Акционерное общество
«СЕВЕРГАЗБАНК»
(АО «БАНК СГБ»)

УТВЕРЖДЕНО
Правлением АО «БАНК СГБ»
(протокол от 30 марта 2022 № ____)

ПОЛИТИКА
обработки и защиты
персональных данных
в Акционерном обществе «СЕВЕРГАЗБАНК»

30 марта 2022 г. № _____
г. Вологда

1. Общие положения

1.1. Политика обработки и защиты персональных данных (далее - Политика) определяет основные положения, реализуемые при обработке Персональных данных в Банке.

1.2. Перечень терминов и условных сокращений приведен в приложении № 1.

1.3. Целью принятия Политики является выполнение требований законодательства Российской Федерации в области Персональных данных.

1.4. Политика разработана с учетом рекомендаций Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 31.07.2017 «Рекомендации по составлению документа, определяющего политику оператора в отношении обработки персональных данных, в порядке, установленном Федеральным законом «О персональных данных».

1.5. Политика распространяется на все основные, обеспечивающие и управляющие бизнес-процессы Банка, а также технологические процессы, подпроцессы, процедуры и операции, в рамках которых осуществляется Обработка Персональных данных.

1.6. Действие Политики не распространяется на отношения, возникающие при:

- обработке Персональных данных физическими лицами исключительно для личных и семейных нужд, если при этом не нарушаются права субъектов Персональных данных;

- организации хранения, комплектования, учета и использования содержащих Персональные данные документов Архивного фонда Российской Федерации и других архивных документов в соответствии с законодательством об архивном деле в Российской Федерации;

- обработке Персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну.

Политика не регулирует взаимоотношения в части применения положений стандартов Комитета по безопасности индустрии платежных карт (PCI SSC).

1.7. Политика обязательна для применения всеми работниками головного офиса, филиалов и представительств Банка, независимо от занимаемой ими должности, включая руководство, а также посетителями/пользователями информационных ресурсов Банка.

1.8. Политика, а также все изменения и дополнения к ней принимаются и утверждаются в установленном в Банке порядке и действуют до замены их новыми.

1.9. Изменения в Политику могут вноситься в случаях изменения законодательства Российской Федерации о Персональных данных и принятых в соответствии с ним нормативных правовых актов, существенного изменения в структуре технологических и бизнес-процессов, в рамках которых осуществляется Обработка Персональных данных, изменения организационной структуры Банка и полномочий Участников процесса, а также по результатам анализа инцидентов информационной безопасности, актуальности, достаточности и эффективности используемых мер обеспечения информационной безопасности, по результатам проведения внутренних аудитов информационной безопасности и других контрольных мероприятий.

1.10. В случае изменения законодательства Российской Федерации о Персональных данных и принятых в соответствии с ним нормативных правовых актов, изменения или введения в действие стандартов, нормативно-методических рекомендаций, требований уполномоченных органов Политика применяется в части, не противоречащей вновь принятым нормативным правовым документам.

1.11. Внутренние нормативные и распорядительные документы Банка, затрагивающие вопросы Обработки и защиты Персональных данных, должны разрабатываться с учетом положений Политики и не противоречить им.

1.12. Политика является общедоступной и подлежит размещению на официальном сайте Банка.

1.13.При разработке Политики использовались документы, перечень которых приведен в приложении № 2.

2. Цели сбора и общие принципы обработки Персональных данных

2.1. Обработка Персональных данных должна ограничиваться достижением законных, конкретных и заранее определенных целей. Не допускается Обработка Персональных данных, несовместимая с целями сбора Персональных данных.

2.2. Обработка Персональных данных осуществляется Банком в целях:

- исполнения требований законодательства Российской Федерации;

- осуществления банковских операций и иной деятельности в соответствии с Уставом и выданными Банку лицензиями;

- заключения с субъектами Персональных данных, в том числе по инициативе субъектов Персональных данных, любых договоров и их дальнейшего исполнения*;

(*В том числе оценка кредитоспособности/платежеспособности при рассмотрении заявок субъекта Персональных данных на предоставление банковских услуг.)

- проведения Банком акций, опросов, маркетинговых и иных исследований;

- обеспечения участия субъектов Персональных данных в программах лояльности, акциях, опросах, маркетинговых и иных исследованиях, организованных Банком и/или третьими лицами, как совместно, так и самостоятельно, получения предусмотренных

условиями таких программ, акций и иных маркетинговых мероприятий привилегий и специальных предложений;

- продвижения услуг (продуктов, работ, имущественных прав) Банка, информирования субъектов Персональных данных о предложениях по продуктам и услугам Банка и/или партнеров Банка, включая оповещение субъектов Персональных данных об изменениях в продуктовой линейке, направление адресных продуктовых предложений;

- ведения кадровой работы и организации учета работников Банка;

- регулирования трудовых и иных, непосредственно связанных с ними отношений, включая применение мер поощрения работников;

- распространения Персональных данных работников Банка, при этом Персональные данные распространяются только с письменного согласия работника на Обработку Персональных данных, разрешенных им для Распространения. Персональные данные иных категорий субъектов Персональных данных Банком не распространяются;

