САМОРЕГУЛИРУЕМАЯ ОРГАНИЗАЦИЯ
НАЦИОНАЛЬНАЯ АССОЦИАЦИЯ
НЕГОСУДАРСТВЕННЫХ
ПЕНСИОННЫХ ФОНДОВ

ПРЕЗИДЕНТ

(НАПФ)

123022, г Москва, ул. 2-ая Звенигородская, д.13, стр.42,
тел./факс (495) 287-85-78,e-mail: info@napf.ru, www.napf.ru

Директору Департамента
информационной безопасности
Банка России
Уварову В.А.

Личный кабинет
Без досылки бумажного экземпляра

«17» июля 2019 г. № 187

Уважаемый Вадим Александрович!

Саморегулируемая организация Национальная ассоциация негосударственных пенсионных фондов выражает Вам свое почтение и просит дать разъяснения о применении негосударственными пенсионными фондами требований Положения Банка России от 17.04.2019 № 684-П «Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций».

Перечень вопросов прилагается.

Выражаем надежду на наше конструктивное взаимодействие с Банком России по всем вопросам, связанным с деятельностью негосударственных пенсионных фондов.

Приложение: на 2 л в 1 экз.

С уважением,

К.С.Угрюмов

Исп.Беляева М.В.
Тел. (495) 287-85-78

Вопросы для разъяснений требований Положения Банка России от 17.04.2019 № 684-П «Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций»

№ п/п	Структурная единица Положения	Вопрос
1	2	3
1	П.1 абз.2	Какая информация содержится в «электронных сообщениях» применительно к деятельности НПФ? Формируются ли «электронные сообщения» в личном кабинете клиента НПФ, если уплата взносов по договору осуществляется из личного кабинета через платежный шлюз банка?
2		Что является финансовой операцией, осуществляемой в электронном виде, работниками и клиентами НПФ?
3	П.2	Существуют ли определенные требования к порядку доведения информации, указанной в этом пункте, до клиентов?
4		Необходимо ли обеспечивать доведение до клиентов – юридических лиц этой информации в случае взаимодействия с НПФ через личный кабинет?
5	П.5-5.3	Каков порядок разработки целевых показателей величины допустимого остаточного операционного риска, связанного с нарушением безопасности информации?
6	П.5.2-5.3	Каков порядок проведения определения применимого к НФО в течение календарного года уровня защиты информации с соблюдением требований пунктов?
7	П.5.4	Каков механизм применения и перечень настроек систем анализа защищённости, с применением которых осуществляется тестирование объектов информационной инфраструктуры НФО на предмет проникновений и поиск уязвимостей информационной безопасности инфраструктуры?
8	П.10	Какой способ подписания электронных сообщений будет считаться достаточным для обеспечения их целостности и подтверждения составления уполномоченным на это лицом?
9	П.6.1	Означает ли словосочетание «с привлечением», что заключение об «оценке определенного уровня защиты» выдает любая организация, в том числе и НПФ самостоятельно? Достаточно ли для исполнения требования указанного пункта привлечения сторонней организации в качестве наблюдателя/соисполнителя за процессом оценки или необходимо, чтобы организация, указанная в этом пункте, провела все работы по оценке и выдала заключение об «оценке определенного уровня защиты информации»?

10	П.11 абз.1	В каком нормативном документе сформулированы риски и методика их составления уполномоченным на это лицом?
11	П.13	Согласно этому пункту НФО необходимо осуществлять регистрацию инцидентов защиты информации при соблюдении требований, указанных в п. 13.1. При этом, в соответствии с п. 13.1 Положения к инцидентам защиты информации относятся события, которые могут привести к осуществлению финансовых операций без согласия клиента и неоказанию услуг. Таким образом, правильно ли понимать, что пункт 13.1 Положения определяет закрытый список событий, которые организация должна относить к инцидентам защиты информации, и данные инциденты, связанные с осуществлением собственных операций НФО, не подлежат обязательной регистрации?
12		Правильно ли понимать, что в этом пункте должностным лицом (отдельным структурным подразделением), ответственным за управление рисками, является руководитель отдельного структурного подразделения, ответственного за организацию системы управления рисками? (в соответствии с формулировкой Федерального закона от 07.05.1998 г. № 75-ФЗ «О негосударственных пенсионных фондах»)
13	П.13.1	В какие сроки будет определен перечень типов инцидентов, согласованный с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности?
14	П.15 абз.2	Просим уточнить порядок и сроки информирования Банка России о выявленных инцидентах защиты информации.