УТВЕРЖДЕНО
приказом генерального директора
АО «Оренбургский НПФ «Доверие»
№120 от 14.12.2017 г.

ПОЛИТИКА

в области обработки и обеспечения безопасности персональных данных

1 Общие положения

1.1. С целью поддержания деловой репутации обеспечения выполнения норм федерального законодательства Акционерное общество «Оренбургский 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.

2 Цели 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 Правила обработки персональных данных

3.1. В Фонде осуществляется обработка ПДн:

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

3.2. 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).

3.3. 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.

3.4. 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).

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

3.6. Фонд не размещает персональные данные субъекта в общедоступных источниках без его предварительного согласия.

3.7. 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.

4 Реализованные требования по обеспечению безопасности персональных данных

4.1. 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.

4.2. 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.

4.3. 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.);

- типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных (утверждены руководством 8 центра ФСБ России 21.02.2008 г. № 149/6/6-622);

- методические рекомендации по обеспечению с помощью крипто средств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации» (утверждены руководством 8 Центра ФСБ России 21.02.2008 г. №149/5-144);

- 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.

4.4. В Фонде действуют следующие организационные меры:

- назначены лица, ответственные за организацию обработки и обеспечения безопасности персональных данных;

- разработаны локальные акты по вопросам обработки персональных данных;

- осуществляется внутренний контроль соответствия обработки персональных данных требованиям к защите персональных данных;

- 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 (работником), ответственным за организацию обработки персональных данных;

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

4.5. 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.