УТВЕРЖДЕНА
Приказом
АО «НПФ «Достойное БУДУЩЕЕ»
от «28» февраля 2023 года
№ 1-28-02-23-0-ОБ

ПОЛИТИКА
АКЦИОНЕРНОГО ОБЩЕСТВА
«НЕГОСУДАРСТВЕННЫЙ ПЕНСИОННЫЙ ФОНД
«ДОСТОЙНОЕ БУДУЩЕЕ»
В ОТНОШЕНИИ ОБРАБОТКИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Москва - 2023

1. Общие положения

1.1. Настоящая Политика АО «НПФ «Достойное БУДУЩЕЕ» в отношении обработки и защиты персональных данных (далее – Политика) является внутренним документом АО «НПФ «Достойное БУДУЩЕЕ» (далее – Фонд), определяющим и регулирующим ключевые направления деятельности Фонда в отношении обработки и защиты персональных данных (далее – ПДн), оператором которых является Фонд.

Политика определяет цели, задачи и основные мероприятия по обеспечению безопасности ПДн в Фонде от несанкционированного доступа, неправомерного их использования или утраты.

1.2. Политика разработана в целях реализации требований законодательства Российской Федерации (далее – РФ) в отношении обработки и защиты ПДн и направлена на обеспечение защиты прав и свобод человека и гражданина при обработке его ПДн в Фонде, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

1.3. Положения Политики распространяются на отношения по обработке и защите ПДн, полученных Фондом как до, так и после утверждения Политики.

1.4. Политика раскрывает основные категории ПДн, обрабатываемых Фондом, цели, способы и принципы обработки Фондом ПДн, права и обязанности Фонда при обработке ПДн, права субъектов ПДн, а также перечень мер, применяемых Фондом в целях защиты и обеспечения безопасности ПДн при их обработке.

1.5. Политика распространяется на работников Фонда, лиц, работающих по гражданско-правовым договорам, на работников сторонних организаций, взаимодействующих с Фондом на основании соответствующих нормативных, правовых и организационно-распорядительных документов, лиц, действующих от имени Фонда.

1.6. Политика размещается на официальном сайте Фонда в сети «Интернет»: www.dfnpf.ru.

2. Источники нормативного правового регулирования

2.1. Политика разработана в соответствии с:

– Трудовым кодексом РФ;

– Налоговым кодексом РФ;

– Федеральным законом от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» (далее – Федеральный закон № 115-ФЗ);

– Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ);

– Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– Федеральным законом от 07.05.1998 № 75-ФЗ «О негосударственных пенсионных фондах» (далее – Федеральный закон № 75-ФЗ);

– Указом Президента РФ от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера»;

– Постановлением Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

– Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– Приказом 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»;

– Приказом ФСБ России от 10.07.2014 № 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»;

– иным законодательством РФ, нормативными правовыми актами РФ, нормативными актами уполномоченных органов.

2.2. Во исполнение требований статьи 18.1 Федерального закона № 152-ФЗ в Фонде приказами Генерального директора утверждены локальные нормативные акты по вопросам обработки и защиты ПДн, в том числе определяющие для каждой цели обработки ПДн, категории и перечень обрабатываемых ПДн, категории субъектов, ПДн которых обрабатываются, способы, сроки их обработки и хранения, порядок уничтожения ПДн при достижении целей их обработки или при наступлении иных законных оснований.

2.3. Политика и иные локальные нормативные акты Фонда не содержат положений, ограничивающих права субъектов ПДн, чьи ПДн обрабатываются в Фонде, а также положения, возлагающие на Фонд не предусмотренные законодательством РФ полномочия и обязанности.

3. Термины и определения

Персональные данные (ПДн) – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту ПДн, далее – субъект ПДн).

Оператор – Фонд, самостоятельно или совместно с другими лицами организующее и (или) осуществляющее обработку ПДн, а также определяющее цели обработки ПДн, состав ПДн, подлежащих обработке, действия (операции), совершаемые с ПДн.

Обработка ПДн – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с ПДн, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн.

Автоматизированная обработка ПДн – обработка ПДн с помощью средств вычислительной техники.

Предоставление ПДн – действия, направленные на раскрытие ПДн определенному лицу или определенному кругу лиц.

Информационная система ПДн (ИСПДн) – совокупность содержащихся в базах данных ПДн и обеспечивающих их обработку информационных технологий и технических средств.

Блокирование ПДн – временное прекращение обработки ПДн (за исключением случаев, если обработка необходима для уточнения ПДн).

