

ПРАВИЛА УДАЛЕННЫХ УСЛУГ

Содержание

1.	Используемые термины и сокращения	1
2.	Общие правила	2
3.	Идентификация Клиента при пользовании Системами	3
4.	Установление полномочий Электронной подписи для Данных для электронной идентификации	5
5.	Пользование <i>PNB Internetbanka</i>	6
6.	Пользование <i>PNB Vision</i>	6
7.	Пользование <i>PNB Trade</i> (в рамках использования <i>PNB Internetbanka</i>).....	6
8.	Пользование <i>PNB SMS-Banka</i>	6
9.	<i>Пользование infoLINE</i>	6
10.	Пользование <i>PNB Chat</i>	7

1. Используемые термины и сокращения

- 1.1. **Удаленная услуга** – услуга, обеспечивающая возможность удаленного доступа к Счету, в т.ч. возможность получать информацию о Счетах и/или распоряжаться денежными средствами на Счетах, возможность заключать договоры (подавать заявки) на получение Услуг, возможность подавать в Банк заявления, заявки, распоряжения, а также осуществлять другие действия, используя автоматизированные системы Банка: *PNB Internetbanka*, *PNB Vision*, *PNB SMS-Banka*, *infoLINE*, *PNB Chat*, *PNB Trade*.
- 1.2. **Пользователь Удаленной услуги** – Клиент и/или лицо, которому Клиент в установленном Банком порядке присвоил право пользования Удаленными услугами, передав в его распоряжение Данные для электронной идентификации и Элементы авторизации.
- 1.3. **Аутентификация** – процедура распознавания, которая по Данным для электронной идентификации позволяет Банку считать, что Удаленной услугой, используя Систему, пользуется Пользователь Удаленной услуги.
- 1.4. **Банк** – AS "PNB Banka", единый регистрационный № 40003072918, юридической адрес: улица Элизабетес 15 - 2, Рига, LV-1010; адрес электронной почты: info@pnbbanka.eu; домашняя страница в Интернете: www.pnbbanka.eu; надзор за Банком осуществляет Комиссия рынка финансов и капитала (улица Кунгу 1, Рига, LV-1050; адрес электронной почты: fktk@fktk.lv).
- 1.5. **DigiPass** – электронное устройство, предусмотренное для формирования Элемента авторизации и Электронной подписи Клиента.
- 1.6. **PNB Internetbanka** – Система с адресом доступа <https://www.ib.pnbbanka.eu>, которая Клиенту обеспечивается удаленный доступ к определенным Банком Услугам.
- 1.7. **infoLINE** – Система, обеспечивающая удаленный доступ к определенным Банком Услугам, используя телефонную связь. Услуга обеспечивается, звоня на номер телефона +371 67 041 100 (в Риге) или (+ 7 495) 780 04 02 (в Москве).
- 1.8. **Кодовая карта** – пластиковая карточка, содержащая определенное количество шестизначных кодов и предусмотренная для формирования Элемента авторизации и Электронной подписи Клиента.
- 1.9. **Договор** – Договор образует поданная Клиентом заявка на получение Удаленной услуги, ОПС, в т.ч. настоящие Правила, и Тарифы.
- 1.10. **Мобильное приложение** – *PNB Internetbanka* в виде мобильного приложения, если у Клиента уже имеется доступ к *PNB Internetbanka* и в его распоряжении имеется мобильный телефон или другое устройство/устройства с операционной системой *Android* или *iOS* и доступом в Интернет.
- 1.11. **PNB Chat** – Система, которая обеспечивает Клиенту возможность с помощью определенного программного обеспечения связываться с Банком в режиме реального времени, в безопасной информационной среде.
- 1.12. **Пароль PNB Chat** – присвоенный Банком Клиенту пароль для доступа в *PNB Chat*.
- 1.13. **PNB SMS-Banka** – Система, дающая возможность с помощью короткого сообщения (SMS) получать на мобильный телефон Клиента определенную Банком информацию.
- 1.14. **PNB Trade** – Система в рамках *PNB Internetbanka*, которая предоставляет Клиенту возможность заключать с Банком сделки купли-продажи валюты.
- 1.15. **PNB Vision** – Система, установленная на компьютере Клиента, с помощью которой Клиенту обеспечивается удаленный доступ к определенным Банком Услугам.
- 1.16. **Пароль PNB Vision** – присвоенный Банком Клиенту пароль для работы в *PNB Vision*.
- 1.17. **Правила** – настоящие «Правила удаленных платежей», которые являются приложением № 3 к «Общим правилам сделок» (ОПС) Банка.
- 1.18. **Код доступа** – присвоенный Банком Клиенту пароль для доступа к *infoLINE*.
- 1.19. **Система(ы)** – автоматизированная(ые) система(ы) Банка (*PNB Internetbanka*, *PNB Vision*, *PNB SMS-Banka*, *infoLINE*, *PNB Chat*, *PNB Trade*).

