Обов'язкові для:
- договорів, укладених з 04 вересня 2020 р.
- договорів, укладених до 3 вересня 2020 р. та договорів, підписаних у рамках «T-Mobile Usługi Bankowe były Oddział Alior Banku S.A.» – з 29 листопада 2020 р.

Правила використання Електронних каналів зв'язку для індивідуальних клієнтів.

Загальні Правила

§1

1. Ці Правила використання Електронних каналів зв'язку для Індивідуальних клієнтів визначають правила та умови надання інформації про продукти Користувача та подання розпоряджень через Електронні канали.
2. Правила є додатком до Договору про надання Банком послуг Фізичній особі та є його невід'ємною частиною.
3. Якщо інше не передбачено Правилами, то Правила не поширюються на договори, укладені з T-Mobile Usługi Bankowe та послуги, що надаються через T-Mobile Usługi Bankowe – діють до 28 листопада 2020 року.

§2

Терміни, що використовуються далі в Правилах, мають такі значення:

Активація системи Мобільного банкінгу – ряд дій, які виконує Користувач у Мобільному банкінгу після встановлення Мобільного додатка, спрямованих на визначення методу ідентифікації та авторизації в Мобільному додатку. На сайті Банку розміщено детальну Інструкцію по активації;

Додаток (застосунок) мобільного банкінгу (Alior Mobile) – програмне забезпечення, яке встановлюється на мобільний пристрій (смартфони, планшети та ПК), що використовується для обслуговування Мобільного банкінгу. З функціональними можливостями Мобільного застосунку, у тому числі видами розпоряджень, інструкціями, які можуть бути подані з його допомогою, можна ознайомитися на сайті Банку;

Банк – Alior Bank Spółka Akcyjna [«Альор Банк» Акціонернене Товариство] з місцезнаходженням у Варшаві;

Інтернет-банкінг – послуга електронного банкінгу (Alior Online) – послуга, що забезпечує доступ до інформації про Продукти Користувача та можливість подачі розпоряджень за допомогою мережі Інтернет та пристрою, оснащеного веб-браузером. З функціональними можливостями Інтернет-банкінгу, в тому числі з видами розпоряджень, які можуть бути подані за його допомогою, можна ознайомитися на сайті Банку.

Мобільний банкінг – послуга електронного банкінгу – послуга, яка забезпечує доступ до інформації про Продукти Користувача та можливість подачі розпоряджень за допомогою мобільних пристроїв, таких як ПК, планшети та мобільні телефони з доступом до Інтернету, через веб-браузери або Мобільний додаток; З функціональними можливостями Мобільного банкінгу, в тому числі з видами розпоряджень, які можуть бути подані з його допомогою, можна ознайомитися на сайті Банку.

Телефонний банкінг – послуга, яка надає доступ до інформації про Продукти Користувача та можливість подачі розпоряджень за допомогою телефону з тоновим режимом (може стягуватися плата за з'єднання згідно з тарифом оператора);

Біометрія – метод ідентифікації та аутентифікації Користувача та авторизації Розпорядження, що полягає у порівнянні індивідуальних фізичних характеристик Клієнта зі зразком, що зберігається в ІТ-системі виробника пристрою, на якому встановлено Мобільний додаток;

Брокерський дім (Маклерське бюро) – відокремлений організаційний підрозділ Банку, відповідальний за надання Банком брокерських послуг;

Контактний центр (Контакт-центр, Contact Center) – підрозділ Банку або Брокерського дому, що надає здійснює телефонне обслуговування актуальних і потенційних Користувачів у сфері інформації, продажу та операцій;

Ідентифікаційні дані – сукупність даних, що дозволяють ідентифікувати фізичну або юридичну особу, або фізичну особу, яка представляє юридичну особу;

Розпорядження (Інструкція) – заява про наміри, подана Користувачем через Електронні канали та авторизована у відповідний для даного каналу спосіб;

Верифікаційна фраза (пароль для зворотної верифікації Банку) – слово, фраза або рядок символів, встановлені Користувачем, що використовуються для автентифікації співробітника Банку, який зв'язується з Користувачем по телефону в ситуації, коли контакт ініційований Банком;

