Приложение № 3
к приказу управы
района Филевский парк города Москвы
№ ПРК-133 от «31» декабря 2019 г.

ПРАВИЛА

осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в управе района Филевский парк города Москвы

1. Общие положения

1.1. Настоящие правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее – Правила) в управе района Филевский парк города Москвы (далее – управа), определяют процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере обработки персональных данных, а также основания, порядок, 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 управе используются информационные системы, перечень которых утверждается руководителем управы (далее – информационные системы).

1.4. Пользователем информационной системы (далее – Пользователь) является работник управы, 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 соблюдений 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 управе и действующего законодательства Российской Федерации в области обработки и защиты персональных данных;

1.5.2 оценка уровня осведомленности и знаний работников управы 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 управе разделяются на следующие виды:

2.1.1 регулярные;

2.1.2 плановые;

2.1.3 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 управе.

2.3. Плановые контрольные мероприятия проводятся периодически в соответствии с утвержденным Планом проведения контрольных мероприятий (далее – План, приложение 1) и направлены на постоянное совершенствование системы защиты персональных данных информационной системы.

2.4. 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:

2.4.1 по результатам расследования инцидента информационной безопасности;

2.4.2 по результатам внешних контрольных мероприятий, проводимых регулирующими органами;

2.4.3 по решению главы управы.

3. План проведения контрольных мероприятий

3.1. Для проведения плановых внутренних контрольных мероприятий ответственный за обеспечение безопасности персональных данных в управе, разрабатывает План внутренних контрольных мероприятий на текущий год.

3.2. План проведения внутренних контрольных мероприятий (как плановых, так и внеплановых) включает следующие сведения по каждому из мероприятий:

3.2.1 цели проведения контрольных мероприятий;

3.2.2 задачи проведения контрольных мероприятий,

3.2.3 объекты контроля (процессы, подразделения, информационные системы и т.п.);

3.2.4 состав участников, привлекаемых для проведения контрольных мероприятий;

3.2.5 сроки и этапы проведения контрольных мероприятий.

3.3. Общий срок контрольных мероприятий не должен превышать пяти рабочих дней. При необходимости срок проведения контрольных мероприятий может быть продлен, но не более чем на десять рабочих дней, соответствующие изменения отображаются в Отчете, выполняемом по результатам проведенных контрольных мероприятий.

4. Оформление результатов проведенных контрольных мероприятий

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

4.1.1 описание проведенных мероприятий по каждому из этапов в соответствии с планом;

4.1.2 отклонения от плана, в случае их наличия;

4.1.3 перечень и описание выявленных нарушений;

4.1.4 рекомендации по устранению выявленных нарушений.

4.1.5 заключение по итогам проведения внутреннего контрольного мероприятия.

4.2. Отчет передается на рассмотрение главе управы.

4.3. Общая информация о проведенном контрольном мероприятии фиксируется в Журнале регистрации проверок в сфере защиты персональных данных.

4.4. Результаты проведения мероприятий по плановому и внеплановому контролю заносятся в протокол проведения внутренних проверок контроля соответствия обработки персональных данных требованиям к защите персональных данных в управе (приложение 2).

5. Общий порядок проведения контрольных мероприятий

5.1. Контрольные мероприятия проводятся ответственным за обеспечение безопасности обработки персональных данных в управе.

5.2. Ответственный за обеспечение безопасности персональных данных в управе не позднее чем за три рабочих дня до начала проведения контрольных мероприятий уведомляет всех руководителей подразделений, в которых планируется проведение контрольных мероприятий, и направляет им для ознакомления План проведения контрольных мероприятий. При проведении внеплановых контрольных мероприятий уведомление не требуется.

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

5.3.1 соответствие полномочий Пользователя правилам доступа;

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

5.3.3 соблюдение Порядка доступа в помещения управы, где ведется обработка персональных данных;

5.3.4 порядок и условия применения средств защиты информации;

5.3.5 состояние учета машинных носителей персональных данных;

5.3.6 наличие (отсутствие) фактов несанкционированного доступа к персональных данных и принятие необходимых мер;

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

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

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

5.3.10. Плановые проверки проводятся не реже одного раза в год в соответствии с Планом внутренних проверок контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее – План внутреннего контроля).

6. Порядок проведения внутренних проверок

6.1. 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.

6.2. Проверки соответствия обработки персональных данных установленным требованиям в управе проводятся на основании утвержденного ответственным за обеспечение безопасности персональных данных в управе плана внутренних проверок контроля соответствия обработки персональных данных требованиям к защите персональных данных, согласно приложению 1 к настоящим Правилам, или на основании поступившего в управу 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.

6.3. Проверки осуществляются лицом, ответственным за обеспечение безопасности персональных данных либо комиссией, образуемой приказом главы управы.