- привлечения и отбора кандидатов на работу;

- ведения единого справочника корпоративных телефонов и корпоративной электронной почты на корпоративном информационном портале Банка;

- организации и обеспечения пропускного и внутриобъектового режима;

- формирования отчетности, в том числе для предоставления государственным органам;

- осуществления Банком управленческой и административно-хозяйственной деятельности, в том числе осуществления технического управления интернет-сервисами Банка, а также проведения анализа функционирования и принятия мер для улучшения работы интернет-сервисов Банка;

- ведения учетных записей (личных кабинетов) клиентов Банка в приложениях и интернет-сервисах Банка;

- проверки платежеспособности для принятия решения о кредитовании;

- выявления случаев мошенничества, хищения денежных средств со счетов, иных противоправных действий, предотвращения таких противоправных действий в дальнейшем и локализации последствий таких действий;

- достижения иных целей, предусмотренных законодательством Российской Федерации, и осуществления выполнения возложенных законодательством Российской Федерации на Банк функций, полномочий и обязанностей (включая предусмотренные законодательством Российской Федерации о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма, о единой системе идентификации и аутентификации и единой биометрической системе, но не ограничиваясь этим).

2.3. Банк осуществляет обработку Персональных данных на основе следующих принципов:

- законности, добросовестности, справедливости и конфиденциальности при обработке Персональных данных;

- законности целей и способов обработки Персональных данных;

- соответствия целей обработки Персональных данных целям, заранее определенным и заявленным при сборе Персональных данных, а также полномочиям Банка;

- соответствия объема и характера обрабатываемых Персональных данных, способов обработки Персональных данных целям обработки Персональных данных;

- достоверности Персональных данных, их достаточности для целей обработки, недопустимости обработки Персональных данных, избыточных по отношению к целям, заявленным при сборе Персональных данных;

- недопустимости объединения созданных для несовместимых между собой целей баз данных Информационных систем Персональных данных;

- соблюдения запретов и условий, установленных работником Банка в согласии на обработку Персональных данных, разрешенных им для распространения, в соответствии с Федеральным законом «О персональных данных».

2.4. Хранение Персональных данных осуществляется в Банке в форме, позволяющей определить субъекта Персональных данных, не дольше, чем этого требуют цели их обработки, если иной срок хранения Персональных данных не установлен законодательством Российской Федерации или договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект Персональных данных, и они подлежат Уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

3. Цели, задачи и общие принципы обеспечения безопасности Персональных данных

3.1. Персональные данные (за исключением Персональных данных, подлежащих раскрытию в соответствии с требованиями законодательства Российской Федерации, и Персональных данных, являющихся разрешенными для Распространения в соответствии с Федеральным законом «О персональных данных»), обрабатываемые Банком, отнесены к конфиденциальной информации в соответствии с официально утвержденным в Банке перечнем информации, в отношении которой Банком установлен режим конфиденциальности, и подлежат защите.

3.2. Основной целью обеспечения безопасности Персональных данных является минимизация рисков и возможного ущерба (потерь) от их реализации, возникших вследствие возможной реализации внутренних и внешних угроз информационной безопасности Персональных данных и уязвимостей объектов защиты.

3.3. Основной задачей обеспечения безопасности Персональных данных при их Обработке в Банке является противостояние угрозам информационной безопасности Персональных данных, в том числе предотвращение утечки Персональных данных по техническим каналам, несанкционированного доступа к ним, предупреждение преднамеренных программно-технических воздействий с целью их разрушения (Уничтожения), искажения в процессе обработки, разглашения, передачи и хранения.

3.4. Основным условием реализации целей и задач обеспечения безопасности Персональных данных является обеспечение необходимого и достаточного уровня защиты Персональных данных.

3.5. Защита Персональных данных осуществляется в Банке на основе следующих принципов:

3.5.1. Законность – защита Персональных данных основывается на положениях и требованиях применимых законов, подзаконных актов, стандартов, нормативно-методических документов по защите Персональных данных.

3.5.2. Системность – системный подход к построению системы защиты Персональных данных предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения безопасности Персональных данных Банком.

3.5.3. Комплексность – безопасность Персональных данных обеспечивается комплексом правовых, организационных и технических мер, реализованных Банком.

3.5.4. Своевременность – принимаемые Банком меры по обеспечению безопасности Персональных данных должны носить упреждающий характер.

3.5.5. Непрерывность – защита Персональных данных обеспечивается на всех этапах их обработки и во всех режимах функционирования систем обработки Персональных данных, в том числе при проведении ремонтных и регламентных работ.

3.5.6. Преемственность и непрерывность совершенствования – предполагают постоянное совершенствование мер и средств защиты Персональных данных на основании результатов анализа функционирования системы защиты и автоматизированных Информационных систем Персональных данных с учетом выявления новых способов и средств реализации угроз безопасности Персональных данных, положительного отечественного и зарубежного опыта в сфере защиты Персональных данных. Банк должен определить действия, необходимые для устранения причин потенциальных несоответствий требованиям по безопасности Персональных данных с целью предотвратить их повторное появление. Предпринимаемые предупреждающие действия должны соответствовать возможным негативным последствиям.

