У Т В Е Р Ж Д Е Н А
Правлением АО «НДБанк»
Протокол от 12.01.2022г. № 01-12/2022П

В В Е Д Е Н А В Д Е Й С Т В И Е
Приказом № 001/003 от 12.01.2022г.

ПОЛИТИКА ОБРАБОТКИ И ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В АО «НДБанк»

Москва, 2022

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Политика определяет порядок обработки персональных данных и меры защиты по обеспечению безопасности персональных данных в АО «НДБанк» (далее – Банк) с целью защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

1.2. Политика обработки и обеспечения безопасности персональных данных в Банке разработана в соответствии с Федеральным законом №152-ФЗ «О персональных данных» от 27.07.2006 г.

1.3. В настоящей Политике используются следующие термины и определения:

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

Банк – АО «НДБанк» – юридическое лицо, самостоятельно или совместно с другими лицами организующее и (или) осуществляющее обработку персональных данных, а также определяющее цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

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

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

обезличивание персональных данных – действия, в результате которых невозможно определить без использования дополнительной информации принадлежность персональных данных конкретному субъекту персональных данных;

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

оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

ответственный сотрудник Банка – специальное должностное лицо, назначаемое в соответствии с требованиями п. 2 ст. 7 Федерального закона от 07.08.2001 г. №115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путём, и финансированию терроризма» приказом Председателя Правления Банка, ответственное за реализацию Правил внутреннего контроля;

Служба финансового мониторинга – структурное подразделение Банка, находящееся в непосредственном подчинении у Ответственного работника Банка;

персональные данные – любая информация, относящаяся к прямо или косвенно определённому или определяемому физическому лицу (субъекту персональных данных);

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

распространение персональных данных – действия, направленные на раскрытие персональных данных неопределённому кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом;

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

уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных и (или) результате которых уничтожаются материальные носители персональных данных.

1.4. Действие Политики распространяется на все персональные данные субъектов, обрабатываемые в Банке с применением средств автоматизации и без применения таких средств.

1.5. К настоящей Политике имеет право доступа любой субъект персональных данных.

2. ПРИНЦИПЫ И УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Обработка персональных данных в Банке осуществляется на основе принципов:

- ✓ законности и справедливой основы;
- ✓ ограничения обработки персональных данных достижением конкретных, заранее определённых и законных целей;

- ✓ недопущения обработки персональных данных, несовместимой с целями сбора персональных данных;
- ✓ недопущения объединения баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;
- ✓ обработка только тех персональных данных, которые отвечают целям их обработки;
- ✓ соответствия содержания и объёма обрабатываемых персональных данных заявленным целям обработки;
- ✓ недопущения обработки избыточных персональных данных по отношению к заявленным целям их обработки;
- ✓ обеспечения точности, достаточности и актуальности персональных данных по отношению к целям обработки персональных данных;
- ✓ уничтожение либо обезличивание персональных данных по достижении целей их обработки или в случае утраты необходимости в достижении этих целей, при невозможности устранения Банком допущенных нарушений при обработке персональных данных.

2.2. Обработка персональных данных в Банке допускается в следующих случаях:

- ✓ обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;
- ✓ обработка персональных данных необходима для достижения целей, предусмотренных законом, для осуществления и выполнения возложенных законодательством Российской Федерации на Банк функций, полномочий и обязанностей;
- ✓ обработка персональных данных необходима для исполнения договора, стороной которого 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;
- ✓ обработка персональных данных необходима для осуществления прав и законных интересов Банка или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;
- ✓ осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе (общедоступные персональные данные);
- ✓ осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с Федеральным законом.

2.3. Банк не раскрывает персональные данные субъекта третьим лицам и не распространяет персональные данные без согласия субъекта персональных данных, если иное не предусмотрено Федеральным законом.

2.4. В целях информационного обеспечения в Банке могут создаваться общедоступные источники персональных данных работников, в том числе справочники и адресные книги. В общедоступные источники персональных данных с письменного согласия работника могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, предоставленные субъектом.

Сведения о работнике должны быть в любое время исключены из общедоступных источников персональных данных по требованию работника либо по решению суда или иных уполномоченных государственных органов.