Уничтожение ПДн – действия, в результате которых становится невозможным восстановить содержание ПДн в информационной системе ПДн и (или) в результате которых уничтожаются материальные носители ПДн.

Трансграничная передача ПДн – передача ПДн на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

Договор негосударственного пенсионного обеспечения (далее – пенсионный договор) – соглашение между Фондом и Вкладчиком Фонда, в соответствии с которым Вкладчик обязуется уплачивать пенсионные взносы в Фонд, а Фонд обязуется выплачивать Участнику (Участникам) Фонда (далее – Участник) негосударственную пенсию.

Вкладчик – физическое или юридическое лицо, являющееся стороной пенсионного договора и уплачивающее пенсионные взносы в Фонд.

Участник – физическое лицо, которому в соответствии с заключенным между вкладчиком и Фондом пенсионным договором должны производиться или производятся выплаты негосударственной пенсии. Участник может выступать вкладчиком в свою пользу.

Договор об обязательном пенсионном страховании – соглашение между Фондом и застрахованным лицом в пользу застрахованного лица или его правопреемников, в соответствии с которым Фонд обязан при наступлении пенсионных оснований осуществлять

назначение и выплату застрахованному лицу накопительной пенсии и/или срочной пенсионной выплаты или единовременной выплаты либо осуществлять выплаты правопреемникам застрахованного лица.

Застрахованное лицо – физическое лицо, заключившее договор об обязательном пенсионном страховании.

Работники Фонда – физические лица, состоящие с Фондом в трудовых отношениях на основании трудового договора или работающие по гражданско-правовым договорам.

Защита ПДн – комплекс осуществляемых Фондом мероприятий технического, организационного и правового характера, направленных на обеспечение безопасности ПДн.

Файлы cookie – файлы, установленные в компьютере, телефоне, планшете или любом другом техническом устройстве пользователя сайта Фонда, и предназначенные для регистрации действий такого пользователя во время просмотра страниц сайта Фонда. С помощью cookie сервер, на котором находится сайт Фонда, распознает используемый пользователем браузер, предоставляя, например, зарегистрированному пользователю доступ к областям и сервисам без необходимости регистрации при каждом посещении и запоминая его предпочтения для будущих посещений. Файлы cookie также используются для вычисления аудитории и параметров трафика, отслеживания прогресса и количества входов. Файлы cookie содержат данные в обезличенной форме.

4. Принципы обработки Фондом ПДн

4.1. Обработка ПДн осуществляется в Фонде на основе следующих принципов:

4.1.1. Обработка ПДн осуществляется на законной и справедливой основе.

4.1.2. Обработка ПДн ограничивается достижением конкретных, заранее определенных и законных целей. Не допускается обработка ПДн, несовместимая с целями сбора ПДн.

4.1.3. Не допускается объединение баз данных, содержащих ПДн, обработка которых осуществляется в целях, несовместимых между собой.

4.1.4. Обработке подлежат только ПДн, которые отвечают целям их обработки.

4.1.5. Содержание и объем обрабатываемых ПДн должны соответствовать заявленным целям обработки. Обрабатываемые ПДн не должны быть избыточными по отношению к заявленным целям их обработки.

4.1.6. При обработке ПДн должны быть обеспечены точность ПДн, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки ПДн. Фонд должен принимать необходимые меры, либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.

4.1.7. Хранение ПДн осуществляется в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен соответствующим федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем, по которому является субъект ПДн. Обрабатываемые ПДн подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральными законами.

4.2. Обработка ПДн осуществляется с соблюдением принципов и правил, предусмотренных Федеральным законом № 152-ФЗ.

4.2.1. Фондом не осуществляется обработка биометрических ПДн (сведений, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность).

4.2.2. Фондом не осуществляется обработка специальных категорий ПДн (сведения, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни).

5. Обработка ПДн

5.1. В соответствии со статьей 15 Федерального закона №75-ФЗ Фонд в установленных законодательством РФ случаях и порядке вправе получать, обрабатывать и хранить информацию,

доступ к которой ограничен в соответствии с федеральными законами, в том числе осуществлять обработку ПДн вкладчиков – физических лиц, страхователей – физических лиц, участников, застрахованных лиц, выгодоприобретателей и правопреемников участников и застрахованных лиц.

К информации, указанной выше, относится также информация, полученная при:

– обработке сведений, содержащихся на пенсионных счетах негосударственного пенсионного обеспечения, пенсионных счетах накопительной пенсии;

– осуществлении срочной пенсионной выплаты, единовременной выплаты;

– выплате негосударственной пенсии и накопительной пенсии, выплатах (переводе) выкупных сумм и выплатах правопреемникам.