3.5.7. Разумная достаточность и адекватность – состояние и стоимость реализации мер защиты должны быть соизмеримы с рисками, связанными с Обработкой и характером защищаемых Персональных данных.

3.5.8. Персональная ответственность – ответственность за обеспечение безопасности Персональных данных в Банке возлагается на каждого работника в пределах его полномочий.

3.5.9. Минимизация полномочий – предоставление и использование прав доступа к Персональным данным должно быть управляемо и ограничено. Доступ к Персональным данным предоставляется работникам Банка только в объеме, необходимом для выполнения их должностных обязанностей.

3.5.10. Профессионализм и специализация – реализация мер по обеспечению безопасности Персональных данных и эксплуатации системы защиты должна осуществляться квалифицированными работниками Банка.

3.5.11. Знание и мотивация лиц, допущенных к Обработке Персональных данных, – Банк должен обладать информацией о своих работниках (кандидатах на работу) и пользователях его информационных ресурсов, позволяющей минимизировать вероятность реализации угроз безопасности Персональных данных, источники которых связаны с человеческим фактором. Банк должен реализовать кадровую политику (тщательный подбор персонала и мотивация работников), позволяющую исключить или минимизировать возможность нарушения безопасности Персональных данных своими работниками.

3.5.12. Наблюдаемость и оцениваемость обеспечения безопасности Персональных данных – принимаемые Банком меры по обеспечению безопасности Персональных данных должны быть спланированы так, чтобы результат их применения был прозрачен и мог быть оценен Регуляторами в пределах своих полномочий.

3.5.13. Обязательность оценки и контроля – неотъемлемой частью работ по защите Персональных данных является оценка эффективности системы защиты Персональных данных. С целью своевременного выявления и пресечения попыток нарушения установленных правил обеспечения информационной безопасности Персональных данных в Банке должны быть определены процедуры для постоянного контроля использования систем обработки и защиты Персональных данных, а результаты контроля должны регулярно анализироваться.

4. Объем и категории обрабатываемых Персональных данных, категории субъектов Персональных данных

4.1. Содержание и объем обрабатываемых Персональных данных должны соответствовать заявленным целям обработки. обрабатываемые Персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

4.2. В соответствии с Федеральным законом «О персональных данных» и степенью тяжести последствий потери свойств безопасности Персональных данных для субъектов Персональных данных, Банк выделяет следующие категории Персональных данных:

- Персональные данные, отнесенные к биометрическим Персональным данным (сведения, которые характеризуют физиологические и биологические особенности человека, на основе которых можно установить его личность и которые используются Банком для установления личности субъекта Персональных данных);

- Персональные данные, отнесенные к специальным категориям Персональных данных (расовая, национальная принадлежность, политические взгляды, религиозные или философские убеждения, состояние здоровья, интимная жизнь);

- Персональные данные, разрешенные субъектом Персональных данных для Распространения в порядке, предусмотренном Федеральным законом «О персональных данных».

- Персональные данные, которые не могут быть отнесены к биометрическим, специальным и разрешенным субъектом Персональных данных для Распространения категориям Персональных данных.

4.3. Банк устанавливает правила (порядок) работы с Персональными данными, в том числе допустимые случаи обработки специальных категорий и биометрических Персональных данных, определяет для каждой цели обработки и категории субъектов Персональных данных содержание обрабатываемых в Банке Персональных данных и утверждает перечни Персональных данных отдельными локальными актами.

4.4. Банк обрабатывает Персональные данные следующих категорий субъектов Персональных данных:

- физические лица, входящие в органы управления Банка;

- физические лица, являющиеся работниками Банка (в том числе работники Банка, Персональные данные которых разрешены ими для Распространения, а их Обработка не нарушает их прав и соответствует требованиям, установленным законодательством Российской Федерации о Персональных данных), и их близкие родственники (в соответствии с требованиями трудового законодательства Российской Федерации);

- физические лица, являющиеся кандидатами на замещение вакантных должностей;

- физические лица, Обработка Персональных данных которых осуществляется для отражения в отчетных документах о деятельности Банка в соответствии с требованиями законодательства Российской Федерации: аффилированные лица или руководитель/работник юридического лица, являющегося аффилированным лицом по отношению к Банку, инсайдеры, акционеры и прочие;

- физические лица, являющиеся контрагентами (партнерами, клиентами) Банка, а также их выгодоприобретателями и/или бенефициарными владельцами, залогодателями, поручителями, принципалами и/или иными лицами, участвующими в договорных отношениях по заключению, исполнению и прекращению договоров с контрагентами (партнерами, клиентами) Банка;

- физические лица, намеревающиеся приобрести продукты и/или услуги Банка, а также приобретшие или намеревающиеся приобрести продукты и/или услуги третьих лиц при посредничестве Банка;

- физические лица, обработка Персональных данных которых осуществляется Банком для достижения целей, предусмотренных законодательством Российской Федерации, или для осуществления и выполнения возложенных законодательством Российской Федерации на Банк функций, полномочий и обязанностей;

- физические лица, в отношении которых осуществляются мероприятия по обеспечению и контролю порядка доступа на объекты (территорию) Банка;

- физические лица – посетители/пользователи официального сайта Банка в информационно-телекоммуникационной сети «Интернет»;

- физические лица, состоящие с Банком в иных отношениях, выразившие согласие на обработку Банком их Персональных данных;

- физические лица, ранее входившие в одну из указанных выше категорий, в случае если это установлено законодательством Российской Федерации или международным законодательством, и в течение срока, установленного законодательством;

- физические лица, являющиеся представителями указанных выше физических и юридических лиц.