2.5. Банк поручает обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено Федеральным законом, на основании заключаемого с этим лицом договора поручения обработки персональных данных. Лицо, осуществляющее обработку персональных данных по поручению Банка, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом №152-ФЗ.

2.6. В договоре поручения обработки персональных данных Банком определяется перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, устанавливается обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также указываются требования к защите обрабатываемых персональных данных в соответствии со статьёй 19 Федерального закона №152-ФЗ «О персональных данных».

В случае, если Банк поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несёт Банк.

2.7. Банком не обрабатываются персональные данные, относящиеся к специальным категориям:

- ✓ расовая принадлежность;
- ✓ национальная принадлежность;
- ✓ политические взгляды;
- ✓ религиозные и философские убеждения;
- ✓ состояния здоровья (за исключением данных о состоянии здоровья работников Банка в случаях, предусмотренных Трудовым кодексом РФ);
- ✓ интимная жизнь;

- ✓ персональные данные о частной жизни, о членстве субъектов персональных данных в общественных объединениях или их профсоюзной деятельности.

  Обработка указанных категорий персональных данных допускается законом в случаях, если:
- ✓ субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных;
- ✓ персональные данные являются общедоступными.

2.8. Обработка персональных данных о судимости может осуществляться Банком исключительно в случаях и в порядке, которые определяются в соответствии с Федеральными законами.

Банк осуществляет обработку данных о судимости работников, занимающих должности (претендующих на должности) членов Совета директоров Банка, руководителей Банка, главного бухгалтера, заместителей главного бухгалтера , управляющих Филиалов и их заместителей, главных бухгалтеров и заместителей главных бухгалтеров Филиалов, Ответственного сотрудника Банка и работников Службы финансового мониторинга Банка, в соответствии с положениями пунктов 3.1 и 6.10 Инструкции Центрального Банка Российской Федерации от 02.04.2010 г. №135-И «О порядке принятия Банком России решения о государственной регистрации кредитных организаций и выдаче лицензий на осуществление банковских операций» Также обработка персональных данных о судимости работников может осуществляться в соответствии с Трудовым кодексом Российской Федерации.

2.9. Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность – биометрические персональные данные – обрабатываются Банком только при наличии согласия субъекта в письменной форме или в случае, когда такая обработка предусмотрена законодательством Российской Федерации, в том числе законодательством о порядке выезда из Российской Федерации и въезда в Российскую Федерацию.

2.10. Трансграничная передача персональных данных на территорию иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных данных, может осуществляться Банком в случаях:

- ✓ наличия согласия в письменной форме субъекта персональных данных на трансграничную передачу его персональных данных;
- ✓ исполнения договора, стороной которого является субъект персональных данных.

3. ЦЕЛЬ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Осуществление функций, возложенных на Банк Федеральным Законом от 02.12.1990г. №395-1 «О банках и банковской деятельности», включая обработку персональных данных клиентов Банка, необходимую для

осуществления основного вида деятельности – оказании банковских услуг (в том числе: сбор и накопление необходимой информации по клиентам, ведение клиентской базы для оказания банковских услуг, оформление и печать документов и договоров, осуществление операционной деятельности Банка согласно законодательству РФ), Федеральным Законом 23.12.2003г. №177-ФЗ «О страховании вкладов физических лиц в банках Российской Федерации;

3.2. В целях организации учета служащих Банка для обеспечения соблюдения законов и иных нормативных правовых актов, содействия служащему в трудоустройстве, обучении, продвижении по службе, пользования различного вида льготами в соответствии с Трудовым кодексом Российской Федерации, Налоговым кодексом Российской Федерации, федеральными законами, в частности: Федеральным законом от 01.04.1996г. №27-ФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования;

3.3. Осуществление функций, возложенных на Банк Федеральным Законом от 7 августа 2001 г. № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», а также нормативными актами Банка России, в том числе Положением Банка России № 321-П от 29 августа 2008г; осуществление функций, возложенных на Банк Федеральным Законом от 30.12.2004г. № 218-ФЗ «О кредитных историях»;

3.4. Осуществление функций, возложенных на Банк Федеральным Законом от 10 декабря 2003г. № 173-ФЗ «О валютном регулировании и валютном контроле»; осуществление функций, возложенных на Банк Федеральным Законом 22 апреля 1996 года №39-ФЗ «О рынке ценных бумаг».