Пароль доступу – рядок символів, самостійно визначених Користувачем в Інтернет-банкінгу, який при використанні разом з Ідентифікатором забезпечує доступ до Інтернет-банкінгу. Для Користувачів, які пов'язані договорами, укладеними з T-Mobile Usługi Bankowe (з 29 листопада 2020: T-Mobile Usługi Bankowe były Oddział Alior Bank S.A.), може використовуватися пароль, визначений в інтернет-банкінгу T-Mobile Usługi Bankowe (з 29 листопада 2020: T-Mobile Usługi Bankowe były Oddział Alior Bank S.A.;

Стартовий пароль – послідовність цифр, що надсилаються Користувачеві на Телефон до кодів авторизації у вигляді текстового повідомлення, що використовується для активації Інтернет-банкінгу;

Ідентифікатор (номер Картотеки Клієнта - CIF) – унікальний номер, присвоєний Користувачеві Банком, з яким чітко пов'язані персональні та адресні дані, які використовуються, зокрема, для ідентифікації при використанні Електронних каналів зв'язку;

Біометричний ідентифікатор – запис індивідуальних фізичних характеристик Клієнта (наприклад, відбиток пальця або скан зображення його обличчя), який зберігається та надається на мобільному пристрої його виробником, що дозволяє увійти в Мобільний додаток та авторизувати вибрані розпорядження через Мобільний додаток. Біометричний ідентифікатор доступний:

1. У Мобільному додатку на пристроях з операційною системою iOS (від версії 11.0), яка підтримує рішення TouchID (зчитування відбитків пальців) або FaceID (зчитування обличчя) і дозволяє:
   a. увійти в Мобільний додаток,
   b. авторизацію вибраних Розпоряджень, доручених через Мобільний банкінг (з версії № 1.8.0).
2. У Мобільному додатку (від версії 1.8.0) на пристрої з операційною системою Android (від версії 6.0), що підтримує рішення Fingerprint Authentication (автентифікації за відбитками пальців) і дозволяє:
   a. вхід у Мобільний додаток ,

б. авторизацію вибраних Розпоряджень, доручених у Мобільному банкінгу.

IVR – послуга, що забезпечує цілодобовий, автоматичний доступ до інформації про Продукти Користувача за допомогою телефону з тоновим режимом;

Електронні канали зв'язку – Інтернет-банкінг (в тому числі, така що розглядається окремо – функційність для ініціювання платежів третіми особами та функційність для доступу третіми особами до інформації про рахунки для здійснення платежів, а також для послуг постачальників, що видають карткові інструменти), Телефонний банкінг, Мобільний банкінг, IVR;

Код авторизації – код у вигляді текстового повідомлення, надісланого на Телефон, визначений Користувачем для авторизації доручень, який використовується для авторизації Розпоряджень, поданих Користувачем у рамках Інтернет-банкінгу, Мобільного банкінгу або Телефонного банкінгу;

Ліміти сум – це параметри, які визначають значення одноразової/добової/місячної суми операції, окремо для інтернет-банкінгу (включаючи постачальників послуг ініціювання платежу), для мобільного банкінгу, для кодів BLIK та для телефонних переказів BLIK.

BLIK код – 6-значний код, згенерований Мобільним додатком, який може використовуватися для деяких операцій у Сервісі BLIK;

PUSH-повідомлення – повідомлення, які дистанційно відправляються до Мобільного банкінгу/Alior Mobile Банком, стосуються подій на Рахунках, продуктів, до яких Клієнт має доступ, або містять іншу інформацію з Банку (при цьому певні функції PUSH-повідомлень будуть доступні з моменту впровадження в Банку після попереднього інформування Користувача не пізніше ніж за 7 днів до дати надання послуги через Електронні канали);

MojeID – система, яка дозволяє авторизувати заяви, на основі механізмів банківської автентифікації, наданих Національною розрахунковою палатою AT. (діє з моменту надання послуги Банку, після інформування Користувача не пізніше ніж за 7 днів до дати надання послуги, через Електронні канали);

ПІН-код авторизації – послідовність цифр, визначена Користувачем у конфіденційний спосіб під час активації Мобільного додатка, що використовується для входу та авторизації Розпоряджень, надаваних через Мобільний додаток;

Установа Банку – організаційний підрозділ Банку, що здійснює банківську діяльність.

