**Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в аппарате Совета депутатов муниципального округа Марьино**

1. Настоящие Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее - Правила) в аппарате Совета депутатов муниципального округа Марьино (далее – аппарат) определяют процедуры, направленные на выявление и предотвращение нарушений законодательства РФ в сфере персональных данных; основания, порядок, формы и методы проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.

2. Настоящие Правила разработаны в соответствии с Федеральным законом от 27.07.2006 N 152-ФЗ "О персональных данных" и другими нормативными правовыми актами, регулирующими вопросы обработки персональных данных.

3. В настоящих Правилах используются основные понятия, определенные в ст. 3 Федерального закона "О персональных данных".

4. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям в аппарате организовывается проведение плановых проверок условий обработки персональных данных согласно Плану проведения внутреннего контроля обработки персональных данных (Приложение №1). Периодичность планового контроля - не реже одного раза в три года.

По результатам поверки должностным лицом, ответственным за организацию обработки персональных данных в аппарате составляется Акт контроля соответствия обработки персональных данных (Приложение №2).

5. Проверки осуществляются должностным лицом, ответственным за организацию обработки персональных данных в аппарате, либо комиссией, образуемой распоряжением аппарата, в состав которой входят лицо, ответственное за организацию обработки персональных данных, муниципальные служащие, депутаты Совета депутатов муниципального округа Марьино. В проведении проверки не может участвовать работник, прямо или косвенно заинтересованный в её результатах.

6. При проведении проверки соответствия обработки персональных данных установленным требованиям должны быть полностью, объективно и всесторонне установлены:

- 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;

- порядок и условия применения средств защиты информации;

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

- состояние учета машинных носителей персональных данных;

- соблюдение правил доступа к персональным данным;

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

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

- осуществление мероприятий по обеспечению целостности персональных данных.

7. Должностное лицо, ответственное за организацию обработки персональных данных в аппарате, имеет право:

- запрашивать у сотрудников аппарата информацию, необходимую для реализации полномочий;

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

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

- вносить главе муниципального округа предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке;

- вносить главе муниципального округа предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства РФ в отношении обработки персональных данных.

9. В отношении персональных данных, ставших известными должностному лицу, ответственному за организацию обработки персональных данных в аппарате в ходе проведения мероприятий внутреннего контроля, должна обеспечиваться конфиденциальность персональных данных.

10. Проверка должна быть завершена не позднее чем через месяц со дня принятия решения о её проведении.

11. Внеплановая внутренняя проверка проводится по решению главы муниципального округа на основании поступившего в аппарат в письменной форме или в форме электронного документа заявления субъекта персональных данных о нарушении законодательства в области персональных данных.

12. При выявлении в ходе внутреннего контроля нарушений разрабатывается перечень мероприятий по устранению выявленных нарушений и сроки их устранения.

Приложение № 1

к Правилам осуществления внутреннего контроля

соответствия обработки персональных данных

требованиям к защите персональных данных

в аппарате Совета депутатов муниципального округа Марьино

**План проведения**

**внутреннего контроля обработки персональных данных**

**аппарата Совета депутатов муниципального округа Марьино**

|  |  |  |
| --- | --- | --- |
| № п/п | Мероприятие | Срок проведения |
| 1 | Проверка полноты, качества и актуальности внутренних распорядительных документов, регламентирующих обработку и обеспечение безопасности персональных данных | Ежегодно |
| 2 | Контроль выполнения требований по режиму доступа в помещение, где ведется обработка персональных данных | Ежегодно |
| 3 | Проверка порядка использования технических средств защиты | Ежегодно |
| 4 | Соблюдение порядка уточнения, блокирования и уничтожения персональных данных | Ежегодно |
| 5 | Работа с обращениями субъектов персональных данных | Ежегодно |
| 6 | Проверка актуальности сведений в Реестр операторов персональных данных Роскомнадзора | Ежегодно |
| 7 | Подведение итогов | Ежегодно |
| 8 | Устранение недостатков | Ежегодно |
| 9 | Составление акта внутреннего контроля | Ежегодно |
| 10 | Доклад главе муниципального округа Марьино | Ежегодно |

Приложение № 2

к Правилам осуществления внутреннего контроля

соответствия обработки персональных данных

требованиям к защите персональных данных

в аппарате Совета депутатов муниципального округа Марьино

**АКТ**

**контроля соответствия обработки персональных данных**

 В соответствии с п.4 ч.1 ст. 18.1 Федерального закона от 27.07.2006 г. № 152-ФЗ « О персональных данных» в аппарате Совета депутатов муниципального округа Марьино проведен контроль соответствия обработки персональных данных следующим актам:

- Федеральному закону от 27.07.2006 г. №152-ФЗ «О персональных данных» и принятым в соответствии с ним нормативно правовым актам, требованиям к защите персональных данных, в том числе «Положению об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утвержденному постановлением Правительства от 15.09.2008 г. №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», и «Требованиям к защите персональных данных при их обработки в информационных системах персональных данных», утвержденных постановлением Правительства от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

- Иным локальным актам.

 В результате проведения внутреннего контроля выявлены нарушения:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 Меры по устранению нарушений:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Срок устранения нарушений:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Ответственный       \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\

 «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_\_г.