- 1.20. **SMS-PIN** – уникальная последовательность определенных символов, которую генерирует Банк и сообщает Клиенту, отправляя на указанный Клиентом номер мобильного телефона в виде короткого сообщения (SMS), предусмотренная для формирования Элемента авторизации и Электронной подписи Клиента.
- 1.21. **Google Authenticator** – элемент авторизации в форме приложения, который генерирует уникальный 6 (шестизначный) код и который используется для авторизации пользователя в *PNB Internetbanka* и для формирования электронной подписи Клиента.
- 1.22. **ОПС** – утвержденные Банком «Общие правила сделок», которые регламентируют правовые отношения между Сторонами и применимы ко всем Услугам.
- 1.23. Если в данных Правилах используются термины или сокращения, которые не оговорены в данном разделе Правил, эти термины и сокращения интерпретируются согласно терминам и сокращениям, приведенным в ОПС.

2. Общие правила

- 2.1. Предоставляя Клиенту Удаленную услугу, Банк взимает с Клиента указанную в Тарифах Комиссионную плату.
- 2.2. Клиент обязуется не разглашать третьим лицам свои Данные для электронной идентификации, которые используются для работы с Системами, а также обязуется не передавать третьим лицам выданные Банком Элементы авторизации.
- 2.3. Для пользования Системами Клиент использует свои собственные (имеющиеся в распоряжении Клиента) устройства (персональный компьютер, стационарный телефон, мобильный телефон и пр.), подключенные к электронным средствам связи (интернет, телефонная сеть). Банк не несет ответственности за качество используемых Клиентом устройств и электронных средств связи, конфиденциальность и безопасность передаваемой через них информации и за перебои в их работе.
- 2.4. Для идентификации Клиента при подключении к Системам и работе с Системами используются специальные Пароли, Электронные подписи, Коды доступа и другие средства идентификации, упомянутые в настоящих Правилах.
- 2.5. Для осуществления операций с имеющимися на Счете денежными средствами Клиент подает в Банк Платежное поручение через Систему. В Платежном поручении должны быть указаны все необходимые для исполнения Платежа реквизиты, и оно должно быть подписано Электронной подписью.
- 2.6. Срок действия Платежного поручения, переданного Банку посредством Системы – 10 (*десять*) календарных дней со дня получения поручения Банком. Если на счете Клиента в течение этого срока отсутствует достаточное количество денежных средств для исполнения Платежного поручения и уплаты Комиссионной платы, Платежное поручение теряет силу, и Банк не обязан его исполнять.
- 2.7. Помимо случаев, указанных в пункте 3.11. ОПС, Банк имеет право не исполнять Платежные поручения, не принимать заявки Клиента, не акцептовать договоры Клиента о предоставлении Услуг или другие заявки Клиента и документы в следующих случаях:
 - 2.7.1. Банк не может идентифицировать Клиента по введенным Данным для электронной идентификации;
 - 2.7.2. у Банка возникли подозрения о подключении к Системе третьего лица;
 - 2.7.3. текст неразборчив или поврежден из-за некачественной связи.
- 2.8. Банк не несет ответственности за последствия использования или неиспользования прав Банка, указанных в пункте 2.7. настоящих Правил.
- 2.9. Помимо случаев, указанных в пункте 2.7. настоящих Правил, Банк не исполняет Платежные поручения, не принимает заявки Клиента, не акцептует договоры Клиента о предоставлении Услуг или другие заявки Клиента и документы в случаях, установленных Применимыми нормативными актами, между Банком и Клиентом заключенными договорами, и в других случаях, оговоренных в ОПС.
- 2.10. При получении платежного поручения Банк вправе повторно связаться с Клиентом для проверки правильности Платежного поручения.
- 2.11. Банк по своему усмотрению вправе определять или менять лимиты Данных для электронной идентификации, в пределах которых возможно списание денежных средств со Счета Клиента, а также определять или менять доступный в Системах ассортимент Услуг в зависимости от используемых Данных для электронной идентификации.
- 2.12. Клиент может установить лимиты списания денежных средств со Счета в порядке, установленном настоящими Правилами.
- 2.13. Если Клиент не согласен с Платежом, который посредством Системы был совершен на Счете, он может предъявить Банку претензию. Если Клиент не предъявляет Банку претензию в течение 13 (*тринадцати*) месяцев, или в течение 3 (*трех*) месяцев – если Клиент не является Потребителем, с момента осуществления Платежа, Банк вправе считать, что Клиент признает данный Платеж правильным.
- 2.14. Клиент незамедлительно должен информировать Банк о любом Неавторизованном платеже на Счете, а также о любой ошибке или неточности Банка, возникшей в процессе обслуживания Счета.
- 2.15. Банк ведет регистрацию (запись) всех действий и разговоров, совершенных посредством Системы, и данная запись может быть использована в качестве доказательства при разрешении споров между Клиентом и Банком.
- 2.16. Банк не несет ответственности за ошибки, задержку расчетов, неточности и другие недостатки, возникшие в результате предоставления Клиентом ошибочной или неполной информации при передаче Банку в Системе Платежных поручений или других документов.