Фінансові повідомлення – послуга, яка дає змогу Користувачеві отримувати інформацію про Продукти та послуги Користувача, що надаються Банком або Брокерським домом; повідомлення надсилаються у відкритому (незашифрованому) вигляді;

Доручення переказу на телефон BLIK – вид внутрішнього (в межах країни) платежу в злотих, що дозволяє замовляти та отримувати доручення на переказ Користувачем, особа якого ідентифікована за номером телефону до кодів авторизації. Доручення здійснення переказу на телефон BLIK доступне без додаткової активації послуги в Мобільному додатку. Відправляючи доручення переказу на телефон BLIK, Користувач дає згоду на передачу Банком номера банківського рахунку іншим учасникам операції. Отримання Доручення переказу BLIK доступне після додаткової активації послуги в Мобільному додатку. Мобільний додаток має функцію зняття з реєстрації даного номера телефону з іншого банку та пов'язання його з рахунком в Alior Bank S.A.;

Поведінковий профіль – профіль Користувача, створений на основі характерних поведінкових особливостей Користувача, пов'язаних з використанням Інтернет-банкінгу або Мобільного банкінгу, включаючи, наприклад, характеристики використання таких пристроїв, як клавіатура, сенсорний екран, сенсорна панель, миша або датчики мобільних пристроїв у цих Електронних каналах. На основі поведінкового профілю може виконуватися Сильна автентифікація, а також авторизація вибраних Розпоряджень;

Прохання переказу BLIK – повідомлення, що дозволяє Користувачу відправляти та отримувати розпорядження на виконання Доручення переказу на телефон BLIK. Прийняття Прохання переказу BLIK його адресатом автоматично запускає виконання Доручення переказу на телефон BLIK відповідно до даних, що містяться в розпорядженні. Термін дії повідомлення становить 72 години з моменту його створення. Прохання переказу BLIK активується автоматично під час активації Доручення переказу на телефон BLIK. Активація Прохання переказу означає згоду Користувача на надання Банком номера банківського рахунку іншим учасникам операції (послуга діє з моменту надання Банком її доступності, після повідомлення Користувача не пізніше ніж за 7 днів до дати надання послуги, через Електронні канали);

Продукт – рахунок або послуга, пропонована Банком або Брокерським домом, що надається на підставі укладення відповідного договору та правил;

Сильна автентифікація – автентифікація, що забезпечує захист конфіденційності даних на основі використання принаймні двох елементів, що належать до категорії:

а) знання про те, що знає лише Користувач,

б) володіння тим, що є лише у Користувача,

в) характерні риси Користувача.

- і є невід'ємною частиною цієї автентифікації та незалежними таким чином, що порушення одного з цих елементів не зменшує вірогідність інших;

Засоби електронної ідентифікації – нематеріальна сутність, що містить дані, що ідентифікують особу та використовуються для автентифікації для онлайн-сервісів;

Телефон для кодів авторизації – номер мобільного телефону, наданий Користувачем, на який надсилаються Стартовий пароль та Коди авторизації;

Tele PIN – рядок цифр, встановлених Користувачем у конфіденційний спосіб під час активації Телефонного банкінгу, що використовується для верифікації Користувача в рамках цієї послуги;

T-Mobile Usługi Bankowe (T-Mobile Банківські послуги) – відділення Alior Bank SA. (діяло до 28 листопада 2020 р.).

Жорсткий носій (носій для тривалого збереження даних) – носій, який дозволяє Клієнту отримати доступ до адресованої йому інформації таким чином, що він має цей доступ до неї протягом періоду, відповідного для цілей підготовки цієї інформації, та дозволяє відновити збережену інформацію в незмінному вигляді.

Договір – Рамковий договір про надання послуг, які пропонує Банк для Фізичної особи, укладений між Банком і фізичною особою, на підставі якого можливе використання Електронних каналів зв'язку.

Пристрій – пристрій (зокрема мобільний телефон, який є смартфоном), на якому встановлено застосунок Alior Mobile (зокрема з Послугою BLIK).

Пристрій за замовчуванням – пристрій, який Користувач використовує для своєї автентифікації і який для цієї мети узгоджується між Банком і Користувачем (пов'язаний з Користувачем). Пристрій за замовчуванням використовується для передачі повідомлень PUSH.

