

АДМИНИСТРАЦИЯ
МУНИЦИПАЛЬНОГО ОКРУГА БЕГОВОЙ
ПОСТАНОВЛЕНИЕ

22.10.2020 № 7

**Об утверждении Правил осуществления
внутреннего контроля соответствия
обработки персональных данных требованиям
к защите персональных данных в администрации
муниципального округа Беговой**

В соответствии с Федеральным законом от 27 июля 2006 г. N 152-ФЗ "О персональных данных", постановлением Правительства Российской Федерации от 21 марта 2012 г. N 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами" администрация муниципального округа Беговой постановляет:

1. Утвердить Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в администрации муниципального округа Беговой (Приложение).

2. Опубликовать настоящее постановление в бюллетене «Московский муниципальный вестник» и разместить на официальном сайте муниципального округа Беговой в информационно-телекоммуникационной сети «Интернет».

3. Контроль за выполнением настоящего постановления возложить на главу муниципального округа Беговой П.А. Адамова.

**Глава муниципального округа
Беговой**

П.А. Адамов

Приложение
к постановлению администрации
муниципального округа Беговой
от 22 октября 2020 года № 7

ПРАВИЛА

осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в администрации муниципального округа Беговой

1. Общие положения

1.1. Настоящие правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее – Правила) в администрации муниципального округа Беговой (далее – администрация), определяют процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере обработки персональных данных, а также основания, п

орядок, формы и методы проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.

1.2. Настоящие Правила разработаны на основании Федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и в соответствии с частью 1 «Перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», утвержденных постановлением Правительства Российской Федерации от 21 марта 2012 г. № 211.

1.3. Для обработки персональных данных в администрации используются информационные системы, перечень которых утверждается главой муниципального округа Беговой (далее – информационные системы).

1.4. Пользователем информационной системы (далее – Пользователь) является муниципальный служащий администрации, участвующий в рамках выполнения своих функциональных обязанностей в процессах автоматизированной обработки персональных данных и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты информации информационной системы.

1.5. Контрольные мероприятия за обеспечением уровня защищенности персональных данных и соблюдения условий использования средств защиты информации, а также соблюдением требований законодательства Российской Федерации по обработке персональных данных в информационных системах проводятся в следующих целях:

1.5.1 проверка выполнения требований организационно-распорядительной документации по защите информации в администрации и действующего законодательства Российской Федерации в области обработки и защиты персональных данных;

1.5.2 оценка уровня осведомленности и знаний муниципальных служащих администрации в области обработки и защиты персональных данных;

1.5.3 оценка обоснованности и эффективности применяемых мер и средств защиты информации.

2. Тематика внутреннего контроля

Тематика внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных:

2.1. Проверки соответствия обработки персональных данных установленным требованиям в администрации разделяются на следующие виды:

2.1.1 регулярные;

2.1.2 внеплановые.

2.2. Регулярные контрольные мероприятия проводятся периодически должностным лицом, ответственным за обеспечение безопасности персональных данных в соответствии с требованиями организационно-распорядительной документации и предназначены для осуществления контроля выполнения требований в области защиты персональных данных в администрации. Не реже одного раза в год.

2.3. Внеплановые контрольные мероприятия проводятся на основании решения комиссии по информационной безопасности. Решение о проведении внеплановых контрольных мероприятий и созданию комиссии по информационной безопасности может быть принято в следующих случаях:

2.3.1 по результатам расследования инцидента информационной безопасности;

2.3.2 по результатам внешних контрольных мероприятий, проводимых регулируемыми органами;

2.3.3 по решению главы муниципального округа Беговой.

3. Оформление результатов проведенных контрольных мероприятий

3.1. По итогам проведения внутренних контрольных мероприятий, ответственный за обеспечение безопасности персональных данных в администрации, разрабатывает отчет, в котором указывается:

3.1.1 перечень и описание выявленных нарушений;

3.1.2 рекомендации по устранению выявленных нарушений.

3.1.3 заключение по итогам проведения внутреннего контрольного мероприятия.

3.2. Отчет передается на рассмотрение главе муниципального округа Беговой.

4. Общий порядок проведения контрольных мероприятий

4.1. Контрольные мероприятия проводятся ответственным за обеспечение безопасности обработки персональных данных в администрации.

4.2. Ответственный за обеспечение безопасности персональных данных в администрации не позднее чем за три рабочих дня до начала проведения контрольных мероприятий уведомляет всех руководителей подразделений, в которых планируется проведение контрольных мероприятий. При проведении внеплановых контрольных мероприятий уведомление не требуется.

4.3. Во время проведения контрольных мероприятий, в зависимости от целей мероприятий, могут выполняться следующие проверки:

4.3.1 соответствие полномочий Пользователя правилам доступа;

4.3.2 соблюдение Пользователями требований инструкций по организации антивирусной и парольной защите, инструкции по обеспечению безопасности персональных данных;

4.3.3 соблюдение Порядка доступа в помещения администрации, где ведется обработка персональных данных;

4.3.4 порядок и условия применения средств защиты информации;

4.3.5 состояние учета машинных носителей персональных данных;

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

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

4.3.8 технические мероприятия, связанные со штатным и нештатным функционированием средств защиты информации;

4.3.9 технические мероприятия, связанные со штатным и нештатным функционированием подсистем средств защиты информации.