- 2.17. Всю передаваемую посредством Системы информацию с использованием Данных для электронной идентификации Клиента Банк считает документами, которые обладают такой же юридической силой, что и документы, подписанные лично Клиентом. Все запросы, сообщения и предупреждения, переданные Банком Клиенту посредством Системы, обладают юридической силой документов, подписанных уполномоченным лицом Банка.
- 2.18. Клиент вправе в любой момент отказаться от пользования Системой, подав в Банк соответствующее заявление.
- 2.19. Банк, получив заявление Клиента об отказе от пользования Системой, в течение 3 (трех) Рабочих дней Банка отключает Клиенту доступ к Системе.
- 2.20. Если Банк закрывает последний подключенный к Системам Счет Клиента в случаях, указанных в ОПС и соответствующих Правилах, доступ Клиента к Системам прекращается автоматически.
- 2.21. Договор считается расторгнутым с момента отключения Клиента от Системы, и когда Клиент полностью рассчитался за Услуги в соответствии с Тарифами.

3. Идентификация Клиента при пользовании Системами

- 3.1. Для доступа к Счету через Систему или для выполнения других действий, осуществление которых обеспечивает Система, Клиент должен себя идентифицировать с помощью введения (сообщения) своих Данных для электронной идентификации.
- 3.2. Данные для электронной идентификации Клиента для доступа в Систему и к Счету следующие:
 - 3.2.1. Код Клиента (CIF);
 - 3.2.2. Коды доступа и Пароли;
 - 3.2.3. Элементы авторизации.
- 3.3. Для подтверждения документов (в т.ч. Платежных поручений), передаваемых посредством Системы, используется Электронная подпись.
- 3.4. Для формирования Электронной подписи и Кода доступа Банк присваивает/сообщает Клиенту специальные Данные для электронной идентификации, учитывая, что в распоряжении Клиента одновременно может находиться несколько Элементов авторизации:
 - 3.4.1. Кодовая карта;
 - 3.4.2. *DigiPass*;
 - 3.4.3. *SMS-PIN*;
 - 3.4.4. *Google Authenticator*;
 - 3.4.5. Код доступа.
- 3.5. Данными для электронной идентификации Клиента, в рамках настоящих Правил, является также номер мобильного телефона, который Клиент зарегистрировал в Банке (сообщил Банку) для получения *SMS-PIN* мобильный телефон или другое устройство, которое будет использоваться для пользования *Google Authenticator*, но, с учетом того, что на данный мобильный телефон (как само устройство) не распространяется действие пункта 3.7., пункта 3.8. и пункта 3.13. настоящих Правил, которые распространяются на Элементы авторизации, указанные в пунктах 3.4.1.-3.4.4. настоящих Правил.
- 3.6. Клиент осознает, что используя Данные для электронной идентификации Клиента, указанные в настоящих Правилах, доступ к счету Клиента может получить любое третье лицо (получать информацию и/или проводить операции с денежными средствами на Счете, в т.