

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 ГБУ «СШОР №63 «Смена» Москомспорта

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 ГБУ «СШОР №63 «Смена» Москомспорта (далее – Правила) устанавливают правила, порядок и формы проведения внутреннего контроля соответствия обработки и защиты персональных данных требованиям, установленным в ГБУ «СШОР №63 «Смена» Москомспорта .

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

– оценка выполнения в ГБУ «СШОР №63 «Смена» Москомспорта требований по обработке и защите персональных данных, установленных законодательством Российской Федерации, Правительства Москвы, а также правовыми актами ГБУ «СШОР №63 «Смена» Москомспорта;

– выявление и предотвращение в ГБУ «СШОР №63 «Смена» 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 «СШОР №63 «Смена» Москомспорта путем проведения проверок соблюдения требований законодательства Российской Федерации, города Москвы и ГБУ «СШОР №63 «Смена» Москомспорта в области обработки и защиты персональных данных (далее по тексту – проверки).

2.2. Внутренний контроль в ГБУ «СШОР №63 «Смена» Москомспорта осуществляется на плановой основе, а также при необходимости – внепланово.

2.3. Внутренний контроль (как плановый, так и внеплановый) проводится комиссией, назначаемой в порядке, установленном в ГБУ «СШОР №63 «Смена» Москомспорта (далее – Комиссия).

2.4. В состав Комиссии могут входить работники ГБУ «СШОР №63 «Смена» Москомспорта 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 руководителем ГБУ «СШОР №63 «Смена» 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 руководства ГБУ «СШОР №63 «Смена» Москомспорта ;
- при существенных изменениях организационной структуры ГБУ «СШОР №63 «Смена» Москомспорта , процессов или процедур обработки и защиты персональных данных;

- по результатам расследования выявленных нарушений требований законодательства Российской Федерации, города Москвы и ГБУ «СШОР №63 «Смена» Москомспорта в области обработки и защиты персональных данных;

- при выявлении большого числа нарушений требований законодательства Российской Федерации, города Москвы и ГБУ «СШОР №63 «Смена» 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 «СШОР №63 «Смена» 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 «СШОР №63 «Смена» Москомспорта для принятия решений о необходимости проведения работ по устранению выявленных нарушений.

2.17. Решения о необходимости проведения работ по устранению выявленных нарушений, принятые руководителем ГБУ «СШОР №63 «Смена» Москомспорта, подлежат реализации в порядке, установленном в ГБУ «СШОР №63 «Смена» Москомспорта.

2.18. 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 ГБУ «СШОР №63 «Смена» Москомспорта;

– запрашивать у работников ГБУ «СШОР №63 «Смена» Москомспорта необходимую информацию;

– вносить на рассмотрение руководителя ГБУ «СШОР №63 «Смена» Москомспорта предложения о необходимых мерах по устранению выявленных нарушений выполнения требований к защите персональных данных в ГБУ «СШОР №63 «Смена» Москомспорта;

– вносить на рассмотрение руководителя ГБУ «СШОР №63 «Смена» Москомспорта 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 «СШОР №63 «Смена» Москомспорта

**Примерный 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 «СШОР №63 «Смена» Москомспорта
2.	Соответствие установленных прав доступа к персональным данным полномочиям в рамках трудовых обязанностей работников
3.	Актуальность Перечня мест хранения материальных носителей персональных данных
4.	Подтверждение факта ознакомления с локальными актами ГБУ «СШОР №63 «Смена» Москомспорта в области обработки и обеспечения безопасности персональных данных
5.	Наличие в поручениях оператора сведений, установленных ч.3 ст. 6 Федерального закона «О персональных данных»
6.	Наличие законных целей и оснований обработки всех персональных данных по всем категориям субъектов персональных данных
7.	Соответствие целей обработки содержанию и объему обрабатываемых персональных данных.
8.	Выборочные проверки уровня знания работниками организационно-распорядительных документов в области обработки и обеспечения безопасности персональных данных
9.	Соблюдение сроков хранения и порядка уничтожения носителей персональных данных
10.	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»
11.	Наличие и (или) необходимость актуализации Уведомления уполномоченного органа по защите прав субъектов персональных данных о начале обработки персональных данных
12.	Соблюдение условий использования средств защиты информации, используемых для обеспечения защиты персональных данных, входящих в зону ответственности ГБУ «СШОР №63 «Смена» Москомспорта, предусмотренных эксплуатационной и технической документацией на них
13.	Функционирование технических средств защиты информации, используемых при обеспечении защиты персональных данных, входящих в зону ответственности ГБУ «СШОР №63 «Смена» Москомспорта

№ п/п	Проводимые проверки
14.	<p>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:</p> <ul style="list-style-type: none"> – 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