

Приложение №1 к приказу
вице-президента
АО "Ханты-Мансийский НПФ"
от 28.10.2025 № 061-П

Политика
в области информационной безопасности
персональных данных
(Редакция №4)

г. Ханты-Мансийск

СОДЕРЖАНИЕ

1. Правовые основания, цели и способы обработки персональных данных.
2. Общие требования при получении, обработке, передаче и предоставлении ПДн.
3. Порядок реагирования на запросы субъектов ПДн.
4. Система защиты информации.
5. Ответственность.

Принятые сокращения

АРМ	-	Автоматизированное рабочее место
АС	-	Автоматизированная система
ВТ	-	Вычислительная техника
ИСПДн	-	Информационная система персональных данных
НМД	-	Нормативно-методический документ
НСД	-	Несанкционированный доступ
ПДн	-	Персональные данные
ПО	-	Программное обеспечение
РД	-	Руководящий документ
СВТ	-	Средство вычислительной техники
СЗИ	-	Средства защиты информации
НПО	-	Негосударственное пенсионное обеспечение
ОПС	-	Обязательное пенсионное страхование
ПДС	-	Программа долгосрочных сбережений
СФР	-	Социальный фонд России
ТК	-	Трудовой кодекс

1. ПРАВОВЫЕ ОСНОВАНИЯ, ЦЕЛИ И СПОСОБЫ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ.

Акционерное общество «Ханты-Мансийский негосударственный пенсионный фонд» (далее – Фонд, Оператор, АО "Ханты-Мансийский НПФ") в рамках выполнения своей основной деятельности осуществляет обработку персональных данных различных категорий субъектов персональных данных. Состав персональных данных, обрабатываемых в Фонде, основания и цели их обработки определены в «Перечне персональных данных, обрабатываемых в АО "Ханты-Мансийский НПФ», который содержит следующие категории персональных данных:

-персональные данные клиентов по НПО (исполнение обязательств по договору негосударственного пенсионного обеспечения);

-персональные данные клиентов по ОПС (исполнение обязательств по договору обязательного пенсионного страхования);

-персональные данные клиентов по ПДС (исполнение обязательств по договору программы долгосрочных сбережений граждан);

-персональные данные, обрабатываемые при исполнении обязательств с СФР;

-персональные данные работников (исполнение обязательств по трудовому договору, гражданско-правовому договору, агентскому договору) и контрагентов Фонда.

Обработка персональных данных в Фонде осуществляется на **основании**:

- Федерального закона от 07.05.1998 № 75-ФЗ "О негосударственных пенсионных фондах";

- Федерального закона от 15 декабря 2001 года N 167-ФЗ "Об обязательном пенсионном страховании в Российской Федерации";

- Федерального закона от 27.07.2006 № 152-ФЗ "О персональных данных";

- Федерального закона от 28.12.2013 №424-ФЗ "О накопительной пенсии";

- Федерального закона от 30.11.2011 №360-ФЗ "О порядке финансирования выплат за счет средств пенсионных накоплений";

- Федерального закона от 07.08.2001 №115-ФЗ "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма";

- Постановления Правительства Российской Федерации от 30.07.2014 №710 "Об утверждении Правил выплаты негосударственным пенсионным фондом, осуществляющим обязательное пенсионное страхование, правопреемникам умерших застрахованных лиц средств пенсионных накоплений, учтенных на пенсионных счетах накопительной пенсии";

- Постановления Правительства РФ от 15.09.2008 № 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации";

- Закона ХМАО-ЮГРЫ от 6 июля 2011 года № 64-ОЗ «О дополнительном пенсионном обеспечении отдельных категорий граждан»;

- договора (НПО, ОПС) между Вкладчиками и Фондом;

- трудовых отношений между работником и Фондом (ст. 16 ТК РФ);

- трудового договора с работником;

- гражданско-правового договора;

- агентского договора;

- договора с контрагентами Фонда.

Применяются следующие **способы обработки** персональных данных:

- смешанная: с передачей по внутренней сети Фонда; с передачей по сетям связи общего пользования в случаях, предусмотренных законодательством и при условиях выполнения требований к передаче ПДн. Трансграничная передача персональных данных не осуществляется.