ч. с кредитными средствами). Обязанность Клиента – держать в тайне и в недоступном для третьих лиц месте свои Данные для электронной идентификации и Элементы авторизации (Код Клиента (CIF), Пароль, Кодовую карту, Код доступа, *DigiPass*, мобильный телефон, номер которого зарегистрирован для получения *SMS-PIN* или мобильный телефон или другое устройство, которое используется для пользования *Google Authenticator*). Клиент должен незамедлительно сообщить Банку, если третьим лицам стали известны Данные для электронной идентификации Клиента (также в случае, если у Клиента есть только подозрения об этом), а также об утере, пропаже, краже или другом противоправном присвоении устройств, используемых для их формирования или получения, или о несанкционированном использовании Данных для электронной идентификации. Клиент также может проинформировать об этом Банк по круглосуточному телефону приема сообщений от Клиентов: **+(371) 67041100**.
- 3.7. Если Клиент сообщил Банку об утере, пропаже Данных для электронной идентификации, или о том, что Данные для электронной идентификации стали известны третьим лицам (даже в случае, если у Клиента есть только подозрения об этом), Данные для электронной идентификации блокируются, в т.ч. блокируется возможность получения *SMS-PIN*, возможность использовать *Google Authenticator* с мобильного телефона или другого устройства, о котором Банку предоставлена информация об утере, пропаже, краже или другом противоправном присвоении, и доступа к Системе *PNB Chat*. Банк выдает/оформляет Клиенту новые Элементы авторизации, Пароли, разблокирует возможность получения Клиентом *SMS-PIN* и возобновляет доступ к Системе *PNB Chat* (в том числе присваивает новый Пароль *PNB Chat*), на основании письменного заявления Клиента, или возобновляет возможность пользоваться *Google Authenticator*, опираясь на звонок Клиента в Контактный центр Банка, и после оплаты Комиссионной платы, указанной в Тарифах.
- 3.8. Банк имеет право заблокировать Данные для электронной идентификации, подключение Клиента к Системам, возможность получения Клиентом *SMS-PIN* или *Google Authenticator* на конкретном телефоне или другом

устройстве, на котором установлено приложение *Google Authenticator*, также в случаях, которые связаны с безопасностью Данных для электронной идентификации, обоснованными подозрениями о неавторизованном использовании Данных для электронной идентификации или использовании в целях мошенничества, или в случаях, когда Данные для электронной идентификации связаны с кредитом и существенно возрос риск того, что Клиент может быть неспособен исполнить свои платежные обязательства перед Банком, а также если Банк получил информацию о смерти Клиента (физического лица) или о смерти единственного законного представителя или представителя, у которого было право представлять Клиента совместно с другими представителями, или о смерти истинного выгодоприобретателя (в понимании Закона Латвийской Республики) Клиента (юридического лица). Блокируя Данные для электронной идентификации, в случаях, указанных в настоящем пункте, Банк информирует об этом Клиента, если это возможно, – до предполагаемой блокировки или сразу после нее, за исключением случаев, когда предоставление информации может угрожать объективно обоснованным соображениям безопасности или предоставление информации запрещено в соответствии с требованиями Применимых нормативных актов. Банк не несет ответственности за последствия использования или неиспользования прав Банка, указанных в настоящем пункте.