5. Права субъектов Персональных данных

5.1. Право субъекта Персональных данных на доступ к его персональным данным

5.1.1. Субъект Персональных данных имеет право на получение сведений, указанных в пункте 5.2, за исключением случаев, предусмотренных пунктом 5.3. Субъект Персональных данных вправе требовать от Банка 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.

5.1.2. Сведения, указанные в пункте 5.2, должны быть предоставлены субъекту Персональных данных Банком 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.

5.1.3. Сведения, указанные в пункте 5.2, предоставляются субъекту Персональных данных или его представителю Банком при обращении либо при получении запроса субъекта Персональных данных или его представителя. Запрос должен 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 Банком (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки Персональных данных Банком, подпись субъекта Персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

5.1.4. В случае если сведения, указанные в пункте 5.2, а также обрабатываемые Персональные данные были предоставлены для ознакомления субъекту Персональных данных по его запросу, субъект Персональных данных вправе обратиться повторно в Банк или направить ему повторный запрос в целях получения сведений, указанных в пункте 5.2, и ознакомления с такими Персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект Персональных данных.

5.1.5. Субъект Персональных данных вправе обратиться повторно в Банк или направить ему повторный запрос в целях получения сведений, указанных в пункте 5.2, а также в целях ознакомления с обрабатываемыми Персональными данными до истечения срока, указанного в пункте 5.1.4, в случае если такие сведения и/или обрабатываемые Персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения

первоначального обращения. Повторный запрос наряду со сведениями, указанными в пункте 5.1.3, должен содержать обоснование направления повторного запроса.

5.1.6. Банк вправе отказать субъекту Персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным пунктами 5.1.4 и 5.1.5. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса возлагается на Банк.

5.2. Субъект Персональных данных имеет право на получение информации, касающейся обработки его Персональных данных, в том числе содержащей:

5.2.1. Подтверждение факта обработки Персональных данных Банком.

5.2.2. Правовые основания и цели обработки Персональных данных.

5.2.3. Цели и применяемые Банком способы обработки Персональных данных.

5.2.4. Наименование и место нахождения Банка, сведения о лицах (за исключением работников Банка), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Банком или на основании федерального закона.

5.2.5. Обрабатываемые Персональные данные, относящиеся к соответствующему субъекту Персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен Федеральным законом «О персональных данных».

5.2.6. Сроки Обработки Персональных данных, в том числе сроки их хранения.

5.2.7. Порядок осуществления субъектом Персональных данных прав, предусмотренных Федеральным законом «О персональных данных».

5.2.8. Информацию об осуществленной или о предполагаемой трансграничной передаче Персональных данных.

5.2.9. Наименование или фамилию, имя, отчество и адрес лица, осуществляющего Обработку Персональных данных по поручению Банка, если Обработка поручена или будет поручена такому лицу.

5.2.10. Иные сведения, предусмотренные Федеральным законом «О персональных данных» или другими федеральными законами Российской Федерации.

5.3. Право субъекта Персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами, в том числе если:

5.3.1. Обработка Персональных данных осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма.

5.3.2. Доступ субъекта Персональных данных к его Персональным данным нарушает права и законные интересы третьих лиц.

5.4. Права субъектов Персональных данных при обработке их Персональных данных в целях продвижения товаров, работ, услуг

5.4.1. Обработка Персональных данных в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи допускается только при условии предварительного согласия субъекта Персональных данных. Указанная обработка Персональных данных признается осуществляемой без предварительного согласия субъекта Персональных данных, если Банк не докажет, что такое согласие было получено.

5.4.2. Банк обязан немедленно прекратить по требованию субъекта Персональных данных Обработку его Персональных данных, указанную в пункте 5.4.1.

5.5. Права субъектов Персональных данных при принятии решений на основании исключительно Автоматизированной Обработки их Персональных данных

5.5.1. 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 пунктом 5.5.2.

5.5.2. Решение, порождающее юридические последствия в отношении субъекта Персональных данных или иным образом затрагивающее его права и законные интересы, может быть принято на основании исключительно Автоматизированной Обработки его Персональных данных только при наличии согласия в письменной форме субъекта Персональных данных или в случаях, предусмотренных федеральными законами, устанавливающими также меры по обеспечению соблюдения прав и законных интересов субъекта Персональных данных.

5.5.3. Банк обязан разъяснить субъекту Персональных данных порядок принятия решения на основании исключительно Автоматизированной Обработки его Персональных данных и возможные юридические последствия такого решения, предоставить возможность заявить возражение против такого решения, а также разъяснить порядок защиты субъектом Персональных данных своих прав и законных интересов.

