Приложение 5
к Методическим рекомендациям
Правила осуществления
внутреннего контроля

ПРАВИЛА
осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

1 Общие положения

1.1. Настоящие Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее – Правила) устанавливают основания, порядок и формы проведения внутреннего контроля соответствия обработки и защиты персональных данных требованиям, установленным Федеральным законом от 27 июля 2006 г. №152-ФЗ «О персональных данных», принятыми в соответствии с ним нормативными, правовыми актами Российской Федерации, города Москвы и [*Наименование Организации*].

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

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

– оценка выполнения в [*Наименование Организации*] требований по обработке и защите персональных данных, установленных законодательством Российской Федерации, Правительства Москвы, а также правовыми актами [*Наименование Организации*];

– выявление и предотвращение в [*Наименование Организации*] нарушений законодательства Российской Федерации и города Москвы в сфере персональных данных.

1.4. Внутренний контроль проводится комиссией, назначаемой в порядке, установленном в [*Наименование Организации*] (далее – Комиссия).

1.5. В состав Комиссии могут входить работники [*Наименование Организации*] и внешние эксперты. В проведении внутреннего контроля не могут участвовать работники [*Наименование Организации*], прямо или косвенно заинтересованные в его результатах.

В случае, если Организация является органом исполнительной власти, в состав Комиссии также могут входит работники подведомственных органу исполнительной власти учреждений и предприятий.

Обязанности по проведению контроля могут быть возложены также на иной создаваемый распоряжением по Организации коллегиальный орган.

В проведении контроля не могут участвовать работники Организации, которые прямо или косвенно заинтересованы в его результатах.

1.6. Члены Комиссии, получившие доступ к персональным данным субъектов персональных данных в ходе проведения внутреннего контроля, обеспечивают конфиденциальность персональных данных субъектов персональных данных.

1.7. 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 [*Наименование Организации*] путем проведения проверок соблюдения требований законодательства в сфере персональных данных и внутренних документов [*Наименование Организации*] по обработке и защите персональных данных (далее по тексту – проверки).

2.2. Проверки проводятся непосредственно на месте обработки персональных данных путем:

– опроса либо, при необходимости, путем осмотра рабочих мест работников, участвующих в процессе обработки персональных данных;

– проверки документов, относящихся к деятельности структурного подразделения в части обработки и (или) защиты персональных данных;

– проведения, при необходимости, инструментальных проверок защищенности информационных систем персональных данных.

2.3. Проверки в [*Наименование Организации*] разделяются на:

– плановые;

– внеплановые.

2.4. 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 внутреннего контроля).

Форма плана внутреннего контроля определяется Организацией самостоятельно. План разрабатывается и утверждается ежегодно.

Примерный перечень возможных проверок в ходе внутреннего контроля:

– проверка соответствия указанных в «Перечне персональных данных» ПДн фактически обрабатываемым в Организации;

– проверка соответствия установленных прав доступа к ПДн полномочиям в рамках трудовых обязанностей работников;

– проверка актуальности Перечня должностей работников, замещение которых предусматривает осуществление обработки ПДн;

– проверка актуальности Перечня мест хранения материальных носителей персональных данных;

– проверка подтверждения факта ознакомления работников с локальными актами Организации в области обработки и обеспечения безопасности ПДн;

– проверка наличия в поручениях оператора сведений, установленных ч.3 ст. 6 Федерального закона «О персональных данных»;

– проверка наличия законных целей и оснований обработки всех ПДн по всем категориям субъектов ПДн;

– проверка соответствия целей обработки содержанию и объему обрабатываемых ПДн;

– выборочные проверки уровня знания работниками организационно-распорядительных документов в области обработки и обеспечения безопасности ПДн;

– проверка соблюдения сроков хранения и порядка уничтожения носителей ПДн;

– проверка соблюдения процедур и сроков подготовки ответов на обращения субъектов ПДн в соответствии со ст.20 и 21 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;

– проверка наличия и (или) необходимости актуализации Уведомления уполномоченного органа по защите прав субъектов персональных данных о начале обработки ПДн;

– проверка соблюдения условий использования средств защиты информации, используемых для обеспечения защиты ПДн, входящих в зону ответственности Организации, предусмотренных эксплуатационной и технической документацией на них;

– проверка функционирования технических средств защиты информации, используемых при обеспечении защиты персональных данных, входящих в зону ответственности Организации;

– проверка выполнения мер по обеспечению безопасности ПДн при их обработке, определенных в соответствии с установленным уровнем защищенности ПДн при их обработке в ИСПДн, 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 ИСПДн;*

- *проверка установки обновлений безопасности программного обеспечения, в т.ч. программного обеспечения средств защиты информации;*
- *проверка регистрации событий информационной безопасности;*
- *проверка реализации процесса управления конфигурациями ИСПДн и системы защиты ПДн;*
- *проверка реализации процесса управления доступом к ресурсам ИСПДн;*

– *проверка правильности эксплуатации средств криптографической защиты информации при их использовании в Организации;*

– *проверка выполнения организационных и технических мероприятий по обеспечению пропускного режима на территорию Организации.*

Перечень и содержание проверок может корректироваться исходя из специфики деятельности Организации.

2.5. План внутреннего контроля разрабатывается *Ответственным за организацию обработки персональных данных*, либо по его поручению. Разработанный План внутреннего контроля утверждается в порядке, установленном в [*Наименование Организации*].

2.6. Количество плановых проверок зависит от:

– результатов проведения предыдущих проверок;

– критичности 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 [*Наименование Организации*].

2.7. Внеплановые внутренние проверки могут проводиться в следующих случаях:

– по результатам расследования выявленных нарушений требований законодательства в сфере персональных данных;

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

– при существенных изменениях процессов или процедур обработки и защиты персональных данных;

– при выявлении большого числа нарушений требований законодательства в сфере персональных данных или повторяемости одних и тех же нарушений от проверки к проверке;

– по указанию руководства [*Наименование Организации*].

2.8. 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.

2.9. 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).

2.10. В Отчете должны быть указаны как минимум:

– основание проверки;

– вид проверки (плановая/внеплановая);

– цель проведения проверки;

– выявленные нарушения.

2.11. Отчет подписывают члены Комиссии, председатель Комиссии.

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

2.13. Результаты проведения внутреннего контроля и план действий по устранению выявленных нарушений доводятся до сведения руководства [*Наименование Организации*] для принятия решений о необходимости проведения работ по устранению выявленных нарушений.

В зависимости от специфики Организации результаты проведения проверок и план действий по устранению выявленных нарушений также может доводиться до сведения лица, ответственного за организацию обработки персональных данных.

2.14. Решения о необходимости проведения работ по устранению выявленных нарушений подлежат реализации в порядке, установленном в [*Наименование Организации*].

2.15. 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 [*Наименование Организации*];

– запрашивать у работников [*Наименование Организации*] необходимую информацию;

– принимать меры по устранению выявленных нарушений;

– вносить 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 сфере персональных данных.

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