Послуга/Послуга BLIK – послуга, яка дає змогу давати доручення за допомогою застосунку Alior Mobile.

Біометрична автентифікація – метод входу в Мобільний додаток, що дозволяє автентифікувати користувача за допомогою Біометричного ідентифікатора;

Користувач – фізична особа, яка уклала Договір і має право на розміщення Розпоряджень через Електронні канали;
Зняття готівки BLIK – операція зняття коштів в банкоматі за допомогою коду BLIK.

УМОВИ НАДАННЯ ДОСТУПУ ДО ЕЛЕКТРОННИХ КАНАЛІВ ЗВЯЗКУ

§3

Електронні канали зв'язку стають доступними після спільного виконання наступних умов:

1. Укладення Договору Користувачем або його законним представником:
   a. особисто, в Установі Банку,
   b. листом,
   c. будь-яким іншим способом, зазначеним Банком, відповідно до чинного законодавства.
2. Активації Користувачем вибраного Електронного каналу шляхом надання Ідентифікатора або вказання персональних даних та:
   a. Стартового пароля і вибрання способу входу – у випадку Інтернет-банкінгу,
   b. встановлення ПІН-коду для Мобільного додатка – у випадку Мобільного банкінгу,
   c. проведення успішної верифікації персональних даних під час розмови з консультантом Контакт-центру – у разі Телефонного банкінгу.

§4

Інтернет-банкінг або Мобільний банкінг можна активувати незалежно один від одного, у будь-якому порядку.

§5

Після активації Електронних каналів Користувач отримує доступ до вибраних Продуктів, у тому числі до тих, які будуть відкриті в майбутньому.

ПОСЛУГИ ЕЛЕКТРОННИХ КАНАЛІВ ЗВЯЗКУ

§6

Електронні канали дають змогу Користувачеві керувати коштами, отримувати інформацію про Продукти, якими володіє, укладати договори на вибрані Продукти та керувати Ідентифікаційними даними (дійсні з моменту надання Банком їх доступності, після інформування Користувача не пізніше ніж за 7 днів до дата надання послуги, через Електронні канали).

§7

Банк може змінити обсяг інформації та Розпоряджень, доступних через Електронні канали, у разі введення нових або зміни загально діючих положень законодавства або внесення змін до пропозиції Банку.

§8

1. Банк надає Користувачам послугу Фінансових повідомлень, яка підтверджує події на рахунку Користувача.
2. Фінансові повідомлення можуть надсилатися:
   a. як SMS-повідомлення,
   b. як повідомлення електронної пошти,
   c. через Інтернет-банкінг,
   d. як повідомлення PUSH.
3. Обсяг повідомлень визначається Користувачем через форму, доступну в Інтернет або Мобільному банкінгу, із застереженням абз. 5.
4. Фінансові повідомлення надсилаються одразу після настання події, за умови, що вночі надсилаються лише критичні сповіщення (інформація про години та обсяг повідомлень надається в Інтернет-банкінгу).
5. Банк має право надсилати додаткові повідомлення з інформацією про події на рахунку. Плата за такі повідомлення не стягується.

РЕАЛІЗАЦІЯ РОЗПОРЯДЖЕННЯ ТА ПРАВИЛА КОРИСТУВАННЯ ЕЛЕКТРОННИМИ КАНАЛАМИ ЗВЯЗКУ

§9

Розпорядження через Електронні канали можна подавати щодня, протягом усієї доби, за винятком раніше оголошених перерв на технічне обслуговування.

§10

Актуальна інформація про порядок та умови виконання Розпорядження розміщена на веб-сайті Банку та Брокерського дому

§11

1. Розпорядження, надані через Інтернет-банкінг, можуть вимагати авторизації з використанням Коду авторизації, PUSH-повідомлення або на основі Поведінкового профілю.
2. Розпорядження, надіслані через Мобільний додаток, можуть вимагати авторизації за допомогою PIN-коду авторизації, Біометричного ідентифікатора, PUSH-повідомлення або на основі Поведінкового профілю.
3. Розпорядження, подані через Телефонний банкінг, можуть вимагати авторизації Кодом авторизації або PUSH-повідомлення (послуга діє з моменту її надання Банком, після повідомлення Користувача не пізніше ніж за 7 днів до дати надання послуги доступно, через Електронні канали).
4. Користувач не може сумніватися в автентичності належним чином авторизованого Розпорядження.