5.5.4. Банк обязан рассмотреть возражение, указанное в пункте 5.5.3, в течение тридцати дней со дня его получения и уведомить субъекта Персональных данных о результатах рассмотрения такого возражения.

5.6. Право на обжалование действий или бездействия Банка

5.6.1. Если субъект Персональных данных считает, что Банк осуществляет обработку его Персональных данных с нарушением требований Федерального закона «О персональных данных» 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.

5.6.2. 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.

6. Обязанности Банка при сборе Персональных данных

6.1. При сборе Персональных данных Банк обязан предоставить субъекту Персональных данных по его просьбе информацию, предусмотренную пунктом 5.2.

6.2. Если предоставление Персональных данных является обязательным в соответствии с федеральными законами Банк обязан разъяснить субъекту Персональных данных юридические последствия отказа предоставить его Персональные данные.

6.3. Если Персональные данные получены не от субъекта Персональных данных, Банк, за исключением случаев, предусмотренных пунктом 6.4, до начала Обработки таких Персональных данных обязан предоставить субъекту Персональных данных следующую информацию:

- наименование и адрес Банка;
- цель Обработки Персональных данных и ее правовое основание;
- предполагаемые пользователи Персональных данных;
- установленные Федеральным законом «О персональных данных» права субъекта Персональных данных;
- источник получения Персональных данных.

6.4. Банк освобождается от обязанности предоставить субъекту Персональных данных сведения, предусмотренные пунктом 6.3, в случаях если:

- субъект Персональных данных уведомлен об осуществлении Банком Обработки его Персональных данных;

- Персональные данные получены Банком на основании федеральных законов или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект Персональных данных;

- обработка Персональных данных, разрешенных для Распространения, осуществляется с соблюдением запретов и условий, предусмотренных статьей 10.1 Федерального закона «О персональных данных»;

- Банк осуществляет Обработку Персональных данных для статистических или иных исследовательских целей либо научной или иной творческой деятельности, если при этом не нарушаются права и законные интересы субъекта Персональных данных;

- предоставление субъекту Персональных данных сведений, предусмотренных пунктом 6.3, нарушает права и законные интересы третьих лиц.

6.5. При сборе Персональных данных, в том числе посредством информационно-телекоммуникационной сети «Интернет», Банк обязан обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение Персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, указанных в пунктах 2, 3, 4, 8 части 1 статьи 6 Федерального закона «О персональных данных».

6.6. Лицо, допущенное к Обработке Персональных данных.

В функции лица, допущенного к Обработке Персональных данных в Банке, входят:

- знание и неукоснительное выполнение требований законодательства Российской Федерации о Персональных данных, Политики, внутренних нормативных документов Банка, регламентирующих порядок и методики Обработки и защиты Персональных данных;

- осознание актуальных угроз безопасности Персональных данных и принятие мер по предотвращению и преодолению их возможных последствий;

- Обработка Персональных данных только в рамках выполнения своих должностных обязанностей;

- неразглашение Персональных данных, полученных в результате выполнения своих должностных обязанностей, а также ставших ему известными по роду своей деятельности;

- пресечение действий других лиц, которые могут привести к разглашению (Уничтожению, искажению) Персональных данных;

- выявление фактов разглашения (Уничтожения, искажения) Персональных данных и информирование об этом ответственных подразделений;

- выполнение иных функции, предусмотренных для лица, допущенного к обработке Персональных данных, должностной инструкцией.

6.7. Обязанности и ответственность Участников процесса регламентируются

должностными инструкциями и внутренними нормативными/распорядительными документами Банка, устанавливающими правила обращения с конфиденциальной информацией в Банке.

7. Правовые основания обработки Персональных данных

7.1. Правовым основанием Обработки Персональных данных является совокупность нормативно-правовых актов, во исполнение которых и в соответствии с которыми Банк осуществляет Обработку Персональных данных, в частности:

- Конституция Российской Федерации;

- Гражданский кодекс Российской Федерации;

- Налоговый кодекс Российской Федерации;

- Трудовой кодекс Российской Федерации;

- Федеральный закон от 02.12.1990 № 395-1 «О банках и банковской деятельности»;

- Федеральный закон от 26.12.1995 № 208-ФЗ «Об акционерных обществах»;

- Федеральный закон от 01.04.1996 № 27-ФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования»;

- Федеральный закон от 22.04.1996 № 39-ФЗ «О рынке ценных бумаг»;

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

- Федеральный закон от 30.12.2004 № 218-ФЗ «О кредитных историях»;

- Федеральный закон от 27.07.2010 № 224-ФЗ «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской федерации»;

- Федеральный закон от 27.06.2011 № 161-ФЗ «О национальной платежной системе»;

- Федеральный закон от 06.12.2011 № 402-ФЗ «О бухгалтерском учете»;

- Федеральный закон от 21.12.2013 № 353-ФЗ «О потребительском кредите (займе)»;

- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

- Методические рекомендации по выполнению законодательных требований при Обработке Персональных данных в организациях банковской системы Российской Федерации, разработанные совместно Банком России, Ассоциацией российских банков и Ассоциацией региональных банков России (Ассоциация «Россия») и опубликованные в совместном письме от 28.06.2010 № 01-23/3148 «О введении в действие Стандартов и Рекомендаций в области стандартизации Банка России по вопросам информационной безопасности банковской организации Российской Федерации»;

- «Устав «Газпромбанк» (Акционерное общество)» Банк ГПБ (АО)», утвержденный решением Общего собрания акционеров от 03.09.2020 (протокол № 02) (в действующей редакции);

- заключенные с Банком договоры (соглашения), стороной которых либо выгодоприобретателем/поручителем по которым является субъект Персональных данных;

- а также иные нормативно-правовые акты, действие которых распространяется на деятельность Банка.