6.4. В проведении проверки не может участвовать работник управы или сотрудник сторонней организации, осуществляющей сопровождение информационной системы по государственному договору или договору подряда, прямо или косвенно заинтересованный в её результатах.

6.5. 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 управы.

6.6. 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 управы.

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

6.8. По результатам проверки составляется протокол проведения внутренней проверки (приложение 2), результаты проверок фиксируются в журнале (приложение 5). Протокол подписывается ответственным за обеспечение безопасности персональных данных или членами комиссии.

6.9. При выявлении нарушений в сфере защиты персональных данных составляется акт (приложение 3), выявленные нарушения фиксируются в журнале (приложение 4).

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

6.11. 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.

6.12. 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 (плановая/внеплановая);

– цель проведения проверки;

– выявленные нарушения.

6.13. Отчет подписывается ответственным за обеспечение безопасности персональных данных либо комиссией, образованной приказом главы управы.

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

6.14. Результаты проведения внутреннего контроля и план действий по устранению выявленных нарушений доводятся до сведения главы управы 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

ПЛАН

внутренних проверок контроля соответствия обработки персональных данных требованиям к защите персональных данных

Мероприятие	**Периодичность**	**Исполнитель**
Контроль соблюдения правил доступа к персональным данным	Еженедельно	Ответственный за обеспечение безопасности персональных данных
Контроль соблюдения режима защиты	Ежедневно	Ответственный за обеспечение безопасности персональных данных
Контроль выполнения антивирусной политики	Еженедельно	Ответственный за обеспечение безопасности персональных данных
Контроль выполнения парольной политики	Еженедельно	Ответственный за обеспечение безопасности персональных данных
Контроль соблюдения режима защиты при подключении к сетям общего пользования и (или) международного обмена	Еженедельно	Ответственный за обеспечение безопасности персональных данных
Проведение внутренних проверок на предмет выявления изменений в режиме обработки и защиты персональных данных	Ежегодно	Ответственный за обеспечение безопасности персональных данных

Контроль обновления ПО и единообразия применяемого ПО на всех элементах ГИС «СПД ЗАО»	Еженедельно	Ответственный за обеспечение безопасности персональных данных
Контроль обеспечения резервного копирования	Ежемесячно	Ответственный за обеспечение безопасности персональных данных
Организация анализа и пересмотра имеющихся угроз безопасности персональных данных, а так же предсказание появления новых, еще неизвестных, угроз	Ежегодно	Ответственный за обеспечение безопасности персональных данных
Поддержание в актуальном состоянии нормативно-организационных документов	Ежемесячно	Ответственный за обеспечение безопасности персональных данных
Контроль запрета на использование беспроводных соединений	Ежемесячно	Ответственный за обеспечение безопасности персональных данных

Приложение 2
к Правилам осуществления
внутреннего контроля соответствия
обработки персональных данных
требованиям к защите персональных
данных

ПРОТОКОЛ (ФОРМА) № ____

проведения внутренних проверок контроля соответствия обработки персональных данных требованиям к защите персональных данных в управе района Филевский парк города Москвы

Настоящий Протокол составлен в том, что «____» _____ 2019г.
_____ (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 _____

Приложение 3
к Правилам осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

А К Т №

выявления нарушений в сфере защиты персональных данных

«_____» _____ 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) _____

Приложение 4
к Правилам осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

ЖУРНАЛ
регистрации выявленных нарушений в сфере защиты персональных данных

Начат «___» _____ 20__ г.

Окончен «___» _____ 20__ г.

№	Дата выявления нарушения	Подразделение, где выявлено нарушение и допустившее нарушение лицо (ФИО, должность)	Кем и при каких обстоятельствах выявлено нарушение (жалоба, плановая проверка и т.д.)	Содержание нарушения	Требования, каких нормативных документов нарушены	Корректирующие и предупреждающие действия по устранению нарушения и предотвращению нарушения в дальнейшем	Ответственное за устранение лицо выявленного нарушения лицо (ФИО, должность и его подпись)	Срок устранения нарушения	Отметка о контроле за выполнением (дата, ФИО и должность проверяющего)
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
1									
2									
3									

Приложение 5
к Правилам осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

ЖУРНАЛ
регистрации проверок в сфере защиты персональных данных

Начат «___» _____ 20__ г.

Окончен «___» _____ 20__ г.

№ п/п	Дата проверки	Вид проверки (плановая, внеплановая)	Основания проверки	Контрольные мероприятия	ФИО, должность проверяемого	Результат проверки	Номер, дата протокола результатов проверки	Результаты проверки	ФИО, должности членов комиссии	Подпись	
										Проверяемого	Членов комиссии
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
1											
2											