комиссия имеет право:

2.11.1. запрашивать у сотрудников в МБУ ДО «ДДТ Ленинского района г.Грозного» информацию, необходимую для реализации полномочий;

2.11.2. требовать от уполномоченных на обработку персональных данных должностных лиц в МБУ ДО «ДДТ Ленинского района г.Грозного». уточнения, блокирования или уничтожения недостоверных, или полученных незаконным путем персональных данных;

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

2.11.4. вносить предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке;

2.11.5. вносить предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в отношении обработки персональных данных.

2.12. В отношении персональных данных, ставших известными ответственному за организацию обработки персональных данных, либо комиссии в ходе проведения мероприятий внутреннего контроля, должна обеспечиваться конфиденциальность персональных данных.

2.13. По результатам проведения проверки оформляется Акт проверки (приложение 2), результаты проверок фиксируются в журнале (приложение 4).

2.14. Акт подписывается ответственным за организацию обработки персональных данных или членами комиссии.

2.15. При выявлении нарушений в сфере защиты персональных данных составляется акт (приложение 3), выявленные нарушения фиксируются в журнале (приложение 4).

2.16. Срок проведения проверки и оформления акта составляет 30 календарных дней со дня начала проверки, указанного в правовом акте о назначении проверки.

2.17. О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, докладывает ответственный за организацию обработки персональных данных либо председатель комиссии, в форме письменного заключения.

2.18. Лицо, ответственное за обеспечение безопасности ПДн, не позднее чем за три рабочих дня до начала проведения контрольных мероприятий должно быть уведомлено о проведении проверки и ознакомлено с Планом проведения контрольных мероприятий. При проведении внеплановых контрольных мероприятий уведомление не требуется