Фонд не обязан получать согласие вкладчиков – физических лиц, страхователей – физических лиц, участников, застрахованных лиц, выгодоприобретателей на обработку в объеме, необходимом для исполнения договора, ПДн, касающихся состояния здоровья указанных лиц и предоставленных ими или с их согласия третьими лицами, т.к. обработка этих данных необходима для исполнения Фондом законодательства.

5.2. Получение ПДн.

5.2.1. ПДн получаются Фондом на основании федеральных законов и иных нормативных правовых актов РФ, в том числе, в необходимых случаях - при наличии согласия субъекта ПДн.

5.2.2. При получении ПДн Фонд сообщает субъекту ПДн по его просьбе о целях, правовых основаниях обработки ПДн, предполагаемых источниках и способах получения и обработки ПДн, перечне действий с ПДн, о лицах (за исключением работников Фонда), которые будут иметь доступ к ПДн, сроке, в течение которого будут обрабатываться и храниться ПДн, а также о юридических последствиях отказа субъекта предоставить свои ПДн и иные сведения, предусмотренные федеральными законами.

5.2.3. Документы, содержащие ПДн, создаются путем:

– оформления пенсионных договоров и/или договоров об обязательном пенсионном страховании;

– оформления документов, связанных с исполнением обязанностей и обязательств по пенсионным договорам и/или договоров об обязательном пенсионном страховании;

– оформления иных форм документов, необходимых для исполнения Фондом обязанностей, предусмотренных законодательством РФ;

– оформления документов, связанных с исполнением Фондом функций и обязанностей юридического лица в процессе своей деятельности;

– копирования оригиналов документов (паспорт, документ об образовании, свидетельство ИНН, пенсионное свидетельство и др.);

– внесения сведений, полученных из оригиналов документов субъекта ПДн, в учетные формы;

– получения оригиналов необходимых документов (трудовая книжка, медицинское заключение, характеристика и др.);

– автоматизированных сервисов сбора статистики сервисов аналитики, функционирующих на ресурсах Фонда в сети «Интернет».

5.2.4. Все ПДн Фонд получает от самого субъекта. Если ПДн субъекта можно получить только у третьей стороны, то субъект уведомляется об этом или Фонд у него получает согласие, за исключением следующих случаев:

– субъект ПДн уведомлен об осуществлении обработки его ПДн соответствующим оператором;

– ПДн получены оператором на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем, по которому является субъект ПДн;

– обработка ПДн, разрешенных субъектом ПДн для распространения, осуществляется с соблюдением запретов и условий, предусмотренных Федеральным законом № 152-ФЗ;

– обработка ПДн для статистических или иных исследовательских целей, если при этом не нарушаются права и законные интересы субъекта ПДн;

– уведомление субъекта ПДн нарушает права и законные интересы третьих лиц.

5.2.5. При сборе ПДн субъектов, в том числе посредством сети «Интернет», Фонд обеспечивает запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, ПДн субъектов с использованием баз данных, находящихся на территории РФ.

Получение согласия субъекта ПДн на обработку его ПДн осуществляется в случае предоставления субъектом ПДн любых ПДн с использованием электронных форм на сайте Фонда.

Сайт Фонда использует файлы cookie и собирает сведения о пользователях, в том числе с использованием сервиса «Яндекс.Метрика», который необходим Фонду для анализа эффективности и улучшения работы сервисов сайта Фонда.

При посещении сайта Фонда пользователи информируются о сборе и использовании файлов cookie, а также об использовании сервиса «Яндекс.Метрика».

Использование сервисов сайта Фонда означает согласие субъекта ПДн на обработку его файлов cookie в соответствии с условиями, определенными Политикой.

В случае отказа от обработки файлов cookie субъект ПДн информируется о необходимости прекратить использование сайта Фонда или отключить файлы cookie в настройках браузера. При этом субъект ПДн также уведомляется и принимает условия, что в таком случае отдельные разделы и/или функции сайта Фонда могут отображаться и/или работать некорректно.

5.3. Обработка ПДн.