- 3.9. Банк не несет ответственности за убытки Клиента, возникшие в результате доступа в Систему третьего лица, в т.ч. если третье лицо использовало Данные для электронной идентификации Клиента, за исключением, если Банк не обеспечил Клиенту возможность в любое время сообщить о потере, краже или другом противозаконном присвоении Данных для электронной идентификации и Клиент в этом случае сам не действовал противозаконно.
- 3.10. Банк не возмещает Клиенту убытки до 150 евро (*сто пятьдесят евро*), если они возникли в результате Неавторизованных платежей в результате потери, кражи или другого противозаконного присвоения Данных для электронной идентификации, или если Клиент не заботился о надежном хранении персонализированных электронных данных идентификации и, таким образом, допустил противозаконное присвоение Данных для электронной идентификации. Указанное в настоящем пункте не относится к убыткам, которые возникли после того, как Клиент, в соответствии с пунктом 3.6 настоящих Правил сообщил Банку о пропаже или потере Данных для электронной идентификации, или о том, что они стали известны третьим лицам, за исключением, если Клиент сам действовал противозаконно.
- 3.11. Банк не возмещает Клиенту убытки, которые у него возникли в связи с Неавторизованными платежами, если Клиент действовал противозаконно или с умыслом (намеренно) или в результате грубой неосмотрительности допустил использование Данных для электронной идентификации в несоответствии с настоящими Правилами, или не исполнил указанную в пункте 3.6 настоящих Правил обязанность информирования.
- 3.12. Банк имеет право по своему усмотрению, принимая во внимание сущность персонализированных элементов безопасности Данных для электронной идентификации и обстоятельства, при которых они были потеряны, украдены или другим образом противозаконно присвоены, и если Клиент не действовал противозаконно и также не констатировано, что Клиент с умыслом (намеренно) допустил использование Данных для электронной идентификации в несоответствии с настоящими Правилами или с умыслом (намеренно) не исполнил указанную в пункте 3.6. настоящих Правил обязанность информирования, уменьшить объем ответственности Клиента, указанный в пунктах 3.10. и 3.11. настоящих Правил. Указанные в настоящем пункте права не считаются обязанностью Банка, обязательной для исполнения.
- 3.13. По требованию Банка Клиент обязан вернуть Банку Данные для электронной идентификации в случаях, установленных ОПС.
- 3.14. Доступ к *PNB Internetbanka* блокируется в случае 5 (*пяти*) последовательных ошибочных попыток ввода символов Электронной подписи или других Данных для электронной идентификации Клиента.
- 3.15. Банк может разрешить совместное пользование устройством *DigiPass* несколькими Клиентами, которые подали Банку заявление стандартизированной формы и которые связаны между собой одним истинным выгодоприобретателем или уполномоченным лицом, или если Клиент входит в признанную Банком группу Клиентов. В таком случае Банк на основании заявления Клиентов может создать группу пользователей, что позволит получить одновременный доступ к счетам всех членов группы пользователей с одним устройством *DigiPass*.
- 3.16. Для получения *SMS-PIN* Клиент должен подать в Банк заявку стандартизированной формы в письменном (бумажном) виде или в электронном виде, через *PNB Internetbanka*, если у Клиента есть подключение к такой Системе, и указать (сообщить Банку) номер мобильного телефона, у которого есть функция отсылки и получения коротких сообщений (*SMS*), на который Клиент хочет получать *SMS-PIN*. Один Клиент может указать не более двух разных номеров мобильного телефона для получения *SMS-PIN*.
- 3.17. Банк не проверяет, является ли номер мобильного телефона, указанный Клиентом в соответствии с условиями пункта 3.16 настоящих Правил, зарегистрированным на имя Клиента (принадлежащим Клиенту). Учитывая условия пункта 3.6 настоящих Правил, Клиент должен самостоятельно обеспечивать недоступность *SMS-PIN* третьим лицам.
- 3.18. После выполнения, указанного в пункте 3.16 настоящих Правил, Банк будет отсылать Клиенту *SMS-PIN* каждый раз, когда Клиент выбирает опцию *SMS-PIN* для доступа в Систему или для формирования Электронной подписи и указывает, на какой именно номер мобильного телефона в настоящий момент Клиент хочет получить *SMS-PIN*. Каждый соответствующий *SMS-PIN* действителен для использования в качестве

Данных для электронной идентификации Клиента в тот день, в который он был получен и в течении времени, указанного в соответствующем коротком сообщении от Банка. После истечения этого времени, если полученный *SMS-PIN* не будет использован, он становится недействительным, и Клиент должен повторно инициировать получение нового *SMS-PIN*.