4. ПРАВОВЫЕ ОСНОВАНИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Политика обработки персональных данных Оператора определяется следующими нормативно-правовыми актами:

4.1.1. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

4.1.2. «Трудовой кодекс Российской Федерации» от 30.12.2001 N 197-ФЗ;

4.1.3. Федеральный закон "О банках и банковской деятельности" от 02.12.1990 N 395-1;

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

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

4.1.6. Иные нормативно-правовые акты РФ, обязательные для Оператора;

4.1.7. Локальные нормативные акты, регулирующие в Обществе вопросы, касающиеся обработки персональных данных.

5. КАТЕГОРИИ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. **Подлежат обработке**

- ✓ фамилия, имя, отчество;
- ✓ год рождения;
- ✓ месяц рождения;
- ✓ дата рождения;
- ✓ место рождения;
- ✓ адрес;
- ✓ семейное положение;
- ✓ социальное положение;
- ✓ имущественное положение;
- ✓ образование;
- ✓ профессия;
- ✓ доходы/

5.2. **Не обрабатываются**

- ✓ расовая принадлежность;
- ✓ национальная принадлежность;
- ✓ политические взгляды;
- ✓ религиозные убеждения;
- ✓ философские убеждения;
- ✓ состояние здоровья;
- ✓ состояние интимной жизни;
- ✓ биометрические персональные данные.

6. СУБЪЕКТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

- ✓ лица, обработка персональных данных, которых осуществляется в связи с трудовыми отношениями Банка, в том числе работники АО «НДБанк» и соискатели на занятие вакантных должностей;
- ✓ лица, обработка персональных данных, которых осуществляется в связи с корпоративными отношениями АО «НДБанк», в том числе Председатель Правления, члены Правления, члены Совета Директоров, члены Ревизионной комиссии, бенефициары АО «НДБанк»;
- ✓ лица, обработка персональных данных, которых осуществляется в связи с гражданско-правовыми отношениями АО «НДБанк», в том числе клиенты, контрагенты Банка;

- ✓ иные лица, в том числе посетители АО «НДБанк».

7. АКТУЛИЗАЦИЯ, СРОК ИЛИ УСЛОВИЕ ПРЕКРАЩЕНИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОТВЕТЫ НА ЗАПРОСЫ СУБЪЕКТОВ НА ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ

7.1. В случае подтверждения факта неточности персональных данных или неправомерности их обработки, персональные данные подлежат их актуализации Оператором, обработка прежних при этом прекращается.

7.2. Обработка персональных данных прекращается при достижении целей такой обработки, а также по истечении срока, предусмотренного законодательством РФ, договором, или согласием субъекта персональных данных на обработку его персональных данных, а также выявлением неправомерной обработки персональных данных.

7.3. При отзыве субъектом персональных данных согласия на обработку его персональных данных обработка осуществляется только в пределах, необходимых для исполнения заключенных с ним договоров и в целях, предусмотренных законодательством РФ.

7.4. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных. Для получения указанной информации субъект персональных данных может отправить письменный запрос.

8. ПРАВА СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ, ОБЕСПЕЧИВАЕМЫЕ БАНКОМ

8.3. Субъект персональных данных принимает решение о предоставлении его персональных данных и даёт Банку согласие на их обработку Банком свободно, своей волей и своём интересе. Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено Федеральным законом.

Обязанность предоставить доказательство получения согласия субъекта персональных данных на обработку его персональных данных или доказательство наличия оснований на обработку, указанных в Федеральном законе №152-ФЗ, возлагается на Банк.

8.4. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, если такое право не ограничено Федеральными законами. Субъект персональных данных вправе требовать от Бака уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно

полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

8.5. Обработка Банком персональных данных в целях продвижения товаров, работ, услуг на рынке путём осуществления прямых контактов с потенциальным потребителем с помощью средств связи допускается только при условии предварительного согласия субъекта персональных данных.

Банк обязан немедленно прекратить по требованию субъекта персональных данных обработку его персональных данных в вышеуказанных целях.

8.6. В Банке запрещается принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы, за исключением случаев, предусмотренных Федеральными законами, или при наличии согласия в письменной форме субъекта персональных данных.

