УТВЕРЖДАЮ
Директор Государственного бюджетного учреждения города Москвы «Центр физической культуры и спорта Западного административного округа города Москвы» Департамента спорта и туризма города Москвы

_____ 2018 г.

_____ /В.М. Цеханович/

ПРАВИЛА
осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом от 27 июля 2006г. №152-ФЗ «О персональных данных», принятыми в соответствии с ним нормативными, правовыми актами Российской Федерации, города Москвы и Государственного бюджетного учреждения города Москвы «Центр физической культуры и спорта Западного административного округа города Москвы» Департамента спорта и туризма города Москвы

1 Общие положения

1.1. Настоящие Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом от 27 июля 2006г. №152-ФЗ «О персональных данных», принятыми в соответствии с ним нормативными, правовыми актами Российской Федерации, города Москвы и Государственного бюджетного учреждения города Москвы «Центр физической культуры и спорта Западного административного округа города Москвы» Департамента спорта и туризма города Москвы (далее – Правила) устанавливают правила, порядок и формы проведения внутреннего контроля соответствия обработки и защиты персональных данных требованиям, установленным в ГБУ «ЦФКиС ЗАО г. Москвы» Москомспорта.

1.2. Целями осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее – внутренний контроль) является:

- оценка выполнения в ГБУ «ЦФКиС ЗАО г. Москвы» Москомспорта требований по обработке и защите персональных данных, установленных законодательством Российской Федерации, Правительства Москвы, а также правовыми актами ГБУ «ЦФКиС ЗАО г. Москвы» Москомспорта;
- выявление и предотвращение в ГБУ «ЦФКиС ЗАО г. Москвы» Москомспорта нарушений законодательства Российской Федерации и города Москвы в сфере персональных данных.

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

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

2.1. Внутренний контроль осуществляется ГБУ «ЦФКиС ЗАО г. Москвы» Москомспорта путем проведения проверок соблюдения требований законодательства Российской Федерации, города Москвы в области обработки и защиты персональных данных (далее по тексту – проверки).

2.2. Внутренний контроль в учреждении осуществляется на плановой основе, а также при необходимости – внепланово.

2.3. Внутренний контроль (как плановый, так и внеплановый) проводится комиссией, состав которой определяется приказом директора учреждения (далее – Комиссия).

2.4. В состав Комиссии могут входить работники учреждения, косвенно незаинтересованные в результатах проверки и внешние эксперты.

2.5. Члены Комиссии, получившие доступ к персональным данным субъектов персональных данных в ходе проведения внутреннего контроля, обязаны обеспечивать конфиденциальность персональных данных субъектов персональных данных.

2.6. Плановые проверки проводятся не реже одного раза в год в соответствии с Планом проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее – План проведения внутреннего контроля).

2.7. План проведения внутреннего контроля разрабатывается ответственным за организацию обработки персональных данных, либо по его поручению. Разработанный План проведения внутреннего контроля утверждается директором ГБУ «ЦФКиС ЗАО г. Москвы» Москомспорта.

2.8. Количество плановых проверок зависит от:

– результатов проведения предыдущих проверок;

– статуса и важности объекта (структурного подразделения, осуществляющего обработку и (или) защиту персональных данных или процесса обработки персональных данных), по которому планируется проведение проверки;

– предложений руководства и специалистов структурных подразделений.

2.9. Внеплановые внутренние проверки могут быть инициированы ответственным за организацию обработки персональных данных в следующих случаях:

– по указанию директора учреждения;

– при существенных изменениях организационной структуры ГБУ «ЦФКиС ЗАО г. Москвы» Москомспорта, процессов или процедур обработки и защиты персональных данных;

– по результатам расследования выявленных нарушений требований законодательства Российской Федерации, города Москвы и ГБУ «ЦФКиС ЗАО г. Москвы» Москомспорта в области обработки и защиты персональных данных;

– при выявлении большого числа нарушений требований законодательства Российской Федерации, города Москвы и ГБУ «ЦФКиС ЗАО г. Москвы» Москомспорта в области обработки и защиты персональных данных или повторяемости одних и тех же нарушений от проверки к проверке;

– по результатам внешних контрольных мероприятий, проводимых уполномоченным органом по защите прав субъектов персональных данных.

2.10. Основными способами проведения внутреннего контроля являются:

– проверка соблюдения работниками ГБУ «ЦФКиС ЗАО г. Москвы» Москомспорта правил обработки и защиты персональных данных;

– устный опрос работников;

– проверка документов, относящихся к деятельности структурного подразделения в части обработки и (или) защиты персональных данных, или возникающих в проверяемых процессах обработки персональных данных;

– инструментальные проверки защищенности информационных систем персональных данных;

– любая комбинация из перечисленного выше.

2.11. Руководители проверяемых структурных подразделений к началу проведения проверок должны обеспечить:

– доступность необходимых для проведения проверок работников;

– доступность необходимых для проведения проверок материалов;

– доступ к информационным ресурсам, владельцами которых они являются;

– доступ в помещения, имеющие отношения к области проведения проверок.