- 3.19. *SMS-PIN* доступен только такому Клиенту (его законному представителю), у которого есть неограниченные права единолично распоряжаться Счетом. На *SMS-PIN* не распространяются условия раздела 4 настоящих Правил.
- 3.20. Плату за пользование *SMS-PIN* в соответствии с Тарифами Клиент платит Банку в соответствующем размере в последний день каждого месяца до момента, пока Банк не получит от Клиента заявление об отказе от использования *SMS-PIN*.
- 3.21. Клиент имеет право в любой момент сообщить Банку другой номер мобильного телефона, на который в дальнейшем Клиент хочет получать *SMS-PIN*, а также имеет право отказаться от дальнейшего использования *SMS-PIN*, предварительно за 3 (*mpu*) Рабочих дня Банка уведомив об этом Банк, подав Банку соответствующую заявку в бумажном виде или в электронном виде, через *PNB Internetbanka*.
- 3.22. Банк не несет ответственности за то, что Клиент не получит *SMS-PIN*, если мобильный телефон Клиента находится вне зоны доступа сигнала или отключен, или из-за неправильной работы телефона.
- 3.23. Для формирования Электронной подписи с использованием Кодовой карты Клиент выбирает один, запрошенный Банком вариант шестизначного кода и сообщает этот шестизначный код Банку путем его ввода в Систему. Банк проверяет соответствие сообщенного (введенного) шестизначного кода имеющейся у Банка информации о данном варианте шестизначного кода.
- 3.24. Для формирования Электронной подписи с использованием *DigiPass* Клиент, в соответствии с инструкцией по использованию устройства *DigiPass* (которая доступна на домашней странице Банка в Интернете www.pnbbanka.eu или в любом Месте обслуживания клиентов Банка), вводит в Систему параметры подписи, сообщая Банку сформированное устройством *DigiPass* значение Электронной подписи.
- 3.25. Для формирования Электронной подписи с использованием *SMS-PIN* Клиент вводит в Систему комбинацию цифр, которую Клиент получил от Банка в виде короткого сообщения. Банк проверяет соответствие сообщенного (введенного) числа имеющейся у Банка информации о данном варианте числа.
- 3.26. Для использования *Google Authenticator*, Клиенту нужно установить это приложение на мобильном телефоне или на другом устройстве и подключить *Google Authenticator* в *PNB Internetbanka* как средство идентификации.
- 3.27. Клиент может подключить *Google Authenticator* в *PNB Internetbanka*, если у Клиента есть хотя бы один из следующих средств идентификации: *DigiPass* или *SMS-PIN*.
- 3.28. Для формирования Электронной подписи в Системе *PNB Vision* с использованием Пароля *PNB Vision*, Клиент вводит этот пароль в Систему *PNB Vision*, и на его основании, и на основании уникальных параметров Системы *PNB Vision*, формируется Электронная подпись.

4. Установление полномочий Электронной подписи для Данных для электронной идентификации

- 4.1. Клиент может запросить подключение своих Данных для электронной идентификации только с правами просмотра или с правами полного доступа.
- 4.2. Если в распоряжении Клиента находится несколько устройств *DigiPass*, Клиент может, заполнив стандартизированное заявление Банка и заплатив Комиссионную плату, предоставить одному или нескольким Данным для электронной идентификации право регулировать объем полномочий других выбранных Данных для электронной идентификации, ограничивая:
 - 4.2.1. доступные виды Банковских операций;
 - 4.2.2. получателей платежей;
 - 4.2.3. доступ к Счетам.
- 4.3. Клиент регулирует объем полномочий Данных для электронной идентификации самостоятельно, отправляя Банку стандартизированные сообщения через *PNB Internetbanka*.
- 4.4. Если в распоряжении Клиента находится несколько устройств *DigiPass*, Клиент, заполнив стандартизированное заявление Банка и заплатив Комиссионную плату, может установить для каждого из устройств *DigiPass* различные полномочия Электронной подписи.
- 4.5. Клиент может выбрать и установить Данным для электронной идентификации полномочия подписывать адресованные Банку документы самостоятельно или только совместно с одним или с несколькими другими Данными для электронной идентификации, выбранными Клиентом.
- 4.6. Банковский документ, подписанный при помощи Данных для электронной идентификации, наделенных полномочиями самостоятельной подписи, принимается к исполнению немедленно.
- 4.7. Банковский документ, подписанный при помощи Данных для электронной идентификации, наделенных полномочиями подписи только совместно с одним или несколькими другими Данными для электронной идентификации, сохраняется в *PNB Internetbanka* и принимается к исполнению только после подтверждения Электронной подписью, созданной при помощи указанных в заявлении Клиента Данных для электронной идентификации.
- 4.8. Банк не несет ответственности за убытки, которые могут возникнуть у Клиента вследствие споров между пользователями Данных для электронной идентификации Клиента.

