

ПРАВИЛА

осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных», принятыми в соответствии с ним правовыми актами государственного бюджетного учреждения Ставропольского края «Спортивная школа олимпийского резерва по художественной гимнастике»

1. Общие положения

1.1. Настоящие Правила разработаны в соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ), постановлением Правительства Российской Федерации от 21 марта 2012 года № 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» и определяют процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, основания и порядок проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом № 152-ФЗ, принятыми в соответствии с ним правовыми актами государственного бюджетного учреждения Ставропольского края «Спортивная школа олимпийского резерва по художественной гимнастике» (далее – внутренний контроль соответствия обработки персональных данных требованиям к защите персональных данных).

2. Условия осуществления внутреннего контроля

2.1. В целях осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в государственном бюджетном учреждении Ставропольского края «Спортивная школа олимпийского резерва по художественной гимнастике» (далее – Учреждение) организовывается проведение периодических проверок условий обработки персональных данных (далее – проверки).

2.2. Проверки осуществляются должностным лицом, ответственным за организацию обработки персональных данных в Учреждении (далее – ответственный за организацию обработки персональных данных), либо комиссией, образуемой правовым актом Учреждения.

2.3. В проведении проверки не может участвовать сотрудник Учреждения прямо или косвенно заинтересованный в её результатах.

2.4. Проверки проводятся на основании утвержденного Учреждением ежегодного Плана осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям к защите персональных данных (плановые проверки) или на основании поступившего в Учреждение письменного заявления о нарушениях правил обработки персональных данных (внеплановые проверки).

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

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

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

2.7.1. 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;

2.7.2. порядок и условия применения средств защиты информации;

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

2.7.4. состояние учета машинных носителей персональных данных;

2.7.5. соблюдение правил доступа к персональным данным;

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

2.7.7. мероприятия по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

2.7.8. осуществление мероприятий по обеспечению целостности персональных данных.

2.8. Ответственный за организацию обработки персональных данных в Учреждении или комиссия имеет право:

2.8.1. запрашивать у работников Учреждения информацию, необходимую для реализации полномочий;

2.8.2. требовать от уполномоченных на обработку персональных данных должностных лиц Учреждения уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;

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

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

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

2.9. 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.

2.10. По результатам проведения проверки оформляется акт проверки, который подписывается ответственным за организацию обработки персональных данных или членами комиссии.

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

2.12. 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.