5.3.1. Обработка ПДн осуществляется:

– с согласия субъекта ПДн на обработку его ПДн;

– в случаях, когда обработка ПДн необходима для достижения целей, предусмотренных законом, для осуществления и выполнения возложенных законодательством РФ на оператора функций, полномочий и обязанностей;

– в случаях, когда обработка ПДн осуществляется в связи с участием лица в конституционном, гражданском, административном, уголовном судопроизводстве, судопроизводстве в арбитражных судах;

– в случаях, когда обработка ПДн необходима для исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством РФ об исполнительном производстве (далее - исполнение судебного акта);

– в случаях, когда обработка ПДн необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн, а также для заключения договора по инициативе субъекта ПДн или договора, по которому субъект ПДн будет являться выгодоприобретателем или поручителем;

– в случаях, когда обработка ПДн необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта ПДн, если получение согласия субъекта ПДн невозможно;

– в случаях, когда обработка ПДн необходима для осуществления прав и законных интересов оператора или третьих лиц, либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта ПДн;

– в случаях, когда обработка ПДн осуществляется в статистических или иных исследовательских целях, при условии обязательного обезличивания ПДн;

– в случаях, когда ПДн, подлежат опубликованию или обязательному раскрытию в соответствии с федеральным законом.

5.3.2. Цели обработки ПДн:

– выполнение Фондом обязательств в рамках трудовых отношений, а также обязательств, связанных с трудовыми отношениями, предусмотренных законодательством Российской Федерации и локальными нормативными актами Фонда;

– выявление и предотвращение конфликтов интересов при осуществлении деятельности по обязательному пенсионному страхованию;

– оформление полисов добровольного медицинского страхования;

– содействие в оформлении банковских карт (в рамках «зарплатного проекта»);

– изготовление визитной карточки;

– обеспечение пропускного режима в помещения Фонда;

– ведение корпоративных справочников;
– обеспечение замещения вакантных должностей в Фонде;
– исполнение требований законодательства Российской Федерации, нормативных актов Российской Федерации, нормативных актов Банка России;
– исполнение требований Федерального закона № 115-ФЗ;
– заключение и исполнение договора обязательного пенсионного страхования;
– заключение и исполнение договора негосударственного пенсионного обеспечения;
– информирование об услугах Фонда, информирование по вопросам обязательного пенсионного страхования и негосударственного пенсионного обеспечения, проведение рекламных мероприятий, исследований, анкетирования путем направления сообщений на мобильный телефон, осуществления вызовов посредством телефонной связи и направления информации по электронной почте;
– регистрация и предоставление доступа к информации в Личном кабинете клиента на официальном сайте Фонда в сети «Интернет»;
– анализ статистики посещаемости и корректности работы сервисов Фонда, в том числе с использованием сервиса «Яндекс.Метрика»;
– прием и обработка обращений, направленных субъектами ПДн в Фонд;
– заключение и реализация договоров.

5.3.3. Категории субъектов ПДн:

– физические лица, состоящие (состоявшие) в трудовых взаимоотношениях с Фондом и/или работающие (работавшие) по договорам гражданско-правового характера, их близкие родственники;
– кандидаты на трудоустройство, их близкие родственники;
– члены органов управления и контроля Фонда;
– бенефициарные владельцы, лица, являющиеся конечными собственниками Фонда, лица, под контролем либо значительным влиянием которых находится Фонд;
– физические лица, являющиеся (являвшиеся) клиентами Фонда (их правопреемниками), представителями клиентов (их правопреемников), выгодоприобретателями;
– представители юридических лиц, ИП, заключившие договоры;
– застрахованные лица (в том числе умершие застрахованные лица), их правопреемники;
– вкладчики (физические лица);
– участники (в том числе умершие участники), их правопреемники;
– представители (застрахованных лиц, вкладчиков, участников и правопреемников), их правопреемники;
– посетители;
– физические лица, письменно обратившиеся в Фонд;
– иные физические лица, на взаимодействие с которыми Фондом или его контрагентом получено согласие;
– пользователи сайта Фонда;
– физические лица, действующие на основании доверенности.

5.3.4. ПДн, обрабатываемые Фондом.

Перечень ПДн субъектов ПДн и цели их обработки в Фонде, утверждается Приказом генерального директора Фонда и по мере изменения состава обрабатываемых ПДн подлежит пересмотру и уточнению.

5.3.5. Обработка ПДн ведется:

– с использованием средств автоматизации, в том числе с передачей внутри Фонда, а также через сеть «Интернет»;
– без использования средств автоматизации.

5.4. Хранение ПДн.

5.4.1. Получение, обработка и передача на хранение ПДн субъектов ПДн может осуществляться Фондом как на бумажных носителях, так и в электронном виде.

5.4.2. ПДн, зафиксированные на бумажных носителях хранятся в запираемых помещениях с ограниченным доступом.

