Приложение 2
к приказу №88/1 от 04.06.2021 г.

ПОЛИТИКА

в области обработки и обеспечения безопасности персональных данных АО «НПФ Доверие»

1 Общие положения

1.1. С целью поддержания деловой репутации обеспечения выполнения норм федерального законодательства Акционерное общество «НПФ Доверие» (далее – Фонд) считает важнейшей задачей обеспечение легитимности обработки и безопасности персональных данных субъектов в бизнес-процессах Фонда.

Для решения данной задачи в Фонде введена, функционирует и проходит периодический пересмотр (контроль) система защиты персональных данных.

1.2 Обработка персональных данных в Фонде основана на следующих принципах:

- законности целей и способов обработки персональных данных и добросовестности;
- соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям Фонда;
- соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;
- достоверности персональных данных, их актуальности и достаточности для целей обработки, недопустимости обработки избыточных по отношению к целям сбора персональных данных;
- легитимности организационных и технических мер по обеспечению безопасности персональных данных;
- непрерывности повышения уровня знаний сотрудников Фонда в сфере обеспечения безопасности персональных данных при их обработке;
- стремления к постоянному совершенствованию системы защиты персональных данных.

1.3. Основные понятия:

- персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);
- оператор персональных данных (оператор) - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных

данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

- обработка персональных данных - любое действие (операция) или совокупность действий (операций) с персональными данными, совершаемых с использованием средств автоматизации или без их использования. Обработка персональных данных включает в себя, в том числе:

- сбор;
- запись;
- систематизацию;
- накопление;
- хранение;
- уточнение (обновление, изменение);
- извлечение;
- использование;
- передачу (распространение, предоставление, доступ);
- обезличивание;
- блокирование;
- удаление;
- уничтожение.

- автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники;

- распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

- предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

- блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

- уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

- обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

- информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

- трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

2 Цели сбора и обработки персональных данных

- исполнение положений Трудового/Гражданского/Налогового кодексов и других нормативных актов РФ;

- принятие решения о трудоустройстве кандидата в НПФ;

- заключение и выполнение обязательств по трудовым договорам и агентским соглашениям;

- заключение и выполнение обязательств по договорам обязательного пенсионного страхования и негосударственного пенсионного обеспечения;

- осуществление выплат правопреемникам участников и застрахованных лиц;

- предотвращение, выявление и минимизация последствий конфликта интересов должностных лиц или сотрудников Фонда, под которым понимаются случаи, когда должностное лицо или сотрудник Фонда имеет материальную или личную выгоду в процессе осуществления служебных обязанностей, связанных с обеспечением деятельности фонда в качестве страховщика по обязательному пенсионному страхованию.

3. Правовые основания обработки персональных данных

3.1. Правовым основанием обработки персональных данных являются следующие правовые акты:

- Конституция Российской Федерации;

- Гражданский кодекс Российской Федерации;

- Трудовой кодекс Российской Федерации;

- Налоговый кодекс Российской Федерации;

- Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации";

- Федеральный закон от 15.12.2001 N 167-ФЗ "Об обязательном пенсионном страховании в Российской Федерации";

- Федеральный закон от 28.12.2013 N 424-ФЗ "О накопительной пенсии";

- Федеральный закон от 07.05.1998 N 75-ФЗ "О негосударственных пенсионных фондах";

- Федеральный закон от 30.04.2008 N 56-ФЗ "О дополнительных страховых взносах на накопительную пенсию и государственной поддержке формирования пенсионных накоплений";

- Федеральный закон от 30.11.2011 N 360-ФЗ "О порядке финансирования выплат за счет средств пенсионных накоплений";

- Федеральный закон от 28.12.2013 N 400-ФЗ "О страховых пенсиях";

- Федеральный закон от 28.12.2013 N 422-ФЗ "О гарантировании прав застрахованных лиц в системе обязательного пенсионного страхования

Российской Федерации при формировании и инвестировании средств пенсионных накоплений, установлении и осуществлении выплат за счет средств пенсионных накоплений";

- Федеральный закон от 07.08.2001 N 115-ФЗ "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма";

- Федеральный закон от 26.12.1995 N 208-ФЗ "Об акционерных обществах";

- Закон РФ от 27.12.1991 N 2124-1 "О средствах массовой информации";

- иные нормативные правовые акты, регулирующие особенности обработки персональных данных, связанные с деятельностью Фонда;

- Устав АО «НПФ Доверие»;

- договоры, заключаемые между Фондом и субъектом персональных данных;

- согласие на обработку персональных данных.