§12

1. Належним чином авторизоване Розпорядження з поточною датою виконання не може бути анульоване.
2. Положення абз. 1 не виключають можливості подання Розпорядження про скасування доручення в рамках надаваних брокерських послуг на умовах, визначених Правилами про надання даної брокерської послуги.

§13

1. Дані, необхідні для правильного виконання Розпорядження, необхідно надати відповідно до опису полів у формі Розпорядження.
2. Перед авторизацією Користувач повинен переконатися, що Розпорядження однозначні та відповідають його намірам, включаючи, зокрема, ті, що доручаються на основі фотографій рахунків-фактур або рахунків, зроблених за допомогою мобільного пристрою.

§14

1. Банк реєструє та зберігає на електронних носіях усі телефонні розмови з Контакт-центром.
2. Користувач погоджується на запис цих розмов.
3. У разі згоди Користувача або аварії записуючого пристрою Банк має право відмовити в прийнятті Розпорядження по телефону.
4. У разі виникнення сумнівів щодо змісту поданого Розпорядження, записи дзвінків є остаточними і можуть бути використані в порядку оскарження та для доказів.

§15

Розпорядження щодо обробки постійних доручень, що виконуються з банківських рахунків, та анулювання доручень переказу з відстроченою датою виконання приймаються не пізніше одного робочого дня до дати виконання Доручення.

§16

При виникненні обґрунтованої підозри щодо достовірності поданого Розпорядження Банк може

призупинити його виконання до з'ясування сумнівів або відмовити у його виконанні.

§17

1. Максимальна сума, на яку можна дати доручення на переказ через Інтернет-банк і Мобільний банк, опублікована на сайті Банку та Брокерського дому, і ці ліміти можуть бути різними для Інтернет-банкінгу та Мобільного додатка та для різних типів Розпоряджень і різних сегментів Користувачів. Доручення переказу понад зазначену суму не виконуються.
2. У разі виконання доручень переказу в іноземній валюті максимальна сума визначається шляхом перерахування в злотих суми, зазначеної в абз. 1. Конвертація здійснюється за поточним курсом купівлі/продажу іноземної валюти, що діє в Банку на момент доручення виконання переказу.
3. Обмеження, зазначене в п. 1. 1 і 2 не поширюються на платіжні доручення, замовлені з використанням шаблону платежу, визначеного у відділенні Банку, та на власні переказні доручення. Платіжні доручення, що здійснюються через Телефонний банкінг, мають інші ліміти. Інформацію про максимальну суму доручення переказу, реалізованого через Контакт-центр, можна отримати на сайті Банку та у консультантів.
4. Користувач після входу в Інтернет-банкінг як уповноважений представник клієнта, в тому числі через суб'єктів, зазначених у § 37, може здійснювати лише ті види діяльності, на які він уповноважений на підставі довіреності.

ПОСЛУГА BLIK, ПОСЛУГА РОЗПОРЯДЖЕНЬ ДОРУЧЕНЬ ПЕРЕКАЗУ НА ТЕЛЕФОН BLIK ТА ПРОХАННЯ ПЕРЕКАЗУ BLIK – ПРАВИЛА РЕЄСТРАЦІЇ ПОСЛУГИ, РОЗПОРЯДЖЕННЯ, ЛІМІТИ ТА РОЗРАХУНКИ ОПЕРАЦІЙ

§18

1. Послугою BLIK, можуть користуватися всі Клієнти, які встановили Мобільний додаток. Статус вищезазначених послуг можна перевірити в налаштуваннях Мобільного додатка, а також активувати та деактивувати ту чи іншу послугу.
2. Коди BLIK активуються Користувачем після активації Мобільного додатка або автоматично під час активації Мобільного додатка.
3. Якщо номер телефону для кодів авторизації не прив'язаний до рахунку в іншому банку, Доручення переказу на телефон BLIK може бути активовано автоматично під час активації Мобільного додатка. Активація означає, що Перекази BLIK, керовані на вказаний вище номер телефону, будуть реєструватися на рахунку в Alior Bank S.A., визначеному в абз. 4 § 20.
4. Зареєструватися в Послузі BLIK, послузі Доручень переказу на телефон BLIK та в послузі Прохання переказу BLIK мають право Клієнти, які в сукупності відповідають таким умовам:
   a. мають відповідне технічне обладнання, зокрема мобільний пристрій, пов'язаний з номером мобільного телефону оператора мобільного зв'язку, що діє на території Республіки Польща,
   b. мають Договір про надання Банком послуг для фізичної особи,
   c. мають активний Мобільний додаток,
   d. мають ощадно-розрахунковий рахунок у злотих в Банку.