5.4.3. ПДн субъектов, обрабатываемые с использованием средств автоматизации в разных целях, хранятся в машинных носителях информации, принадлежащих Фонду.

5.4.4. Не допускается хранение и размещение документов, содержащих ПДн, в открытых электронных каталогах (файлообменниках) в ИСПДн.

5.4.5. Хранение ПДн в форме, позволяющей определить субъекта ПДн, осуществляется не дольше, чем этого требуют цели их обработки, если срок хранения ПДн не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем, по которому является субъект ПДн. ПДн подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

5.5. Прекращение обработки ПДн

5.5.1. Обработка ПДн прекращается в следующих случаях:

– субъект ПДн потребовал немедленно прекратить обработку его ПДн, обрабатываемых в целях продвижения товаров, работ, услуг на рынке.

– выявлена неправомерная обработка ПДн, осуществляемая оператором или лицом, действующим по поручению оператора;

– достигнута цель обработки ПДн;

– отзыв субъектом ПДн согласия на обработку его ПДн и в случае, если сохранение ПДн более не требуется для целей обработки ПДн или если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, иным соглашением между оператором и субъектом ПДн, либо если оператор не вправе осуществлять обработку ПДн без согласия субъекта ПДн на основаниях, предусмотренных законодательством РФ.

5.6. Уничтожение ПДн.

5.6.1. Уничтожение документов (носителей), содержащих ПДн производится путем сожжения, дробления (измельчения). Для уничтожения бумажных документов допускается применение шредера.

5.6.2. ПДн на электронных носителях уничтожаются путем стирания или форматирования носителя.

5.6.3. Уничтожение документов (носителей), содержащих ПДн, производится комиссией. Факт уничтожения ПДн подтверждается документально актом об уничтожении носителей, подписанным членами комиссии.

5.6.4. Уничтожение ПДн на электронных носителях сопровождается записями в журналах аудита программных средств, применяемых для уничтожения ПДн.

5.7. Передача ПДн.

5.7.1. Фондом осуществляется передача ПДн третьим лицам если она предусмотрена законодательством или если субъект выразил свое согласие на передачу. Во втором случае перечень лиц, которым передаются ПДн, указан в согласии на обработку ПДн, подписанном субъектом ПДн.

5.8. Поручение обработки ПДн

5.8.1. Фонд имеет право на поручение обработки ПДн третьим лицам в следующих случаях:

– субъект ПДн выразил свое согласие на поручение;

– поручение предусмотрено Российским или иным применимым законодательством в рамках установленной законодательством процедуры.

6. Принципы обеспечения безопасности ПДн

6.1. Основной задачей обеспечения безопасности ПДн при их обработке в Фонде является предотвращение несанкционированного доступа к ним третьих лиц, предупреждение преднамеренных программно-технических и иных воздействий с целью хищения ПДн, разрушения (уничтожения) или искажения их в процессе обработки.

6.2. Для обеспечения безопасности ПДн Фонд руководствуется следующими принципами:

1) законность: защита ПДн основывается на положениях нормативных правовых актов и методических документов уполномоченных государственных органов в области обработки и защиты ПДн;

2) системность: обработка ПДн в Фонде осуществляется с учетом всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности ПДн;

3) комплексность: защита ПДн строится с использованием функциональных возможностей информационных технологий, реализованных в информационных системах Фонда и других имеющихся в Фонде систем и средств защиты;

4) непрерывность: защита ПДн обеспечивается на всех этапах их обработки и во всех режимах функционирования систем обработки ПДн, в том числе при проведении ремонтных и регламентных работ;

5) своевременность: меры, обеспечивающие надлежащий уровень безопасности ПДн, принимаются до начала их обработки;

6) преемственность и непрерывность совершенствования: модернизация и наращивание мер и средств защиты ПДн осуществляется на основании результатов анализа практики обработки ПДн в Фонде с учетом выявления новых способов и средств реализации угроз безопасности ПДн, отечественного и зарубежного опыта в сфере защиты информации;

7) персональная ответственность: ответственность за обеспечение безопасности ПДн возлагается на работников в пределах их обязанностей, связанных с обработкой и защитой ПДн;

8) минимизация прав доступа: доступ к ПДн предоставляется работникам только в объеме, необходимом для выполнения их должностных обязанностей;

9) гибкость: обеспечение выполнения функций защиты ПДн при изменении характеристик функционирования информационных систем ПДн Фонда, а также объема и состава обрабатываемых ПДн;

