ПРАВИЛА
осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в [*Наименование организации, учреждения*]

1. Общие положения

1.1. Настоящие Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в [*Наименование организации, учреждения*] (далее – Правила) устанавливают основания, порядок и формы проведения внутреннего контроля соответствия обработки и защиты персональных данных (далее - ПД) требованиям, установленным в [*Наименование организации, учреждения*] (далее – [*Наименование организации, учреждения*]).

1.2. Настоящие Правила разработаны в соответствии с законодательством Российской Федерации в области обработки и защиты ПД и иными правовыми актами, принимаемыми в соответствии с данным законодательством (далее – законодательство в сфере персональных данных).

1.3. Целями осуществления внутреннего контроля являются:

- оценка общего состояния выполнения в процессах [*Наименование организации, учреждения*] требований по обработке и защите ПД, закрепленных законодательно, а также в локальных актах [*Наименование организации, учреждения*];
- выявление и предотвращение нарушений законодательства в сфере персональных данных.

1.4. Проверки проводятся Комиссией по обеспечению безопасности ПД, создаваемой приказом [*Наименование организации, учреждения*] (далее – Комиссией).

1.5. В состав Комиссии могут входить государственные служащие Департамента образования города Москвы (далее - ДОгМ) и работники подведомственных ДОгМ организаций. В проведении проверки не может участвовать государственный гражданский служащий ДОгМ, прямо или косвенно заинтересованный в ее результатах.

1.6. Члены Комиссии, получившие доступ к ПД субъектов ПД в ходе проведения проверки, обеспечивают конфиденциальность ПД субъектов ПД, не раскрывают третьим лицам и не распространяют ПД без согласия субъекта ПД.

2. Порядок осуществления внутреннего контроля

2.1. Внутренний контроль соответствия обработки ПД установленным требованиям (далее – внутренний контроль) осуществляется [*Наименование организации, учреждения*] путем проведения проверок соблюдения требований законодательства в сфере ПД.

2.2. Проверки разделяются на:

- плановые;
- внеплановые.

2.3. Плановые проверки проводятся не реже одного раза в год.

2.4. Непосредственно перед началом проведения плановой проверки, за 10 (десять) рабочих дней, о тветственным за организацию обработки ПД направляются уведомления руководителям структурных подразделений, в которых планируется проведение внутреннего контроля.

2.5. Внеплановые внутренние проверки могут проводиться в следующих случаях:

- по результатам расследования выявленных нарушений требований законодательства в сфере ПД;
- по результатам внешних контрольных мероприятий, проводимых уполномоченным органом по защите прав субъектов ПД.

2.6. Проверка представляет собой комплекс мероприятий, который состоит из следующих этапов:

- подготовка к проведению проверки;
- сбор свидетельств проверки;
- анализ соответствия контрольным параметрам;
- подготовка заключения по проверке.

2.7. В ходе подготовки к проведению проверки Комиссия определяет:

- границы и описание области, подвергающейся проверки;
- перечень контрольных параметров;
- объекты контроля (процессы, подразделения, информационные системы ПД и т.п.);
- состав участников, привлекаемых для проведения проверки;
- сроки и этапы проведения проверки.

2.8. Типовой перечень контрольных параметров приведен в приложении к настоящим Правилам (Приложение 1).

2.9. Сбор свидетельств проверки включает:

- анализ организационно-распорядительных и регламентирующих документов по обработке и защите ПД;
- опрос персонала, участвующего в процессах обработки ПД, обслуживании и эксплуатации информационных систем ПД.

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

2.11. Свидетельства проверки сопоставляются с контрольными параметрами для формирования заключения по проверке.

2.12. Общий срок проверки не должен превышать 20 (двадцати) рабочих дней. При необходимости срок проведения проверки может быть продлен, но не более чем на 10 (десять) рабочих дней.

3. Права Комиссии при проведении проверки

3.1. Комиссия для реализации своих полномочий имеет право:

- привлекать к проведению проверок служащих [*Наименование организации, учреждения*] и работников подведомственных [*Наименование организации, учреждения*] организаций;

- запрашивать у сотрудников [*Наименование организации, учреждения*] и подведомственных [*Наименование организации, учреждения*] организаций необходимую информацию;

- принимать меры по устранению выявленных нарушений выполнения требований к защите ПД в [*Наименование организации, учреждения*];

- вносить предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности ПД при их обработке;

- вносить предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в отношении обработки ПД.

3.2. Проверки могут проводиться с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации.

4. Порядок фиксирования результатов проверки

4.1. Факт проведения проверок и результаты проверки фиксируются в журнале проведения проверок (Приложение 2).

4.2. По результатам проверки Комиссией, при необходимости, проводится заседание. Решения, принятые на заседаниях Комиссии, оформляются протоколом.

4.3. В целях контроля устранения выявленных нарушений Комиссия проводит повторную проверку.

Приложение 1
к Правилам осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в [*Наименование организации, учреждения*] информационных технологий города Москвы
(справочное)

ПЕРЕЧЕНЬ
контрольных параметров проверок в области обработки и обеспечения безопасности персональных данных
(типовой)

№ п/п	Контрольные параметры и объекты проверок
1.	Соответствие установленных в перечне персональных данных категорий персональных данных фактически обрабатываемым в [*Наименование ОИВ, организации, учреждения*]
2.	Соответствие установленных прав доступа к персональным данным полномочиям в рамках трудовых обязанностей работников
3.	Подтверждение факта ознакомления с локальными актами [*Наименование ОИВ, организации, учреждения*] в области обработки и обеспечения безопасности персональных данных
4.	Наличие в договорах с третьими лицами положений, касающихся обеспечения конфиденциальности и безопасности персональных данных
5.	Наличие законных целей и оснований обработки всех категорий персональных данных
6.	Выборочные проверки сотрудников на предмет знания организационно-распорядительных документов в области обработки и обеспечения безопасности персональных данных
7.	Соблюдение сроков хранения и порядка уничтожения персональных данных
8.	Соблюдение процедур и сроков подготовки ответов на обращения субъектов персональных данных
9.	Необходимость актуализации Уведомления уполномоченного органа по защите прав субъектов персональных данных

Приложение 2
к Правилам осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в [*Наименование ОИВ, организации, учреждения*] (типовая форма)
(рекомендуемое)

ЖУРНАЛ
проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

№	Дата проведения проверки	Основание проверки	Заключение по проверке (кратко)	Подпись председателя Комиссии	Примечание