§19

1. Операції, що здійснюються через Мобільний додаток із Послугою BLIK та Послугою Доручень переказу на телефон BLIK, можуть виконуватися в межах одноразових, добових та щомісячних лімітів суми для цієї Послуги.
2. Після активації граничні значення, зазначені в абз. 1, відповідають лімітам, встановленим Банком.
3. Користувач може використовувати функціонал оформлення замовлень без входу в Мобільний додаток
4. Користувач не може змінювати ліміти сум для Послуги BLIK.
5. Банк приймає розпорядження, подані через мобільний канал, за винятком періоду перерв, необхідних для технічного обслуговування, технічного ремонту або відновлення належної роботи мобільного каналу, у тому числі Мобільного додатка із Послугою BLIK.

§ 20

1. В рамках послуги BLIK та послуги Доручення переказу на телефон BLIK Банк надає можливість:
   a. оплати товарів або послуг, придбаних через веб-сайт або додаток суб'єкта, що пропонує ці товари чи послуги, шляхом авторизації операцій Користувачем в Мобільному додатку із Послугою BLIK,
   b. зняття готівки в окремих банкоматах і платіжних терміналах POS,
   c. здійснення розрахункових операцій за товари та послуги у визначених пунктах, обладнаних POS-терміналами або іншими пристроями, що дають змогу виконувати операції, замовлені через мобільний канал.
2. В рамках послуги Прохання переказу BLIK Банк надає можливість:
   a. дати розпорядження виконання Доручення переказу на телефон BLIK;
   b. автоматично заблокувати отримання розпоряджень Доручення переказу на телефон BLIK, надісланих іншими учасниками операції;
   c. автоматично відхилити отримані Доручення переказу на телефон BLIK, надіслані іншими учасниками операції.
3. Кожен раз номер телефону для кодів авторизації (далі Alias) встановлюється як номер телефону, пов'язаний з рахунком, визначеним у абз. 4. Активуючи послугу BLIK, Користувач дає згоду на обробку даних, що містяться в адресній книзі цього телефону, з метою представлення одержувачів, чиї телефонні номери зареєстровані в базі даних BLIK. Підключаючи послугу, Користувач погоджується на передачу Банком номера банківського рахунку іншим учасникам операції. Розпорядження Доручення переказу на телефон BLIK та Прохання переказу BLIK вимагає від Користувача вказати номер телефону одержувача, суму та назву доручення на переказ. Зміна Телефону для Кодів авторизації, у разі активної послуги Доручень переказу на телефон BLIK та Прохання переказу на телефон BLIK, автоматично її відключає. Якщо ви хочете оновити Alias у послузі Доручення переказу BLIK, вам необхідно повторно його активувати. Актуалізація Alias в послузі Доручень переказу на телефон BLIK автоматично актуалізує номер телефону, визначений у Послузі Прохання переказу BLIK.
4. Рахунком , дебетованим в рамках Послуги BLIK, для обслуговування Доручень переказу на телефон BLIK та Прохання переказу BLIK є зареєстрований платіжний рахунок, який є ощадно-розрахунковим рахунком в– злотих ;
5. Доручення переказу на телефон BLIK, що виходять з Банку, можливі лише тоді, коли номер телефону одержувача зареєстрований в базі даних телефонів BLIK, тоді вони виконуються як:
   a. доручення внутрішнього переказу, якщо рахунок одержувача є рахунком в Банку,

b. платіжні доручення Express Elixir, якщо рахунок одержувача є рахунком, який не ведеться в Банку.

