

*Утверждена решением
Наблюдательного совета Фонда
от 2 февраля 2015 г. (протокол № 18)*

**Политика
Автономной некоммерческой организации «Фонд защиты вкладчиков»
в отношении обработки персональных данных**

1. Общие положения

1.1. Настоящая политика (далее - Политика) разработана в соответствии со ст. 18.1 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее - Закон № 152-ФЗ) и является основополагающим внутренним регулятивным документом Автономной некоммерческой организации «Фонд защиты вкладчиков» (далее - Фонд), определяющим ключевые направления его деятельности в области обработки и защиты персональных данных (далее - ПДн), оператором которых является Фонд.

1.2. Политика разработана в целях реализации требований законодательства в области 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, личной и семейной тайн.

1.3. Положения Политики распространяются на отношения по обработке и защите ПДн, полученных Фондом как до, так и после утверждения Политики, за исключением случаев, когда по причинам правового, организационного и иного характера положения Политики не могут быть распространены на отношения по обработке и защите ПДн, полученных до ее утверждения.

1.4. Если в отношениях с Фондом участвуют наследники (правопреемники) и (или) представители субъектов ПДн, то Фонд становится оператором ПДн лиц, представляющих указанных субъектов. Положения Политики и другие внутренние регулятивные документы Фонда распространяются на случаи обработки и защиты ПДн наследников (правопреемников) и (или) представителей субъектов ПДн, даже если эти лица во внутренних регулятивных документах прямо не упоминаются, но фактически участвуют в правоотношениях с Фондом.

2. Основания обработки и состав персональных данных, обрабатываемых в Фонде

2.1. Обработка ПДн в Фонде осуществляется в связи с выполнением законодательно возложенных на Фонд функций, определяемых:

1) Федеральным законом от 02 апреля 2014 г. № 39-ФЗ «О защите интересов физических лиц, имеющих вклады в банках и обособленных структурных подразделениях банков, зарегистрированных и (или) действующих на территории Республики Крым и на территории города федерального значения Севастополя» (в ред. Федерального закона от 04 июня 2014 г. № 149-ФЗ «О внесении изменений в Закон Российской Федерации "Об организации страхового дела в Российской Федерации" и отдельные законодательные акты Российской Федерации»);

2) иными нормативными правовыми актами Российской Федерации.

2.2. Обработка ПДн необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн, в том числе в случае реализации Фондом своего права на уступку прав (требований) по такому договору, а также для заключения договора по инициативе субъекта ПДн или договора, по которому субъект ПДн будет являться выгодоприобретателем или поручителем.

2.3. Кроме того, обработка ПДн в Фонде осуществляется в ходе трудовых и иных непосредственно связанных с ними отношений, в которых Фонд выступает в качестве работодателя (гл. 14 Трудового кодекса Российской Федерации), в связи с реализацией Фондом своих прав и обязанностей как юридического лица.

2.4. В рамках осуществления функции возложенных на Фонд обрабатываются ПДн:

вкладчиков банков и обособленных структурных подразделений банков, зарегистрированных и (или) действовавших на территории Республики Крым и на территории города федерального значения Севастополя по состоянию на 16 марта

2014 г.;

представителей (наследников, правопреемников) субъектов ПДн вкладчиков банков и обособленных структурных подразделений банков, зарегистрированных и (или) действовавших на территории Республики Крым и на территории города федерального значения Севастополя;

2.5. В связи с трудовыми и иными непосредственно связанными с ними отношениями, в которых Фонд выступает в качестве работодателя, обрабатываются ПДн лиц, претендующих на трудоустройство в Фонд, работников Фонда (далее - Работники) и бывших Работников.

2.6. В связи с реализацией своих прав и обязанностей как юридического лица, Фондом обрабатываются ПДн физических лиц, являющихся контрагентами (возможными контрагентами) Фонда по гражданско-правовым договорам, ПДн руководителей, членов коллегиальных исполнительных органов и представителей юридических лиц, ПДн иных физических лиц, представленные участниками закупки, физических лиц, ПДн которых используются для осуществления пропускного режима в занимаемых Фондом помещениях, а также граждан, письменно обращающихся в Фонд по вопросам его деятельности (помимо лиц, указанных в пунктах 2.4. 2.5 Политики).