7.2. Кроме этого, Обработка Персональных данных возможна в следующих случаях:

7.2.1. 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.

7.2.2. Осуществляется Обработка Персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральными законами и принятыми в соответствии с ними нормативными-правовыми актами.

7.2.3. 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.

7.2.4. Обработка Персональных данных осуществляется в связи с участием лица в конституционном, гражданском, административном, уголовном судопроизводстве, судопроизводстве в арбитражных судах.

7.2.5. Обработка Персональных данных необходима для исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве.

7.2.6. Обработка Персональных данных необходима для защиты жизни, здоровья, или иных жизненно важных интересов субъекта Персональных данных, если получение согласия субъекта персональных данных невозможно.

7.2.7. Обработка Персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей.

7.3. Обработка Персональных данных возможна в случае получения согласия субъекта Персональных данных на обработку Персональных данных, в том числе отдельного согласия на Распространение.

7.3.1. Субъект Персональных данных принимает решение о предоставлении его Персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку Персональных данных, в том числе на Распространение, должно быть конкретным, информированным и сознательным.

7.3.2. 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 федеральными законами или нормативными актами Банка.

При этом согласие на обработку Персональных данных, разрешенных для Распространения, должно быть дано работником непосредственно в Банк отдельно от иных согласий на Обработку Персональных данных и исключительно в письменной форме.

В случае получения согласия на обработку Персональных данных от представителя субъекта Персональных данных полномочия данного представителя на дачу согласия от имени субъекта Персональных данных проверяются Банком.

7.3.3. Согласие на обработку Персональных данных может быть отозвано субъектом Персональных данных. В случае отзыва субъектом Персональных данных согласия на обработку Персональных данных Банк вправе продолжить обработку Персональных данных без согласия субъекта Персональных данных при наличии оснований, указанных в пунктах 2–11 части 1 статьи 6, части 2 статьи 10 Федерального закона «О персональных данных».

8. Порядок и условия обработки Персональных данных

8.1. Обработка Персональных данных в Банке может осуществляться в виде автоматизированной обработки Персональных данных, обработки без использования средств автоматизации, а также смешанной обработки Персональных данных.

8.2. Содержание и объем обрабатываемых Персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые Персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

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

8.4. Персональные данные хранятся и обрабатываются Банком в течение сроков, необходимых для достижения целей обработки Персональных данных или утраты необходимости в достижении этих целей (если иное не предусмотрено федеральными законами), указанных в согласии субъекта Персональных данных, выполнения возложенных законодательством Российской Федерации на Банк функций, полномочий и обязанностей,

защиты прав и законных интересов Банка и третьих лиц, в том числе в рамках судебного и административного производства.

8.5. Передача (в том числе трансграничная) Персональных данных третьим лицам может осуществляться с согласия субъекта Персональных данных, в том числе путем поручения Банка на обработку Персональных данных третьим лицом, либо в соответствии с федеральным законом или в целях исполнения договора, стороной которого/выгодоприобретателем или поручителем по которому является субъект Персональных данных либо другому оператору при наличии согласия субъекта Персональных данных. Трансграничная передача Персональных данных на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов Персональных данных, может осуществляться при наличии письменного согласия субъекта на трансграничную передачу его Персональных данных.

8.6.Банк вправе передавать Персональные данные государственным органам, органам следствия и дознания, иным уполномоченным органам по основаниям, предусмотренным действующим законодательством Российской Федерации.

8.7. Банк вправе поручить обработку Персональных данных третьему лицу с согласия субъекта Персональных данных, если иное не предусмотрено законодательством Российской Федерации. Определение цели (ей) обработки Персональных данных, состава Персональных данных, подлежащих обработке, действий (операций), совершаемых с Персональными данными, осуществляется Банком и не может быть поручено третьему лицу. В случае поручения обработки Персональных данных субъектов другому лицу в договоре (соглашении) должны быть определены цель(ли) обработки Персональных данных, состав Персональных данных, подлежащий обработке, действия (операции), совершаемые с Персональными данными, должны быть указаны требования к защите обрабатываемых Персональных данных в соответствии со статьей 19 Федерального закона «О персональных данных», в том числе установлена обязанность лица, осуществляющего обработку Персональных данных по поручению Банка, должны соблюдаться конфиденциальность Персональных данных и обеспечиваться безопасность Персональных данных при их обработке, а также соблюдаться принципы и правила обработки Персональных данных, предусмотренные Федеральным законом «О персональных данных».