MojeID

§21

1. Системою MojeID можуть користуватися всі Користувачі, які мають видані Банком засоби електронної ідентифікації.
2. Засіб електронної ідентифікації містить Ідентифікаційні дані.
3. Засоби електронної ідентифікації можуть бути видані лише Користувачам з ідентифікацією, підтвердженою Банком.
4. Засіб електронної ідентифікації видається на визначений термін.
5. Ідентифікаційні дані для фізичних осіб включають:
   a. прізвище;
   b. ім'я або імена;
   c. дату народження;
   d. PESEL.
6. Зміна ідентифікаційних даних Користувачем призводить до втрати чинності актуальних Засобів електронної ідентифікації та заміни їх новими.
7. У системі MojeID додаткові дані можуть передаватися за згодою Користувача. Ці дані будуть надані як додаткові атрибути.

ПРАВИЛА БЕЗПЕКИ

§22

Надаючи послуги на підставі цих Правил, Банк зобов'язується забезпечити Користувачеві безпеку виконання Розпоряджень з належною ретельністю та з використанням відповідних технічних рішень.

§23

Користувач не може подавати неправомірні дані та зобов'язаний дотримуватися вказівок Банку щодо правил безпеки при використанні Електронних каналів зв'язку; зокрема, Користувач повинен ретельно захистити дані, які використовуються для входу в Електронні канали (Ідентифікатор, включаючи біометричні ідентифікатори, паролі, PIN-коди) та мобільний телефон, номер якого вказано в Банку як Телефон для кодів авторизації, і зобов'язаний щоразу уважно читати зміст SMS-повідомлення, що містить код авторизації або PUSH-повідомлення, щоб перевірити його відповідність поданому ним Розпорядженню. Користувач також зобов'язаний належним чином захистити пристрій із встановленим Мобільним додатком.

§24

Користувач зобов'язаний негайно повідомити Банк та негайно змінити PIN-пароль або заблокувати Електронні канали у разі:

1. розкриття або передачі даних для входу третім особам або підозри на таку подію,
2. несанкціонованого використання Електронних каналів зв'язку,
3. виявлення неавторизованих транзакцій і операцій на своїх рахунках,
4. втрати або крадіжки даних для входу,
5. зміни, втрати або розкриття третім особам номера телефону, який використовується для зв'язку з Банком, зокрема номера, який використовується для авторизації операцій,
6. втрати мобільного пристрою, що дозволяє користуватися мобільним банкінгом,
7. підозри на зараження пристрою зловмисним програмним забезпеченням.

§25

Банк залишає за собою право ввести додаткові обмеження та запобіжні заходи щодо розпоряджень, розміщених в Електронних каналах зв'язку, у разі важливих обставин, що виправдовують введення таких заходів.

§26

1. Детальна інформація про принципи безпечного використання Електронних каналів зв'язку та ризики, пов'язані з їх використанням, вказана в §27 та розміщена на веб-сайтах Банку, а також надається консультантами Контакт-центру.
2. Користувач зобов'язаний дотримуватися правил безпечного використання Електронних каналів зв'язку, а в разі їх недотримання діє на власний ризик і несе відповідальність за наслідки такого порушення.

§27

Користувач визнає, що електронний доступ до систем Інтернет-банкінгу, мобільного та телефонного банкінгу пов'язаний з ризиком – зокрема, у разі недотримання визначених Банком правил безпеки. Цей ризик включає:

1. Втрату або крадіжку неуповноваженими особами даних або пристроїв:
   a. що використовуються для входу в систему (наприклад, ідентифікатор, включаючи біометричний ідентифікатор, PIN-код для мобільного додатка),
   b. що використовується для затвердження транзакцій (наприклад, мобільний пристрій із встановленим додатком).
2. Випадки атак соціальної інженерії, під час яких треті сторони, видаючи себе за Банк, переконують Користувача затвердити операцію (наприклад, неправдива інформація про необхідність придбання транзакції).
3. Несвідоме затвердження Користувачем непланованих доручень (наприклад, без читання операції, описаної в Коді авторизації або в PUSH-повідомленні).
4. Використання при користуванні електронними каналами зв'язку пристроїв, над якими треті сторони взяли контроль віддалено або фізично (наприклад, за допомогою шкідливих програм, наприклад вірусів).
5. Наслідками виникнення вищезазначених подій можуть бути:
   a. доступ третьої сторони до даних Користувача, доступних в Електронних каналах зв'язку,
   b. можливість виконувати топерації транзакції третіми особами від імені Користувача, в тому числі фінансові (наприклад, виконання платіжних доручень),
   c. можливість затвердження Користувачем небажаної транзакції.