5. Порядок проведения внутренних проверок

5.1. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям

ответственный за обеспечение безопасности обработки персональных данных организует проведение периодических проверок условий обработки персональных данных.

5.2. Внеплановые проверки соответствия обработки персональных данных установленным требованиям в администрации проводятся на основании поступившего в администрацию письменного заявления о нарушениях правил обработки персональных данных (внеплановые проверки). Проведение внеплановой проверки организуется в течение 3-х рабочих дней с момента поступления соответствующего заявления.

5.3. Проверки осуществляются лицом, ответственным за обеспечение безопасности персональных данных либо комиссией, образуемой распоряжением главы муниципального округа Беговой.

5.4. В проведении проверки не может участвовать муниципальный служащий администрации или сотрудник сторонней организации, осуществляющей сопровождение информационной системы по государственному договору или договору подряда, прямо или косвенно заинтересованный в её результатах.

5.5. Количество регулярных 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 администрации.

5.6. 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 главы муниципального округа Беговой.

5.7. Проверки проводятся непосредственно на месте обработки персональных данных путем опроса либо, при необходимости, путем осмотра рабочих мест работников, участвующих в процессе обработки персональных данных.

5.8. По результатам проверки составляется протокол проведения внутренней проверки (приложение 1), результаты проверок фиксируются в журнале (приложение 3). Протокол подписывается ответственным за обеспечение безопасности персональных данных или членами комиссии.

5.9. При выявлении нарушений в сфере защиты персональных данных составляется акт (приложение 2).

5.10. При выявлении в ходе проверки нарушений, в протоколе делается запись о мероприятиях по устранению нарушений и сроках исполнения.

5.11. Протоколы и акты хранятся у лица, ответственного за обеспечение безопасности персональных данных. Уничтожение протоколов и актов проводится лицом ответственным за обеспечение безопасности персональных данных самостоятельно в январе года следующего за проверочным годом. При необходимости протоколы могут храниться до полного устранения нарушений.

5.12. Результаты проведения внутренних проверок фиксируются в Отчете по результатам проведения внутренних проверок соответствия обработки персональных данных требованиям к защите персональных данных (далее по тексту – Отчет).

6.12. В Отчете должны быть указаны как минимум:

- основание проверки;
- вид проверки (регулярная/внеплановая);
- цель проведения проверки;
- выявленные нарушения.

5.13. Отчет подписывается ответственным за обеспечение безопасности персональных данных либо комиссией, образованной распоряжением главы муниципального округа Беговой.

5.14. По результатам проведения внутреннего контроля ответственным за обеспечение безопасности персональных данных проводится анализ выявленных нарушений и разрабатывается план действий по устранению выявленных нарушений.

5.14. Результаты проведения внутреннего контроля и план действий по устранению выявленных нарушений доводятся до сведения главы муниципального округа Беговой для принятия решений о необходимости проведения работ по устранению выявленных нарушений.

Приложение 1
к Правилам осуществления внутреннего
контроля соответствия обработки
персональных данных требованиям к защите
персональных данных в администрации
муниципального округа Беговой

ПРОТОКОЛ № _____

проведения внутренних проверок контроля соответствия обработки
персональных данных требованиям к защите персональных данных
в администрации муниципального округа Беговой

Настоящий Протокол составлен в том, что « _____ » _____ 20__ г.
_____ (комиссией)

_____ (должность, Ф.И.О. работника)

проведена проверка _____
(тема проверки)

Проверка осуществлялась в соответствии с требованиями:

_____ (название документа)

В ходе проверки проверено:

Выявленные нарушения:

Меры по устранению нарушений:

Срок устранения нарушений: _____

Ответственный за обеспечение
безопасности персональных данных _____

Председатель комиссии:
фамилия и инициалы / подпись / должность

Члены комиссии:
фамилия и инициалы / подпись / должность
фамилия и инициалы / подпись / должность

Приложение 2
к Правилам осуществления внутреннего
контроля соответствия обработки
персональных данных требованиям к защите
персональных данных в администрации
муниципального округа Беговой

А К Т №
выявления нарушений в сфере защиты персональных данных

г. Москва

« ___ » _____ 20__ г.

Настоящий акт составлен в том, что в _____

_____ (наименование структурного подразделения, где выявлено нарушение)

_____ (ФИО и должность лица, допустившего нарушение)

допущено нарушение установленных требований в сфере защиты персональных данных и иной конфиденциальной информации.

Содержание нарушения _____

Требования каких нормативных документов нарушены _____

Комиссия (или уполномоченное лицо), выявившая нарушения

Подписи

_____ (подпись) _____ (Ф. И. О.)

_____ (подпись) _____ (Ф. И. О.)

_____ (подпись) _____ (Ф. И. О.)

С актом ознакомлены:

подпись лица, допустившего нарушение _____ (ФИО) _____

подпись руководителя структурного подразделения, где допущено нарушение _____ (ФИО) _____