8.8. Условиями прекращения обработки Персональных данных могут являться достижение целей обработки Персональных данных, истечение срока действия согласия или отзыв согласия субъекта Персональных данных на обработку его Персональных данных, требование о прекращении обработки Персональных данных, ранее разрешенных для Распространения, решение суда, а также выявление неправомерной обработки Персональных данных.

9. Порядок актуализации, исправления, удаления и уничтожения Персональных данных

9.1. В случае выявления неправомерной обработки Персональных данных при обращении субъекта Персональных данных или его представителя либо по запросу субъекта Персональных данных или его представителя либо уполномоченного органа по защите прав субъектов Персональных данных Банк обязан осуществить Блокирование неправомерно

обрабатываемых Персональных данных, относящихся к этому субъекту Персональных данных, или обеспечить их Блокирование (если обработка Персональных данных осуществляется другим лицом, действующим по поручению Банка) с момента такого обращения или получения указанного запроса на период проверки. Порядок реагирования на обращения и запросы субъектов Персональных данных и их представителей, уполномоченных органов по вопросам обработки Персональных данных устанавливается отдельным нормативным документом Банка в соответствии с Политикой.

9.2. В случае подтверждения факта неточности Персональных данных Банк на основании сведений, представленных субъектом Персональных данных или его представителем, или иных необходимых документов обязан уточнить персональные данные либо обеспечить их уточнение (если обработка Персональных данных осуществляется другим лицом, действующим по поручению Банка) в течение семи рабочих дней со дня представления таких сведений и снять Блокирование Персональных данных.

9.3. В случае выявления неправомерной обработки Персональных данных, осуществляемой Банком или лицом, действующим по поручению Банка, Банк в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку Персональных данных или обеспечить прекращение неправомерной обработки Персональных данных лицом, действующим по поручению Банка.

9.3.1. В случае если обеспечить правомерность обработки Персональных данных невозможно, Банк в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки Персональных данных, обязан уничтожить такие Персональные данные или обеспечить их Уничтожение.

9.3.2. Об устранении допущенных нарушений или об Уничтожении Персональных данных Банк обязан уведомить субъекта Персональных данных или его представителя, а в случае, если обращение субъекта Персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов Персональных данных были направлены уполномоченным органом по защите прав субъектов Персональных данных, также указанный орган.

9.4. В случае достижения цели обработки Персональных данных Банк обязан прекратить обработку Персональных данных или обеспечить ее прекращение (если обработка Персональных данных осуществляется другим лицом, действующим по поручению Банка) и уничтожить Персональные данные или обеспечить их Уничтожение (если Обработка Персональных данных осуществляется другим лицом, действующим по поручению Банка) в срок, не превышающий тридцати дней с даты достижения цели обработки Персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект Персональных данных, иным соглашением между Банком и субъектом Персональных данных либо если Банк не вправе осуществлять обработку Персональных данных без согласия субъекта Персональных данных на основаниях, предусмотренных федеральными законами.

9.5. В случае отзыва субъектом Персональных данных согласия на обработку Персональных данных Банк обязан прекратить их обработку или обеспечить прекращение такой обработки (если обработка Персональных данных осуществляется другим лицом,

действующим по поручению Банка) и в случае если сохранение Персональных данных более не требуется для целей обработки Персональных данных, уничтожить Персональные данные или обеспечить их Уничтожение (если обработка Персональных данных осуществляется другим лицом, действующим по поручению Банка) в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект Персональных данных, иным соглашением между Банком и субъектом Персональных данных либо если Банк не вправе осуществлять обработку Персональных данных без согласия субъекта Персональных данных на основаниях, предусмотренных федеральными законами.

9.6. В случае отсутствия возможности Уничтожения Персональных данных в течение срока, указанного в пунктах 9.3, 9.4, 9.5, Банк осуществляет Блокирование таких Персональных данных или обеспечивает их Блокирование (если обработка Персональных данных осуществляется другим лицом, действующим по поручению Банка) и обеспечивает Уничтожение Персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

9.7. Банк обязан прекратить обработку Персональных данных, разрешенных для Распространения, в течение трех рабочих дней с момента получения письменного требования работника Банка или в срок, указанный во вступившем в законную силу решении суда, а если такой срок в решении суда не указан, то в течение трех рабочих дней с момента вступления решения суда в законную силу.

10. Сведения о реализуемых требованиях к обеспечению безопасности Персональных данных

10.1. Банк для выполнения своих обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, в частности для обеспечения безопасности и защиты Персональных данных от неправомерного или случайного доступа к ним, Уничтожения, изменения, Блокирования, копирования, Предоставления, Распространения Персональных данных, а также от иных неправомерных действий в отношении Персональных данных принимает следующие правовые, организационные и технические меры:

- инвентаризация Информационных систем Персональных данных, хранилищ и картотек, содержащих Персональные данные;

- оценка наличия основания для обработки Персональных данных каждой категории субъектов и каждой категории данных;

- издание и опубликование для неограниченного круга лиц Политики;

- разработка пакета локальных актов по вопросам обработки и защиты Персональных данных, ознакомление работников Банка (их представителей), пользователей Информационных систем Персональных данных и/или обучение указанных лиц;

- корректировка бизнес-процессов, связанных с обработкой Персональных данных;