10) открытость алгоритмов и механизмов защиты: структура, технологии и алгоритмы функционирования системы защиты ПДн Фонда не дают возможности преодоления имеющихся в Фонде систем защиты возможными нарушителями безопасности ПДн;

11) научная обоснованность и техническая реализуемость: уровень мер по защите ПДн определяется современным уровнем развития информационных технологий и средств защиты информации;

12) специализация и профессионализм: реализация мер по обеспечению безопасности ПДн и эксплуатация средств защиты ПДн осуществляются работниками, имеющими необходимые для этого квалификацию и опыт;

13) эффективность процедур отбора кадров и выбора контрагентов: кадровая политика Фонда предусматривает тщательный подбор персонала и мотивацию работников, позволяющую исключить или минимизировать возможность нарушения ими безопасности ПДн; минимизация вероятности возникновения угрозы безопасности ПДн, источники которых связаны с человеческим фактором, обеспечивается получением наиболее полной информации о контрагентах Фонда до заключения договоров;

14) непрерывность контроля и оценки: устанавливаются процедуры постоянного контроля использования систем обработки и защиты ПДн.

7. Доступ к обрабатываемым ПДн

7.1. Доступ к обрабатываемым в Фонде ПДн имеют лица, уполномоченные приказом Генерального директора Фонда.

Перечень работников, допущенных к обработке ПДн в Фонде, разрабатывается и пересматривается по мере необходимости (изменение организационно-штатной структуры, введение новых должностей и т.п.) или на основании заявок руководителей структурных подразделений.

7.2. В целях разграничения доступа при обработке ПДн в Фонде утверждаются и поддерживаются в актуальном состоянии матрицы доступа к информационным системам.

7.3. Доступ работников к обрабатываемым ПДн осуществляется в соответствии с их должностными обязанностями и требованиями локальных нормативных актов Фонда.

Допущенные к обработке ПДн работники под подпись знакомятся с документами Фонда, устанавливающими порядок обработки ПДн, включая документы, устанавливающие права и обязанности конкретных работников.

Работник Фонда получает доступ к ПДн субъектов ПДн после:

– изучения и ознакомления под подпись с локальными нормативными актами Фонда, устанавливающими порядок обработки и защиты ПДн, включая документы, устанавливающие права и обязанности конкретных работников;

– прохождения инструктажа по информационной безопасности;

– ознакомления с видами ответственности за нарушение (невыполнение) норм законодательства РФ в сфере обработки ПДн.

7.4. Порядок доступа субъекта ПДн к его ПДн, обрабатываемым Фондом, определяется в соответствии с законодательством РФ и локальными нормативными актами Фонда.

8. Реализуемые требования к защите ПДн

8.1. Фонд принимает правовые, организационные и технические меры (или обеспечивает их принятие), необходимые и достаточные для обеспечения исполнения обязанностей, предусмотренных Федеральным законом № 152-ФЗ и принятыми в соответствии с ним нормативными правовыми актами, для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн.

8.2. Состав указанных в пункте 8.1 Политики мер, включая их содержание и выбор средств защиты ПДн, определяется, а локальные нормативные акты по обработке и защите ПДн утверждаются (издаются) Фондом, исходя из требований источников, указанных в разделе 2 Политики.

8.3. В соответствии с требованиями нормативных документов в Фонде создана система защиты ПДн (далее – СЗПДн), состоящая из подсистем правовой, организационной и технической защиты.

8.4. Подсистема правовой защиты представляет собой комплекс локальных нормативных актов, обеспечивающих создание, функционирование и совершенствование СЗПДн.

8.5. Подсистема организационной защиты включает в себя организацию структуры управления СЗПДн, разрешительной системы, защиты информации при работе с работниками, партнерами и сторонними лицами, защиты информации в открытой печати, публикаторской и рекламной деятельности, аналитической работы.

8.6. Подсистема технической защиты включает в себя комплекс технических, программных, программно-аппаратных средств, обеспечивающих защиту ПДн.