2.7. ПДн получают и обрабатываются Фондом на основании федеральных законов и иных нормативных правовых актов Российской Федерации, для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн, в том числе в случае реализации Фондом своего права на уступку прав (требований) по такому договору, а также для заключения договора по инициативе субъекта ПДн или договора, по которому субъект ПДн будет являться выгодоприобретателем или поручителем, а в необходимых случаях - при наличии письменного согласия субъекта ПДн.

2.8. В целях исполнения возложенных на Фонд функций Фонд в установленном Законом о ПДн порядке вправе поручить обработку ПДн третьим лицам.

В договоры с лицами, которым Фонд поручает обработку ПДп, включаются условия, обязывающие таких лиц соблюдать предусмотренные законодательством требования к обработке и защите ПДн.

2.9. Фонд предоставляет обрабатываемые им ПДн государственным органам и организациям, имеющим, в соответствии с федеральным законом, право на получение соответствующих ПДн.

2.10. В Фонде не производится обработка ПДн, несовместимая с целями их сбора. По окончании обработки ПДн в Фонде, в том числе при достижении целей их обработки или утраты необходимости в достижении этих целей, обрабатывавшиеся Фондом ПДн уничтожаются или обезличиваются, если иное не предусмотрено Законом о ПДн.

2.11. При обработке ПДн обеспечиваются их точность, достаточность, а при необходимости - и актуальность по отношению к целям обработки. Фонд принимает необходимые меры по удалению или уточнению неполных или неточных ПДн.

3. Принципы обработки ПДн

3.1. Обработка Фондом ПДн осуществляется на законной и справедливой основе, ограничивается достижением конкретных, заранее определенных и законных целей, непосредственно связанных с деятельностью Фонда.

3.2. Не допускается обработка ПДн, несовместимая с целями сбора ПДн, а также объединение содержащих ПДн баз данных, обработка которых осуществляется в целях, несовместимых между собой. При этом:

обработке подлежат только ПДн, которые отвечают целям их обработки;

содержание и объем обрабатываемых ПДн должны соответствовать заявленным целям обработки (обрабатываемые ПДн не должны являться избыточными);

обеспечивается точность ПДн, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки ПДн. Фонд принимает необходимые меры по удалению или уточнению неполных или неточных ПДн (либо обеспечивает принятие таких мер);

хранение ПДн осуществляется в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн, если срок хранения не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн;

обрабатываемые ПДн по достижении целей обработки (или в случае утраты необходимости в достижении этих целей) уничтожаются либо обезличиваются, если иное не предусмотрено федеральным законом, либо передаются в установленном порядке в архив в составе архивных документов.

4. Доступ к обрабатываемым Фондом персональным данным

4.1. Доступ к обрабатываемым в Фонде ПДн имеют лица, уполномоченные приказом Фонда, лица, которым Фонд поручил обработку ПДн на основании заключенного договора, а также лица, чьи ПДн подлежат обработке.

4.2. Доступ Работников к обрабатываемым ПДн осуществляется в соответствии с их должностными обязанностями и требованиями внутренних регулятивных документов Фонда.

Допущенные к обработке ПДн Работники под роспись знакомятся с документами Фонда, устанавливающими порядок обработки ПДн, включая документы, устанавливающие права и обязанности конкретных Работников.

4.3. Порядок доступа субъекта ПДн к его ПДн, обрабатываемым Фондом, определяется в соответствии с законодательством и внутренними регулятивными документами Фонда.

5. Принципы обеспечения безопасности персональных данных

5.1. 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.

5.2. 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 (далее - ИС) 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 персональных данных Фонда (далее - ИСПДн), а также объема и состава обрабатываемых ПДн;

10) открытость алгоритмов и механизмов защиты: структура, технологии и алгоритмы функционирования системы защиты ПДн Фонда (далее - СЗПДн) 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 СЗПДн 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) наблюдаемость и прозрачность: меры по обеспечению безопасности ПДн должны быть спланированы так, чтобы результаты их применения были явно наблюдаемы (прозрачны) и могли быть оценены лицами, осуществляющими контроль;

15) непрерывность контроля и оценки: устанавливаются процедуры постоянного контроля использования систем обработки и защиты ПДн, а результаты контроля регулярно анализируются.