- определение актуальных угроз и уровня защищенности;

- моделирование угроз для каждой Информационной системы Персональных данных;

- оценка эффективности принимаемых мер по обеспечению безопасности Персональных данных до ввода в эксплуатацию Информационной системы Персональных данных;

- техническое проектирование и развертывание системы защиты Персональных данных;

- применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации. При выборе средств защиты информации для системы защиты Персональных данных Банк руководствуется нормативными правовыми актами Регуляторов во исполнение части 4 статьи 19 Федерального закона «О персональных данных»;

- обнаружение фактов несанкционированного доступа к Персональным данным и принятие мер;

- обнаружение, предупреждение и ликвидация последствий компьютерных атак на Информационные системы Персональных данных и реагирование на компьютерные инциденты в них;

- установление правил доступа к Персональным данным, обрабатываемым в Информационной системе Персональных данных, в Информационных системах Персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с Персональными данными;

- учет лиц, допущенных к обработке Персональных данных;

- учет машинных носителей Персональных данных;

- контроль за принимаемыми мерами по обеспечению безопасности Персональных данных.

11. Заключительные положения

11.1. Политика вступает в силу с даты ее утверждения Правлением АО «БАНК СГБ».

Начальник
Управления информационной безопасности
Департамента безопасности **В.В. Художилов**

Приложение № 1
к «Политике
обработки и защиты персональных данных
в Акционерном обществе «СЕВЕРГАЗБАНК»
от 30 марта 2022 г. N_____

Перечень терминов и условных сокращений

Автоматизированная обработка Персональных данных – обработка Персональных данных с помощью средств вычислительной техники.

Банк – Акционерное общество «СЕВЕРГАЗБАНК», АО «БАНК СГБ».

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 технологических средств.

Обработка Персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без их использования с Персональными данными. обработка Персональных данных Банком включает в себя в том числе сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (Распространение, предоставление, доступ), Блокирование, удаление, Уничтожение Персональных данных.

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту Персональных данных).

Персональные данные, разрешенные субъектом Персональных данных для Распространения, – персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом Персональных данных путем дачи согласия на Обработку Персональных данных, разрешенных субъектом Персональных данных для распространения в порядке, предусмотренном Федеральным законом «О персональных данных».

Распространение Персональных данных (Распространение) – действия, направленные на раскрытие Персональных данных неопределенному кругу лиц.

Регуляторы – в соответствии с Федеральным законом «О персональных данных» функции регуляторов осуществляют Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор), Федеральная служба безопасности Российской Федерации (ФСБ России), Федеральная служба по технологическому и экспортному контролю (ФСТЭК России).

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

Участники процесса – самостоятельные структурные подразделения головного офиса, филиалов, дирекций, подразделений, представительств Банка (их работники), которые участвуют в процессе обработки и/или защиты Персональных данных, то есть имеют здесь определенные права и обязанности.

Федеральный закон «О персональных данных» – Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

Приложение № 2
к «Политике
обработки и защиты персональных данных
в Акционерном обществе «СЕВЕРГАЗБАНК»
от 30 марта 2022 г. N_____

Перечень документов, использованных при разработке Политики

1. Федеральный закон от 02.12.1990 № 395-1 «О банках и банковской деятельности».
2. Федеральный закон от 26.12.1995 № 208-ФЗ «Об акционерных обществах».
3. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
4. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».
5. Указ Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении Перечня сведений конфиденциального характера».
6. Постановление Правительства Российской Федерации от 06.07.2008 № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных».
7. Постановление Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».
8. Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении Требований к защите персональных данных при их обработке в информационных системах персональных данных».
9. Методические рекомендации по выполнению законодательных требований при обработке персональных данных в организациях банковской системы Российской Федерации, разработанные совместно Банком России, Ассоциацией российских банков и Ассоциацией региональных банков России (Ассоциация «Россия») и опубликованные в совместном письме от 28.06.2010 № 01-23/3148 «О введении в действие Стандартов и Рекомендаций в области стандартизации Банка России по вопросам информационной безопасности банковской организации Российской Федерации».
10. Приказ ФСБ России и ФСТЭК России от 31.08.2010 № 416/489 «Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования».
11. «Административный регламент исполнения Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций государственной функции по осуществлению государственного контроля (надзора) за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных», утвержден приказом Министерства связи и массовых коммуникаций Российской Федерации от 14.11.2011 № 312.
12. Приказ ФСТЭК России от 18.02.2013 № 21 «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в ИСПДн».
13. Национальный стандарт Российской Федерации. «Система стандартов по информации, библиотечному и издательскому делу. Делопроизводство и архивное дело. Термины и определения» ГОСТ Р 7.0.8-2013, утвержденный приказом Росстандарта от 17.10.2013 № 1185-ст.
14. Стандарт Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» СТО БР ИББС-1.0-2014, принятый и введенный в действие Распоряжением Банка России от 17.05.2014 № Р-399.

15. «Перечень типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения», утвержден Приказом Росархива от 20.12.2019 № 236.
16. Устав Банка, утвержденный решением единственного акционера Банка от 06.02.2020 (№ 25)