2.12. Примерный перечень возможных проверок в ходе внутреннего контроля приведен в приложении к настоящим Правилам (Приложение 1).

2.13. Результат проведения внутреннего контроля фиксируются в Отчете по результатам проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее по тексту – Отчет). В Отчете должны быть указаны как минимум:

– основание проверки;

– вид проверки (плановая/внеплановая);

– цель проведения проверки;

– выявленные нарушения.

2.14. Отчет подписывают члены Комиссии, председатель Комиссии.

2.15. По результатам проведения внутреннего контроля Комиссией проводится анализ выявленных нарушений и разрабатывается план действий по устранению выявленных нарушений.

2.16. Результаты проведения проверок и план действий по устранению выявленных нарушений доводятся до сведения руководителя ГБУ «ЦФКиС ЗАО г. Москвы» Москомспорта

для принятия решений о необходимости проведения работ по устранению выявленных нарушений.

2.17. В целях контроля устранения выявленных нарушений Комиссия может проводить повторные проверки.

3 Права Комиссии

3.1. Комиссия для реализации своих полномочий имеет право:

– привлекать к проведению проверок работников учреждения;

– запрашивать у работников учреждения необходимую информацию;

– вносить на рассмотрение директора предложения о необходимых мерах по устранению выявленных нарушений выполнения требований к защите персональных данных в ГБУ «ЦФКиС ЗАО г. Москвы» Москомспорта;

– вносить на рассмотрение директора предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке;

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

3.2. К проведению проверок могут привлекаться лица на договорной основе в соответствии с действующим законодательством.

Приложение 1
к Правилам осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в ГБУ «ЦФКиС ЗАО г. Москвы» Москомспорта

Перечень
проверок, осуществляемых в ходе проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (типовой)

№ п/п	Проводимые проверки
1.	Соответствие указанных в «Перечне персональных данных» персональных данных фактически обрабатываемым в ГБУ «ЦФКиС ЗАО г. Москвы» Москомспорта
2.	Соответствие установленных прав доступа к персональным данным полномочиям в рамках трудовых обязанностей работников
3.	Актуальность Перечня должностей работников ГБУ «ЦФКиС ЗАО г. Москвы» Москомспорта, замещение которых предусматривает осуществление обработки персональных данных
4.	Актуальность Перечня мест хранения материальных носителей персональных данных
5.	Подтверждение факта ознакомления с локальными актами ГБУ «ЦФКиС ЗАО г. Москвы» Москомспорта в области обработки и обеспечения безопасности персональных данных
6.	Наличие в поручениях оператора сведений, установленных ч.3 ст. 6 Федерального закона «О персональных данных»
7.	Наличие законных целей и оснований обработки всех персональных данных по всем категориям субъектов персональных данных
8.	Соответствие целей обработки содержанию и объему обрабатываемых персональных данных.
9.	Выборочные проверки уровня знания работниками организационно-распорядительных документов в области обработки и обеспечения безопасности персональных данных
10.	Соблюдение сроков хранения и порядка уничтожения носителей персональных данных
11.	Соблюдение процедур и сроков подготовки ответов на обращения субъектов персональных данных в соответствии со ст.20 и 21 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»
12.	Наличие и (или) необходимость актуализации Уведомления уполномоченного органа по защите прав субъектов персональных данных о начале обработки персональных данных
13.	Соблюдение условий использования средств защиты информации, используемых для обеспечения защиты персональных данных, входящих в зону ответсвенности ГБУ «ЦФКиС ЗАО г. Москвы» Москомспорта, предусмотренных эксплуатационной и технической документацией на них

№ п/п	Проводимые проверки
14.	Функционирование технических средств защиты информации, используемых при обеспечении защиты персональных данных, входящих в зону ответсвенности ГБУ «ЦФКиС ЗАО г. Москвы» Москомспорта
15.	Выполнения мер по обеспечению безопасности персональных данных при их обработке, определенных в соответствии с установленным уровнем защищенности персональных данных, обрабатываемых в информационных системах персональных данных, включая, но не ограничиваясь: – Проверка регулярности обновления средств антивирусной защиты (актуальности вирусных баз) – Проверка проведения резервного копирования программных средств, архивов, журналов, информационных активов, используемых и создаваемых в процессе эксплуатации информационных системах персональных данных – Проверка установки обновлений безопасности программного обеспечения, в т.ч. программного обеспечения средств защиты информации – Проверка регистрации событий информационной безопасности – Проверка реализации процесса управления конфигурациями информационных системах персональных данных и системы защиты персональных данных – Проверка реализации процесса управления доступом к ресурсам информационных системах персональных данных
16.	Правильности эксплуатации средств криптографической защиты информации при их использовании ГБУ «ЦФКиС ЗАО г. Москвы» Москомспорта
17.	Выполнение организационных и технических мероприятий по обеспечению пропускного режима на территорию ГБУ «ЦФКиС ЗАО г. Москвы» Москомспорта