Обработка ведётся как без использования средств автоматизации, так и с использованием таковых, для чего в Фонде эксплуатируются информационные системы персональных данных (ИСПДн), организованные в соответствии с требованиями нормативных документов в области безопасности ПДн.

2. ОБЩИЕ ТРЕБОВАНИЯ ПРИ ПОЛУЧЕНИИ, ОБРАБОТКЕ, ПЕРЕДАЧЕ И ПРЕДОСТАВЛЕНИИ ПДн.

2.1. Перечень ПДн, цели обработки, основания обработки, сроки хранения, основания для прекращения обработки ПДн - утверждаются приказом вице-президента Фонда.

2.2. В Фонде не обрабатываются специальные категории персональных данных и биометрические персональные данные.

2.3. Обработка персональных данных субъектов ПДн Фондом допускается только при наличии хотя бы одного из следующих условий:

- обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;

- обработка персональных данных необходима для достижения целей, предусмотренных законодательством Российской Федерации, для осуществления Фондом функций, полномочий и обязанностей, возложенных соответствующим законом;

- обработка персональных данных необходима для исполнения договора, стороной либо выгодоприобретателем или поручителем, по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;

- осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе.

2.4. Персональные данные поступают в Фонд непосредственно от субъекта на основании договорных отношений или норм действующего законодательства или от третьей стороны в рамках исполнения норм действующего законодательства Российской Федерации, обрабатываются и хранятся в Фонде не дольше, чем этого требуют цели обработки персональных данных и требования действующего законодательства Российской Федерации.

2.5. Обработка персональных данных Субъектов ПДн Фонда может осуществляться исключительно в целях обеспечения соблюдения Конституции Российской Федерации, Федерального закона от 07.05.1998 №75-ФЗ «О негосударственных пенсионных фондах» (далее – Закон № 75-ФЗ), Трудового Кодекса Российской Федерации и иных нормативных правовых актов РФ, содействия субъектам персональных данных в трудоустройстве, контроля количества и качества выполняемой работы, обеспечения личной безопасности субъекта персональных данных и членов его семьи, а также в целях обеспечения сохранности принадлежащего ему имущества и имущества оператора.

2.6. Обработка персональных данных с использованием средств автоматизации осуществляется в рамках информационных систем персональных данных акционерного общества "Ханты-Мансийский негосударственный пенсионный фонд".

2.7. Перечень информационных систем персональных данных утвержден Приказом Фонда, для каждой ИСПДн назначен Администратор безопасности ИСПДн.

2.8. Эксплуатация информационных систем персональных данных, организована в соответствии с требованиями нормативных документов в области безопасности ПДн.

2.9. Обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы (далее - персональные данные), считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека. К неавтоматизированной обработке относится любая обработка персональных данных, зафиксированных на материальных носителях (например, на бумаге, электронных носителях информации), даже если ранее эти персональные данные циркулировали исключительно в информационной системе персональных данных.

2.10. Особенности обработки персональных данных без использования средств автоматизации определены «Инструкцией об организации работы с документами, содержащими сведения конфиденциального характера».

2.11. Работники Фонда, которые в рамках исполнения должностных обязанностей имеют доступ к персональным данным, обязаны соблюдать режим конфиденциальности персональных данных на всех этапах их обработки.

2.12. Доступ работников Фонда и иных лиц в помещения, в которых осуществляется обработка и хранение персональных данных, ограничивается организационными мерами, инструкцией о пропускном и внутриобъектовом режиме, приказами об определении границ контролируемой зоны для ИСПДн.

2.13. Персональные данные субъектов хранятся не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении. ПДн в ИСПДн уничтожаются с использованием сертифицированных средств защиты информации или средств гарантированного уничтожения в соответствии с утвержденными инструкциями пользователю ИСПДн или администратору безопасности ИСПДн.

2.14. Фонд не в праве передавать информацию, в отношении которой в соответствии с федеральными законами установлена обязанность соблюдать ее конфиденциальность третьим лицам, за исключением случаев, предусмотренных Законом №75-ФЗ и другими федеральными законами.