6. Реализуемые требования к защите персональных данных

6.1. Фонд принимает правовые, организационные и технические меры (или обеспечивает их принятие), необходимые и достаточные для обеспечения исполнения обязанностей, предусмотренных Законом о ПДн 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.

6.2. Состав указанных в пункте 6.1 Политики мер, включая их содержание и выбор средств защиты ПДн, определяется, а внутренние регулятивные документы об обработке и защите ПДн утверждаются (издаются) Фондом исходя из требований:

Закона № 152-ФЗ;

Трудового кодекса Российской Федерации;

постановления Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

приказа ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности ПДн при их обработке в информационных системах ПДн»;

постановления Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

постановления Правительства Российской Федерации РФ от 6 июля 2008 г. № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»;

иных нормативных правовых актов Российской Федерации об обработке и защите ПДн.

6.3. В предусмотренных законодательством случаях обработка ПДн осуществляется Фондом с согласия субъектов ПДн.

Фондом производится устранение выявленных нарушений законодательства об обработке и защите ПДн.

6.4. Хранение ПДн осуществляется в форме, позволяющей определить субъекта ПДн, не дольше чем этого требуют цели обработки ПДн, если срок хранения не установлен законом о ПДн, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн.

6.5. Фондом осуществляется ознакомление работников Фонда, непосредственно осуществляющих обработку ПДн, с положениями законодательства о ПДн, в том числе требованиями к защите ПДн, Политикой и иными внутренними регулятивными документами по вопросам обработки ПДн, и (или) обучение указанных работников по вопросам обработки и защиты ПДн.

6.6. При обработке ПДн с использованием средств автоматизации Фондом, в частности, применяются следующие меры:

1) назначается Ответственный за организацию обработки ПДн в Фонде, являющийся одним из заместителей Исполнительного директора Фонда, определяется его компетенция;

2) утверждаются (издаются) внутренние регулятивные документы по вопросам обработки и защиты ПДн, в том числе устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства, устранение последствий таких нарушений;

3) осуществляется внутренний контроль и (или) аудит соответствия обработки ПДн Закону о ПДн и принятым в соответствии с ним нормативным правовым актам, требованиям к защите ПДн, Политике и внутренним регулятивным документам Фонда;

4) проводится оценка вреда, который может быть причинен субъектам ПДн в случае нарушения Закона о ПДн, определяется соотношение указанного вреда и принимаемых Фондом мер, направленных на обеспечение исполнения обязанностей, предусмотренных Законом о ПДн.

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

1) определения угроз безопасности ПДн. Тип актуальных угроз безопасности ПДн 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 СЗПДн 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, когда применение таких средств необходимо для нейтрализации актуальных угроз.

В Фонде, в том числе, осуществляются:

оценка эффективности принимаемых и реализованных мер по обеспечению безопасности ПДн;

учет машинных носителей ПДн, обеспечение их сохранности;

обнаружение фактов несанкционированного доступа к ПДн и принятие соответствующих мер;

восстановление ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

установление правил доступа к обрабатываемым ПДн, а также обеспечение регистрации и учета действий, совершаемых с ПДн;

организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности

неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

контроль за принимаемыми мерами по обеспечению безопасности ПДн, уровня защищенности ИСПДн.

6.8. Обеспечение защиты ПДн в Фонде при их обработке, осуществляемой без использования средств автоматизации, достигается, в частности, путем:

- 1) обособления ПДн от иной информации;
- 2) недопущения фиксации на одном материальном носителе ПДн, цели обработки которых заведомо не совместимы;
- 3) использования отдельных материальных носителей для обработки каждой категории ПДн;
- 4) принятия мер по обеспечению отдельной 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;
- 5) соблюдения требований:
 - к отдельной обработке зафиксированных на одном материальном носителе ПДн и информации, не относящейся к ПДн;
 - уточнению ПДн;
 - уничтожению или обезличиванию части ПДн;
 - использованию типовых форм документов, характер информации в которых предполагается или допускается включение в них ПДн;
 - ведению журналов, содержащих ПДн, необходимых для выдачи однократных пропусков субъектам ПДн в занимаемые Фондом здания и помещения;
 - хранению ПДн, в том числе к обеспечению отдельного хранения ПДн (материальных носителей), обработка которых осуществляется в различных целях, и установлению перечня лиц, осуществляющих обработку ПДн либо имеющих к ним доступ.