8.7. Если субъект персональных данных считает, что Банк осуществляет обработку его персональных данных с нарушением требований Федерального закона №152-ФЗ или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие Банка в Уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

9. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

9.3. Безопасность персональных данных, обрабатываемых Банком, обеспечивается реализацией правовых, организационных и технических мер, необходимых и достаточных для обеспечения требований Федерального законодательства в области защиты персональных данных

9.4. Для целенаправленного создания в Банке неблагоприятных условий и труднопреодолимых препятствий для нарушителей, пытающихся осуществить несанкционированный доступ к персональным данным в целях овладения ими, их видоизменения, уничтожения, заражения вредоносной компьютерной программой, подмены и совершения иных несанкционированных действий, Банком применяются следующие организационно-технические меры:

- ✓ назначение должностных лиц, ответственных за организацию обработки и защиты персональных данных;
- ✓ ограничение и регламентация состава работников, имеющих доступ к персональным данным;
- ✓ ознакомление работников с требованиями Федерального законодательства и нормативных документов Банка по обработке и защите персональных данных;

- ✓ обеспечение учёта и хранения материальных носителей информации и их обращения, исключающее хищение, подмену, несанкционированное копирование и уничтожение;
- ✓ определение угроз безопасности персональных данных при их обработке, формирование на их основе моделей угроз и постоянное поддержание их актуальности;
- ✓ разработка на основе модели угроз системы защиты персональных данных для соответствующего класса информационных систем;
- ✓ регулярная проверка готовности и эффективности используемых средств защиты информации;
- ✓ реализация разрешительной системы доступа пользователей к информационным ресурсам, программно-аппаратным средствам обработки и защиты информации;
- ✓ регистрация и учёт действий пользователей информационных систем персональных данных;
- ✓ парольная защита доступа пользователей к информационной системе персональных данных;
- ✓ применение средств контроля доступа к коммуникационным портам, устройствам ввода-вывода информации, съёмным машинным носителям и внешним накопителям информации;
- ✓ применение в необходимых случаях средств криптографической защиты информации для обеспечения безопасности персональных данных при передаче по открытым каналам связи и хранении на машинных носителях информации;
- ✓ осуществление антивирусного контроля, предотвращение внедрения в корпоративную сеть вредоносных программ (программ-вирусов) и программных закладок;
- ✓ применение межсетевого экранирования;
- ✓ обнаружение вторжений в корпоративную сеть Банка, нарушающих или создающих предпосылки к нарушению установленных требований по обеспечению безопасности персональных данных;
- ✓ анализ защищённости информационных систем персональных данных Банка с применением специализированных программных средств (сканеров безопасности);
- ✓ централизованное управление системой защиты персональных данных;
- ✓ резервное копирование информации;
- ✓ обеспечение восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- ✓ обучение работников, использующих средства защиты информации, применяемые в информационных системах персональных данных, правилам работы с ними;

- ✓ учёт применяемых средств защиты информации, эксплуатационной и технической документации к ним;
- ✓ использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия;
- ✓ систематическое проведение мониторинга действий пользователей, проведение разбирательств по фактам нарушения требований безопасности персональных данных;
- ✓ размещение технических средств обработки персональных данных, в пределах охраняемой территории;
- ✓ организация пропускного режима на территорию Банка, охраны помещений и собственно технических средств обработки персональных данных;
- ✓ поддержание технических средств охраны, сигнализации помещений в состоянии постоянной готовности, ведение видеонаблюдения.

10. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

10.1. Согласие на обработку персональных данных субъект представляет в профильное подразделение Банка, представляющее банковскую услугу.

10.2. Иные права и обязанности Банка, связанные с обработкой им персональных данных, определяются законодательством Российской Федерации в области персональных данных.

10.3. Должностные лица Банка, виновные в нарушении норм, регулирующие обработку и защиту персональных данных, несут материальную, дисциплинарную, административную, гражданско-правовую или уголовную ответственность в порядке, установленном Федеральными законами.

Согласовано:

Должность	Ф.И.О.	Подпись	Дата
Начальник Управления информационных технологий			
Начальник Отдела кадров			
Руководитель Службы внутреннего контроля			
Начальник Управления рисков и финансового анализа			
Начальник Юридического Управления			