2.15. Предоставление персональных данных субъекта персональных данных государственным органам производится в соответствии с требованиями действующего законодательства Российской Федерации.

2.16. В соответствии со ст. 15 Законом №75-ФЗ список третьих лиц, с которыми Фонд имеет право осуществлять обмен персональными данными клиентов, ограничен следующим перечнем:

- правопреемники участников и застрахованных лиц;
- специализированный депозитарий фонда;
- по требованию следственные, судебные, налоговые органы, Банк России, Агентство по страхованию вкладов, в установленных законодательством Российской Федерации случаях;
- организации, которые в соответствии с договором осуществляют ведение пенсионных счетов, если указание на такие организации содержится в правилах фонда, а также иные организации, если это необходимо для исполнения пенсионного договора, договора долгосрочных сбережений, договора об обязательном пенсионном страховании. В этих случаях фонд не обязан получать

согласие субъектов персональных данных на дачу поручения обработки персональных данных третьим лицам.

2.17. Фонд вправе поручить в соответствии с ч.3 ст.6 Федерального закона №152-ФЗ, обработку персональных данных третьему лицу, если это необходимо для исполнения пенсионного договора, договора долгосрочных сбережений, договора об обязательном пенсионном страховании. В этих случаях Фонд не обязан получать согласие субъектов персональных данных на дачу поручения обработки персональных данных третьим лицам.

2.18. Представителю субъекта (в том числе адвокату) ПДн передаются в порядке, установленном действующим законодательством и «Положением по организации и проведению работ по обеспечению безопасности персональных данных».

2.19. ПДн субъекта могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого субъекта, за исключением случаев, когда передача ПДн субъекта без его согласия допускается действующим законодательством РФ.

3. ПОРЯДОК РЕАГИРОВАНИЯ НА ЗАПРОСЫ СУБЪЕКТОВ ПДН.

3.1. В процессе основной деятельности Фонд непрерывно взаимодействует с субъектами персональных данных в рамках исполнения договорных обязательств, требуя от субъекта поддержания своих персональных данных в актуальном состоянии.

3.2. Субъект персональных данных имеет право на получение сведений о наличии в фонде его персональных данных, а также на ознакомление с такими персональными данными.

3.3. Субъекты персональных данных имеют право обращения к Фонду по вопросам обработки их персональных данных или направления запроса, связанного с обработкой его персональных данных. Ответ на обращение/запрос должен быть направлен в течение 10 рабочих дней с даты получения обращения/запроса субъекта персональных данных или его представителя. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления Фондом в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации. Сведения должны быть предоставлены субъекту персональных данных в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

3.4. Обращение субъекта должно содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с Фондом (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Фондом, подпись субъекта персональных данных или его представителя.

3.5. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством РФ. Фонд должен предоставить информацию субъекту персональных данных или его

представителю в той форме, в которой направлены соответствующие обращение либо запрос, если иное не указано в обращении или запросе.

3.6. В соответствии с частью 3 статьи 20 Федерального закона № 152-ФЗ, Фонд обязан предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных.

3.7. Частью 8 статьи 14 Федерального закона № 152-ФЗ устанавливается ряд случаев, когда право субъекта персональных данных на доступ к его персональным данным может быть ограничено.

В случае отказа в предоставлении информации о наличии персональных данных, Фонд обязан дать в письменной форме мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 Федерального закона 152-ФЗ или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий десяти рабочих дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса субъекта персональных данных или его представителя. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления оператором в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

3.8. При предоставлении в АО "Ханты-Мансийский НПФ" в рамках исполнения договорных обязательств персональных данных правопреемников субъект принимает на себя обязательства по уведомлению указанного им правопреемника о целях и способах обработки его персональных данных.

3.9. Правопреемники субъекта персональных данных вправе получить от Фонда информацию об обработке и доступе к своим персональным данным, полученным Фондом от субъекта персональных данных в соответствии с федеральным законодательством, на основании подлинника или нотариально заверенной копии документа о смерти субъекта персональных данных.