8.7. Обеспечение безопасности ПДн в Фонде при их обработке в ИСПДн достигается в Фонде, в частности, путем:

1) определения угроз безопасности ПДн и оценки возможностей потенциальных нарушителей информационной безопасности. Тип актуальных угроз безопасности ПДн, оценка возможностей потенциальных нарушителей и необходимый уровень защищенности ПДн определяются в соответствии с требованиями законодательства и с учетом проведения оценки возможного вреда;

2) определения в установленном порядке состава и содержания мер по обеспечению безопасности ПДн, выбора средств защиты информации. При невозможности технической реализации отдельных выбранных мер по обеспечению безопасности ПДн, а также с учетом экономической целесообразности Фондом могут разрабатываться компенсирующие меры, направленные на нейтрализацию актуальных угроз безопасности ПДн. В этом случае в ходе разработки средств защиты ПДн проводится обоснование применения компенсирующих мер для обеспечения безопасности ПДн;

3) применения организационных и технических мер по обеспечению безопасности ПДн, необходимых для выполнения требований к защите ПДн, обеспечивающих определенные уровни защищенности ПДн, включая применение средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства РФ в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз;

4) применения прошедших в установленном порядке процедуру оценки соответствия требованиям законодательства РФ в области обеспечения безопасности информации средств криптографической защиты информации, когда применение таких средств необходимо для нейтрализации актуальных угроз;

5) проведения оценки эффективности принимаемых и реализованных мер по обеспечению безопасности ПДн;

6) учета машинных носителей ПДн, обеспечение их сохранности;

7) обнаружения фактов несанкционированного доступа к ПДн и принятие соответствующих мер, в том числе мер по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные системы ПДн и по реагированию на компьютерные инциденты в них;

8) восстановления ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним или воздействия внешних факторов;

9) установления правил доступа к обрабатываемым ПДн, а также обеспечения регистрации и учета действий, совершаемых с ПДн в ИСПДн;

10) установления индивидуальных паролей доступа работников в информационную систему в соответствии с их должностными обязанностями;

11) организации режима обеспечения безопасности помещений, в которых производится обработка ПДн, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

12) осуществления контроля за принимаемыми мерами по обеспечению безопасности ПДн и уровня защищенности ИСПДн.

8.8. Обеспечение защиты ПДн в Фонде при их обработке, осуществляемой без использования средств автоматизации, достигается, в том числе, путем:

1) недопущения фиксации на одном материальном носителе ПДн, цели обработки которых заведомо не совместимы;

2) принятия мер по обеспечению раздельной обработки ПДн при несовместимости целей обработки ПДн, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку ПДн отдельно от других зафиксированных на том же носителе ПДн;

3) соблюдения требований:

– к раздельной обработке зафиксированных на одном материальном носителе ПДн и информации, не относящейся к ПДн;

– к уточнению ПДн;

– к уничтожению и обезличиванию;

– к использованию типовых форм документов, характер информации в которых предполагает или допускает включение в них ПДн;

– к хранению ПДн, в том числе к обеспечению раздельного хранения ПДн (материальных носителей), обработка которых осуществляется в различных целях, и установлению перечня лиц, осуществляющих обработку ПДн либо имеющих к ним доступ.

8.9. Для обеспечения защиты ПДн в Фонде:

8.9.1. Назначено лицо, ответственное за организацию обработки ПДн, которое осуществляет организацию процессов обработки и защиты ПДн, внутренний контроль за соблюдением Фондом и его работниками законодательства РФ о ПДн, в том числе требований к защите ПДн, доводит до сведения работников Фонда положения законодательства РФ о ПДн, локальных актов по вопросам обработки ПДн, требований к защите ПДн и осуществляет контроль за приемом и обработкой обращений и запросов субъектов ПДн или их представителей

8.9.2. Разработаны документы, определяющие политику Фонда в отношении обработки ПДн, локальные нормативные акты по вопросам обработки ПДн, а также локальные нормативные акты, устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства РФ, устранение последствий таких нарушений;

8.9.3. Разработана техническая документация на ИСПДн Фонда, а также на систему защиты ПДн Фонда;

8.9.4. Применяются средства защиты информации, прошедшие в установленном порядке процедуру оценки соответствия;

8.9.5. Соблюдаются условия, обеспечивающие сохранность ПДн и исключающие несанкционированный к ним доступ;

8.9.6. Осуществляется ознакомление работников, непосредственно задействованных в обработке ПДн, с положениями законодательства РФ о ПДн, в том числе требованиями к защите ПДн, Политикой и иными локальными нормативными актами по вопросам обработки и защиты ПДн, и/или обучение указанных работников по вопросам обработки и защиты ПДн;

8.9.7. Осуществляется внутренний контроль и аудит соответствия обработки ПДн Федеральному закону № 152-ФЗ и принятым в соответствии с ним локальными нормативными актам, требованиям к защите ПДн, Политике Фонда в отношении обработки ПДн, локальным актам Фонда;

8.9.8. Проводится оценка вреда, который может быть причинен субъектам ПДн в случае нарушения Федерального закона № 152-ФЗ, определяется соотношение указанного вреда и принимаемых Фондом мер, направленных на обеспечение исполнения обязанностей, предусмотренных вышеуказанным Федеральным законом.

