Утверждено
Приказом и.о. генерального директора
Фонда капитального ремонта ВО
от 18.12.2018 № 110/3

ПРАВИЛА
осуществления внутреннего контроля соответствия обработки персональных данных требованиям в области обработки и защиты персональных данных

1. Общие положения

Настоящие Правила осуществления внутреннего контроля соответствия обработки персональных данных (ПДн) требованиям к защите ПДн разработаны с учетом Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и Постановления Правительства РФ от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

Настоящие Правила определяют порядок осуществления внутреннего контроля соответствия обработки ПДн требованиям к защите ПДн в некоммерческой организации «Фонд капитального ремонта многоквартирных домов Владимирской области» (далее по тексту - Фонд).

2. Тематика проверок обработки ПДн с использованием средств автоматизации:

- соответствие полномочий пользователя матрице доступа;
- соблюдение пользователями информационных систем персональных данных (ИСПДн) парольной политики;
- соблюдение пользователями ИСПДн антивирусной политики;
- соблюдение порядка доступа в помещения, где расположены элементы ИСПДн;
- соблюдение порядка резервирования баз данных и хранения резервных копий;
- соблюдение порядка работы со средствами защиты информации;
- знание пользователей ИСПДн о своих действиях во внештатных ситуациях.

3. Тематика проверок обработки ПДн без использования средств автоматизации:

- хранение бумажных носителей с ПДн;
- доступ к бумажным носителям с ПДн;
- доступ в помещения, где обрабатываются и хранятся бумажные носители с ПДн.

4. Осуществление внутреннего контроля

В целях осуществления внутреннего контроля соответствия обработки ПДн установленным требованиям Фонд организует проведение периодических проверок условий обработки ПДн.

Внутренние проверки проводятся в соответствии с Планом внутренних проверок, утвержденным приказом генерального директора Фонда. Форма Плана приведена в Приложении 1 к настоящим Правилам. При необходимости План может быть изменен.

План внутренних проверок составляется в декабре текущего года на следующий год, и включает в себя все тематики проверок, равномерно распределенные на весь год.

Проверки осуществляются непосредственно на месте обработки ПДн путем опроса либо, при необходимости, путем осмотра рабочих мест сотрудников, участвующих в процессе обработки ПДн.

Для каждой проверки составляется Протокол проведения внутренней проверки. Форма Протокола приведена в Приложении 2 к настоящим Правилам.

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

Протоколы хранятся у ответственного за обработку ПДн в течение текущего года. Уничтожение Протоколов проводится Ответственным за обработку ПДн в январе следующего за проверочным годом.

О результатах проверки и мерах, необходимых для устранения нарушений, генеральному директору Фонда докладывает Ответственный за обработку ПДн

Приложение 1

План
внутренних проверок условий обработки персональных данных

№	Мероприятие	Периодичность	Исполнитель
1.	Проверка актуальности перечня должностных лиц, имеющих право самостоятельного доступа в помещения, где обрабатываются или хранятся ПДн		
2.	Проверка соответствия полномочий пользователя матрице доступа		
3.	Проверка соблюдения пользователями ИСПДн парольной политики		
4.	Проверка соблюдения пользователями ИСПДн антивирусной политики		
5.	Проверка соблюдения порядка доступа в помещения, где расположены элементы ИСПДн		
6.	Проверка своевременности исполнения запросов субъектов персональных данных		
7.	Проверка соблюдения порядка работы со средствами защиты информации		
8.	Проверка знания пользователей ИСПДн о своих действиях во внештатных ситуациях		
9.	Соблюдение порядка хранения и доступа к бумажным носителей с ПДн		
10.	Актуализация локальных нормативных актов по вопросам обеспечения безопасности ПДн		
11.	Контроль ознакомления вновь принимаемых работников с локальными нормативными актами, регламентирующими обработку ПДн		

Приложение 2

Протокол
проведения внутренней проверки условий обработки персональных данных

Настоящий Протокол составлен в том, что __.__.20__ ответственным за организацию обработки персональных данных/начальником отдела информационно-технического обеспечения по внутреннему контролю 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: _____.

Должность Ответственного _____ И.О. Фамилия
либо начальником отдела информационно-технического обеспечения

Должность руководителя
проверяемого подразделения _____ И.О. Фамилия