3.10. Общий контроль за реагированием на обращения субъектов ПДн по вопросам реализации их прав как субъектов ПДн в Фонде осуществляется вице-президентом Фонда Пономаренко С.А. - ответственным за организацию обработки персональных данных в АО «Ханты-Мансийский НПФ». Все обращения и запросы субъектов ПДн отписываются соответствующему исполнителю руководителем Фонда для подготовки ответа и принятия мер по существу запроса. Исполнитель после принятия мер в соответствии с Федеральным законом от 27.07.2006 N 152-ФЗ "О персональных данных" и подготовки ответа субъекту согласовывает свои действия с начальником общего отдела и фиксирует их в журнале «Учета обращений субъектов ПДн о выполнении их законных требований». Ответственность за полноту отражённых сведений в журнале несёт сотрудник, которому было поручено реагировать на запрос субъекта ПДн. Документы, содержащие ПДн субъекта, могут быть отправлены через оператора почтовой связи. При этом должна быть обеспечена их конфиденциальность. За обеспечение конфиденциальности документов при пересылке через оператора почтовой связи отвечает непосредственно оператор почтовой связи, который обязан гарантировать соблюдение тайны связи и нести ответственность за её нарушение, в соответствии со статьей 15 Федерального закона от 17.07.1999 № 176-ФЗ «О почтовой связи».

Лицо, ответственное за организацию обработки персональных данных, в частности, обязано:

- осуществлять внутренний контроль за соблюдением работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;
- доводить до сведения работников положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;
- организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.

4. СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ.

4.1. Общие сведения.

Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, включающей комплекс правовых, режимных, организационных, программно-технических мер и средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, программно-технических воздействий на технические средства обработки персональных данных), а также используемые в информационной системе информационные технологии. Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

Методы и способы защиты информации в информационных системах устанавливаются Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности Российской Федерации в пределах их полномочий.

Средства защиты информации, предназначенные для обеспечения безопасности ПДн при их обработке в ИСПДн, в обязательном порядке должны быть сертифицированы ФСТЭК России и ФСБ России (для криптографических средств защиты информации).

4.2. Система защиты персональных данных реализуется комплексом правовых, режимных, организационных и программно-технических мер:

4.2.1. Правовые меры защиты:

- письменное обязательство (расписка) всех сотрудников о соблюдении конфиденциальности, включение в трудовые контракты (соглашения, договоры) работников обязанности соблюдения требований по защите конфиденциальной информации Фонда;
- определение и применение санкций за нарушение требований по защите информации (в соответствии с действующим законодательством);
- наличие в Положениях о структурных подразделениях и должностных инструкциях сотрудников - обязанностей соблюдать требования по защите конфиденциальной информации Фонда;

4.2.2. Режимные меры защиты:

- мероприятия по установлению, поддержанию и осуществлению контроля за состоянием информационной безопасности;
- физическая охрана (контрольно-пропускной режим, и др.), ведение регистрации постановки и снятия с охранно-пожарной сигнализации (журналы снятия-постановки объектов и список допущенных лиц);

4.2.3. Организационные меры (организационные меры, прежде всего, заключаются в разработке и осуществлении контроля за соблюдением нормативных документов и правил документооборота, приказов и распоряжений в части обеспечения безопасности информации):

- установление правил доступа на объекты, в помещения, в информационные системы, применению в этих целях систем охраны и управления доступом;

- формирование условий и технологических процессов обработки, хранения и передачи конфиденциальной информации отвечающих требованиям информационной безопасности;

- организация работы с персоналом, включая ознакомление с кандидатами, обучение персонала требованиям информационной безопасности;

воспитание у работников понимания важности сохранения в тайне доверенных им конфиденциальных сведений и создание угрозы ответственности и серьезных последствий для них за нарушение конфиденциальности по их вине доверенных им конфиденциальных данных и т.д.

- разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;
- резервное копирование;

- гарантированное уничтожение остаточных данных;
- ограничение оборота черновиков и их уничтожение;
- регулярная смена паролей;
- уничтожение конфиденциальных документов, достигших цели обработки

4.2.4. Технические меры:

- установка и настройка средств защиты информации;
- организация эксплуатации СВТ и СЗИ.

5. ОТВЕТСТВЕННОСТЬ.

Сотрудники АО "Ханты-Мансийский НПФ", субъекты ПД, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с действующим законодательством РФ.