5. Пользование *PNB Internetbanka*

- 5.1. *PNB Internetbanka* предоставляет Клиенту возможность посредством Интернета: распоряжаться денежными средствами на Счетах путем подачи Банку электронного Платежного поручения;
- 5.1.1. получать информацию о Счетах и операциях;
- 5.1.2. подавать заявки и заключать с Банком договоры о получении различных Услуг или отказе от дальнейшего использования Услуг.
- 5.2. Адрес доступа к *PNB Internetbanka*: <https://www.ib.pnbbanka.eu>.
- 5.3. Для пользования *PNB Internetbanka* Клиенту необходим *Internet Explorer* (версии 9.0 или более новой) и совместимый с ним интернет-браузер, поддерживающий *JavaScript*, и подключение к сети Интернет.
- 5.4. Доступ в *PNB Internetbanka* возможен круглосуточно.
- 5.5. При использовании Мобильного приложения Клиент может воспользоваться Услугой в таком объеме, который обеспечивает Мобильное приложение.
- 5.6. В отношении использования Мобильного приложения применяются условия пользования *PNB Internetbanka*.

6. Пользование *PNB Vision*

- 6.1. *PNB Vision* предоставляет Клиенту возможность, используя модем или другое подключение к Интернету:
- 6.1.1. распоряжаться денежными средствами на Счетах путем подачи Банку электронного Платежного поручения;
- 6.1.2. получать информацию о Счетах и потоке денежных средств;
- 6.1.3. подавать заявки и заключать с Банком договоры о получении различных Услуг.
- 6.2. Для пользования *PNB Vision* Клиенту необходим компьютер с операционной системой *MS Windows 98/NT/2000/XP*, модем или другое подключение к сети Интернет.
- 6.3. Данные для электронной идентификации Клиента в *PNB Vision*: Пароль *PNB Vision* и/или Электронная подпись.
- 6.4. Доступ в *PNB Vision* возможен круглосуточно.

7. Пользование *PNB Trade* (в рамках использования *PNB Internetbanka*)

- 7.1. В рамках пользования *PNB Internetbanka* Клиенту предоставляется возможность пользоваться также *PNB Trade*, которая предоставляет Клиенту возможность заключать с Банком сделки купли-продажи валюты.
- 7.2. Для пользования *PNB Trade* Клиенту необходимо подать заявку в Банк на получение услуги купли-продажи валюты, а также, в случае необходимости, заключить с Банком договор купли-продажи безналичной валюты на маржинальных счетах. Сделки купли-продажи валюты и купли-продажи безналичной валюты на маржинальных счетах заключаются согласно правилам заключения соответствующих сделок.
- 7.3. Доступ в *PNB Trade* возможен круглосуточно.