8.10. Перечень ПДн субъектов ПДн и цели их обработки в Фонде утверждается Приказом Генерального директора Фонда.

8.11. Организация и проведение мероприятий по обеспечению защиты ПДн в Фонде осуществляется в соответствии с внутренними организационно-распорядительными и техническими документами Фонда.

8.12. Общее руководство организацией работ по защите ПДн в Фонде осуществляет директор департамента безопасности Фонда.

8.13. Деятельность Фонда по обеспечению безопасности ПДн контролируется уполномоченным органом по защите прав субъектов ПДн.

9. Основные права субъекта ПДн и обязанности Фонда

9.1. Основные права субъекта ПДн.

9.1.1. Субъект ПДн имеет право требовать от Фонда уточнения его ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

9.1.2. Субъект ПДн имеет право на обращение к Фонду и направление ему запросов.

9.1.3. Субъект ПДн имеет право на получение информации, касающейся обработки его ПДн, в том числе содержащей:

- подтверждение факта обработки ПДн Фондом;
- правовые основания и цели обработки ПДн;
- цели и применяемые Фондом способы обработки ПДн;
- наименование и место нахождения Фонда, сведения о лицах (за исключением работников Фонда), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с Фондом или на основании федерального закона;
- обрабатываемые ПДн, относящиеся к соответствующему субъекту ПДн, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- сроки обработки ПДн, в том числе сроки их хранения;

– порядок осуществления субъектом ПДн прав, предусмотренных Федеральным законом № 152-ФЗ;

– информацию об осуществленной или о предполагаемой трансграничной передаче данных;

– наименование или фамилию, имя, отчество (при наличии) и адрес лица, осуществляющего обработку ПДн по поручению Фонда, если обработка поручена или будет поручена такому лицу;

– информацию о способах исполнения Фондом обязанностей, установленных статьей 18.1 Федерального закона 152-ФЗ;

– иные сведения, предусмотренные Федеральным законом № 152-ФЗ или другими федеральными законами.

– наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению Фонда, если обработка поручена или будет поручена такому лицу;

– иные сведения, предусмотренные Федеральным законом № 152-ФЗ или другими федеральными законами.

9.1.4. Порядок направления субъектами ПДн запросов на предоставление сведений об обработке ПДн определен требованиями Федерального закона № 152-ФЗ. В частности, в соответствии с указанными требованиями запрос на получение информации в Фонд должен содержать:

– сведения о документе, удостоверяющем личность субъекта ПДн (представителя субъекта ПДн), сведения о дате выдачи указанного документа и выдавшем его органе;

– сведения, подтверждающие участие субъекта ПДн в отношениях в Фондом (номер договора, дата заключения договора, условное словесное обозначение и/или иные сведения), либо сведения, иным образом подтверждающие факт обработки ПДн в Фонде;

– подпись субъекта ПДн (представителя субъекта ПДн).

9.1.5. В случае направления запроса представителем субъекта ПДн, запрос должен содержать документ (копию документа), подтверждающий полномочия данного представителя.

9.1.6. Субъект ПДн имеет право на обжалование действий или бездействий Фонда.

9.2. Обязанности Фонда.

Фонд обязан:

– при сборе ПДн предоставить субъекту ПДн по его просьбе информацию, предусмотренную частью 7 статьи 14 Федерального закона № 152-ФЗ;

– в случаях если ПДн были получены не от субъекта ПДн, уведомить субъекта ПДн, если субъект не был уведомлен соответствующим оператором;

– в случае отказа субъекта ПДн в предоставлении ПДн, разъяснять субъекту ПДн юридические последствия такого отказа;

– опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки ПДн, к сведениям о реализуемых требованиях к защите ПДн;

– принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн;

– давать ответы на запросы и обращения субъектов ПДн, их представителей и уполномоченного органа по защите прав субъектов ПДн.

9.3. Фонд предпринимает необходимые и достаточные меры для поддержания точности и актуальности обрабатываемых ПДн, а также удаления ПДн в случаях, если они являются устаревшими, недостоверными или излишними, либо если достигнуты цели их обработки.

9.4. Иные права и обязанности субъектов и Фонда определены положениями Федерального закона № 152-ФЗ и иными нормативными правовыми актами.