4. Категории субъектов персональных данных

4.1. Субъектами персональных данных, чьи персональные данные обрабатываются Фондом, являются:

- действующие и бывшие сотрудники/стажеры/практиканты Фонда, кандидаты на замещение вакантных должностей, а также родственники сотрудщников/стажеров/практикантов Фонда, когда обработка их персональных данных предусмотренном действующим законодательством Российской Федерации или нормативными актами Банка России;

- клиенты Фонда по обязательному пенсионному страхованию (застрахованные лица, их правопреемники, представители застрахованных лиц и их правопреемников), в том числе потенциальные;

- клиенты Фонда по негосударственному пенсионному обеспечению (вкладчики, участники, их правопреемники (наследники), представители вкладчиков, участников и их правопреемников), в том числе потенциальные;

- контрагенты Фонда - физические лица, в том числе потенциальные;

- представители/сотрудники клиентов и контрагентов Фонда – юридических лиц, в том числе потенциальных;

- физические лица, персональные данные которых включены в общедоступные источники персональных данных;

- физические лица, персональные данные которых подлежат опубликованию или обязательному раскрытию в соответствии с федеральным законом (физические лица, входящие в органы управления Фонда, или аффилированные лица Фонда);

- физические лица, персональные данные которых обрабатываются Фондом с их согласия (посетители Фонда или лица, обратившиеся в Фонд по каналам связи, в том числе посетители сайта Фонда).

5 Правила обработки персональных данных

5.1. В Фонде осуществляется обработка ПДн:

- согласно утвержденному Перечню персональных данных с указанием мест и сроков хранения ПДн, обрабатываемых в Фонде.

5.2. В Фонде не допускается обработка следующих категорий ПДн:

- расовая принадлежность;

- политические взгляды;
- философские убеждения;
- состояние интимной жизни;
- национальная принадлежность;
- религиозные убеждения;
- биометрические персональные данные (сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность);
- сведений о состоянии здоровья субъектов персональных данных, за исключением сведений о трудоспособности субъектов персональных данных в случае, когда такие сведения необходимы Фонду для осуществления его функций работодателя либо функций по негосударственному пенсионному обеспечению и обязательному пенсионному страхованию.

5.3. Фонд в ходе своей деятельности может предоставлять персональные данные субъектов следующим лицам:
- Федеральной налоговой службе России;
- Пенсионному фонду России;
- негосударственным пенсионным фондам;
- государственные (правоохранительные органы и др.) органы;
- страховым компаниям;
- медицинским учреждениям;
- кредитным организациям;
- иным организациям в порядке, установленном законодательством или согласием субъекта персональных данных.

5.4. В Фонде не осуществляется трансграничная передача персональных данных (передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу).

5.5. В Фонде запрещено принятие решений относительно субъектов персональных данных на основании исключительно автоматизированной обработки их персональных данных.

5.6. Фонд не размещает персональные данные субъекта в общедоступных источниках без его предварительного согласия субъектов персональных данных за исключением случаев, прямо предусмотренных действующим законодательством.

5.7. Фонд в ходе своей деятельности может предоставлять и (или) поручать обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом. При этом обязательным условием предоставления и (или) поручения обработки персональных данных другому лицу является обязанность сторон по соблюдению конфиденциальности и обеспечению безопасности персональных данных при их обработке.

5.8. Фонд установил следующие условия прекращения обработки персональных данных:
- достижение целей обработки персональных данных и (или) максимальных сроков хранения;

- трата необходимости в достижении целей обработки персональных данных;

- предоставление субъектом персональных данных или его законным представителем сведений, подтверждающих, что персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки;

- невозможность обеспечения правомерности обработки персональных данных;

- отзыв субъектом персональных данных согласия на обработку персональных данных, если сохранение персональных данных более не требуется для целей обработки персональных данных;

- истечение сроков исковой давности для правоотношений, в рамках которых осуществляется либо осуществлялась обработка персональных данных;

- ликвидация юридического лица.