8. Пользование *PNB SMS-Banka*

- 8.1. *PNB SMS-Banka* обеспечивает Клиенту возможность получать информацию об остатке на Счете, изменениях в остатке Счета.
- 8.2. Для пользования *PNB SMS-Banka* Клиенту необходим мобильный телефон с функцией получения и отправления коротких сообщений (SMS) и/или электронная почта.
- 8.3. Данными для электронной идентификации Клиента при использовании *PNB SMS-Banka* является номер мобильного телефона Клиента, который Клиент сообщил Банку, и Электронная подпись.
- 8.4. Клиент обязан обеспечивать недоступность третьим лицам своего мобильного телефона, электронной почты, присланных на них Банком информации и поручений, а также информации и поручений, отосланных Банку с мобильного телефона Клиента.
- 8.5. Клиент обязан обеспечивать сохранность номера мобильного телефона, зарегистрированного на получение Услуги *PNB SMS-Banka*, и следить за тем, чтобы он не попал в распоряжение третьих лиц (в том числе, не допускать переоформления номера на имя третьего лица). Клиент обязан незамедлительно сообщать Банку об утрате прав собственности на указанный номер и о смене номера оператора мобильной связи.
- 8.6. Если мобильный телефон, зарегистрированный на получение Услуги *PNB SMS-Banka*, находится вне зоны доступа сигнала или отключен дольше 3 (трех) Рабочих дней Банка, Банк не обеспечивает предоставление Услуги Клиенту, и:
 - 8.6.1. Банк имеет право отказаться от исполнения поданных Клиентом Платежных поручений и/или прекратить предоставление Удаленной услуги;
 - 8.6.2. Банк не несет ответственности за убытки, возникшие у Клиента в результате доступа третьих лиц к *PNB SMS-Banka* и/или ее использования третьими лицами.
- 8.7. Банк не несет ответственности, если информация, присланная на мобильный телефон или электронную почту Клиента или информация, или Платежные поручения, отправленные с мобильного телефона Клиента, становятся доступными третьим лицам.
- 8.8. Доступ к *PNB SMS-Banka* возможен круглосуточно.
- 8.9. Если у Клиента выставлены другие настройки на получение информации о сделках по Карте, информация будет отправлена, используя именной номер Услуги *PNB SMS-Banka* - «PNBBanka».

9. Пользование *infoLINE*

- 9.1. *infoLINE* предоставляет Клиенту возможность получения информации о Счетах по телефону.

- 9.2. Для получения информации Клиенту необходим телефон с подключением к телефонной сети.
- 9.3. Для подключения к *infoLINE* Клиент должен обратиться в Банк или связаться со специалистом Банка по круглосуточному телефону +(371) 67041118 и назвать запрашиваемую работником Банка информацию. После завершения подключения и сообщения упомянутой информации работник Банка называет Клиенту Код доступа, который в дальнейшем будет применяться для использования *infoLINE*.
- 9.4. Получение информации в *infoLINE* возможно круглосуточно. Номера телефона для получения информации: +(371) 67011566 (информация на латышском языке) и +(371) 67011565 (информация на русском языке).
- 9.5. Данные для электронной идентификации Клиента в *infoLINE* следующие:
 - 9.5.1. для получения информации о Счете – присвоенный Банком Клиенту при открытии Счета Код Клиента (CIF) и Код доступа, присвоенный Банком Клиенту при подключении *infoLINE*;
 - 9.5.2. для получения информации о Карточном счете – 6 (*шесть*) последних цифр номера Карты и Код доступа, присвоенный Банком Клиенту при подключении *infoLINE*.
- 9.6. Идентификация Клиента в *infoLINE* осуществляется, когда Клиент вводит указанные в пункте 9.5. настоящих Правил Данные для электронной идентификации, используя клавиатуру телефона.

10. Пользование *PNB Chat*

- 10.1. *PNB Chat* предоставляет Клиенту возможность связаться с Банком в режиме онлайн для выяснения вопросов возможных условий сделок по купле-продаже безналичной валюты, а также заключить с Банком данные Сделки. Сделки по купле-продаже валюты заключаются в соответствии с Правилами соответствующей Услуги.
- 10.2. Для того, чтобы начать использовать *PNB Chat*, Клиент должен подать в Банк соответствующую заявку через *PNB Internetbanka*. После получения соответствующей заявки Клиента, Банк регистрирует Клиента в *PNB Chat* и сообщает Клиенту в *PNB Internetbanka* Данные для электронной идентификации Клиента (в том числе Пароль *PNB Chat*) для доступа в *PNB Chat*.
- 10.3. Адрес доступа в *PNB Chat*: <https://chat.pnbbanka.eu>
- 10.4. Для использования *PNB Chat*, Клиенту необходимо иметь браузер *Google Chrome* или *Mozilla Firefox*, который поддерживает *JavaScript*, а также подключение к сети Интернета.
- 10.5. Доступ в *PNB Chat* доступен круглосуточно, но связь с Банком в режиме онлайн и заключение Сделок возможно в те дни, когда латвийские и зарубежные банки открыты для проведения финансовых операций с соответствующими валютами, в следующие часы (по латвийскому времени): для резидентов Латвийской Республики – с 8:00 до 18:00, для нерезидентов Латвийской Республики – с 8:00 до 18:30.

* * *