6 Реализованные требования по обеспечению безопасности персональных данных

6.1. Руководство Фонда осознает необходимость и заинтересовано в обеспечении должного как с точки зрения требований нормативных документов РФ, так и обоснованного с точки зрения оценки рисков для бизнеса уровня безопасности персональных данных, обрабатываемых в рамках выполнения основной деятельности.

6.2. Каждый вновь принимаемый сотрудник Фонда, непосредственно осуществляющий обработку персональных данных, ознакамливается с требованиями законодательства Российской Федерации по обработке и обеспечению безопасности персональных данных, с настоящей Политикой и другими локальными актами Фонда по вопросам обработки и обеспечения безопасности персональных данных и обязуется их соблюдать.

6.3. С целью обеспечения безопасности персональных данных при их обработке в Фонде реализуются требования следующих нормативных документов РФ в области обработки и обеспечения безопасности персональных данных:

- Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных»;

- постановление Правительства РФ от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

- постановление Правительства Российской Федерации от 15.09.2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

- базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утверждена заместителем директора ФСТЭК России 15.02.2008 г.);

- методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утверждена заместителем директора ФСТЭК России 14.02.2008 г.);

- Приказ ФСБ от 10 июля 2014 года N 378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

- «Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», утвержденная приказом ФАПСИ от 13 июня 2001 года № 152;;

- приказ ФСТЭК России от 18.02.2013 №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

- отраслевой стандарт обеспечения безопасности персональных данных СТО НАПФ 4.1-2010.

6.4. В Фонде действуют следующие меры по надлежащей организации обработки и обеспечению безопасности персональных данных:

- назначено ответственное лиц, за организацию обработки и обеспечение безопасности персональных данных;

- разработаны локальные акты по вопросам обработки персональных данных;

- осуществляется внутренний контроль и (или) аудит соответствия обработки персональных данных Федеральному закону от 27.07.2006 г. № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, требованиями к защите персональных данных, локальными актами Фонда;

- проводится оценка вреда, который может быть причинен субъектам персональных данных, и определяются актуальные угрозы безопасности персональных данных. В соответствии с выявленными актуальными угрозами Фонд применяет необходимые и достаточные организационные и технические меры, включающие в себя использование средств защиты информации, обнаружение фактов несанкционированного доступа, восстановление персональных данных, установление правил доступа к персональным данным, а также контроль и оценку эффективности применяемых мер;

- утвержден документ, определяющий перечень лиц, доступ которых к персональным данным необходим для выполнения ими служебных обязанностей;

- все лица, уполномоченные Фондом на обработку персональных данных, ознакомлены с положениями законодательства РФ о персональных данных, в том числе с требованиями к защите персональных данных, документами, определяющими политику Фонда в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных;- осуществляется управление конфигурацией информационной системы и системы защиты персональных данных, анализ потенциального воздействия планируемых

изменений в конфигурации информационной системы и системы защиты персональных данных на обеспечение защиты персональных данных и согласование изменений в конфигурации информационной системы с должностным лицом (сотрудником), ответственным за организацию обработки персональных данных;

- выполняется документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных.

6.5. В Фонде действуют следующие технические меры:

- в здании установлены охранная и пожарная сигнализации, а также системы видеонаблюдения;

- сведения на бумажных носителях хранятся в сейфах или запирающихся шкафах, доступ к которым ограничен;

- обеспечивается физическая охрана, предусматривающая контроль доступа в помещения посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения;

- обмен персональными данными при их обработке в информационных системах осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и путем применения технических средств (используются антивирусные средства защиты информации, межсетевое экранирования и иные технические средства);

- осуществляется идентификация и проверка подлинности пользователя при входе в информационную систему по паролю;

- обеспечено наличие средств резервного копирования и восстановления персональных данных;

- разработаны правила доступа к персональным данным, обрабатываемым в информационных системах персональных данных, а также обеспечивается регистрация и учет действий, совершаемых с персональными данными в информационных системах персональных данных.

7. Заключительные положения

7.1. Настоящая политика является общедоступным документом и подлежит размещению на официальном сайте Фонда.

7.2. Настоящая политика подлежит пересмотру в случае появления новых законодательных актов и специальных нормативных документов по обработке и защите персональных данных.