§28

При використанні Інтернет-банкінгу та Мобільного банкінгу Банк рекомендує використовувати веб-браузери, пристрої та операційні системи з рекомендаційного списку, розміщеного на сайті Банку. Банк не несе відповідальності за будь-які порушення в роботі Інтернет-банкінгу та Мобільного банку у разі використання браузерів, що не входять до цього переліку.

§29

Основні правила безпеки при використанні електронних каналів зв'язку:

1. Ви завжди повинні перевіряти правильність адреси для входу в Інтернет-банкінг (https://system.aliorbank.pl/). При вході зверніть увагу на те, чи не відображає браузер попередження, пов'язані з сертифікатом безпеки (перевірте та зверифікуйте його реквізити) і з

префіксом HTTPS в адресі сторінки входу, який підтверджує, що підключення до сторінки системи Інтернет-банкінгу зашифровано.
2. Вам слід уважно читати вміст Кодів авторизації та Повідомлень PUSH- авторизації. Перш ніж підтвердити операцію, уважно прочитайте весь зміст SMS-повідомлення або PUSH-повідомлення авторизації. Банк ніколи не просить підтвердити операцію, яка не була замовлена Користувачем.
3. Банк рекомендує регулярно оновлювати операційну систему та встановлене на ній програмного забезпечення, зокрема антивірусне програмне забезпечення (включаючи базу сигнатур вірусів) та використовуваний веб-браузер.
4. Не використовуйте ненадійні пристрої для входу в Інтернет-банкінг (наприклад, в інтернет-кафе) або на комп'ютері, на який ввійшов інший користувач – також не варто використовувати для цього загальнодоступні мережі Wi-Fi.
5. Не слід використовувати ненадійні пристрої для встановлення Мобільного додатка та входу в нього – також не варто використовувати для цього загальнодоступні мережі Wi-Fi.
6. Слід звернути особливу увагу на атаки, спрямовані на те, щоб переконати вас виконати певну дію (наприклад, натиснути на посилання, завантажити програмне забезпечення, надати свої дані), схвалити PUSH-повідомлення авторизації, які надсилаються електронною поштою, SMS/MMS повідомленнями, в соціальних мережах, або передаються по телефону.
7. Банк рекомендує не відкривати додатки та не використовувати посилання з підозрілих електронних листів (наприклад, з граматичними помилками, описками, неточною граматикою; з адреси, відмінної від офіційної, що не очікувалися тощо), а також не відповідати на них. Підроблені електронні листи є найпоширенішою причиною зараження комп'ютера небезпечними шкідливими програмами.
8. Важливі дані (адреса, номери PESEL, паролі, логіни та інші конфіденційні дані) повинні бути належним чином захищені. Для Користувача неприпустимо передавати свої дані ненадійним юридичним або фізичним особам. Ви повинні захистити свої документи, а в разі втрати чи крадіжки – негайно застерегти їх. Зверніть увагу, що злочинці можуть використати перехоплення ваших даних для крадіжки вашої особи, даних або коштів.
9. Звертайте увагу на інформацію про нові загрози – на сайтах Банку є інформація про те, як їх розпізнати та уникнути (у розділі Нові загрози та через інформаційні банери на сторінці входу).
10. Зверніть увагу на зміст сторінки входу в Інтернет-банкінг. Якщо процес входу виглядає інакше, ніж зазвичай (наприклад, займає набагато більше часу, з'являються нові вікна, користувачеві пропонується виконати додаткові дії), слід негайно звернутися до Контакт-центру – це може означати, що комп'ютер заражений шкідливим програмним забезпеченням.
11. Користувач несе повну відповідальність за операції та дії, здійснені особами, яким він розкрив дані для входу або надав пристрій, що використовується для автентифікації та/або авторизації операцій в Електронному каналі зв'язку, а також за дії та операції, що сталися в результаті порушення користувачем положень цих Правил.
12. Користувач зобов'язується захищати доступ до свого мобільного пристрою та приймає до відома, що отримання його зареєстрованих біометричних ідентифікаторів третіми особами може призвести до несанкціонованого доступу цих третіх осіб до Мобільного додатка.
13. Користувач несе відповідальність за дозвіл третім особам реєструвати свої біометричні ідентифікатори на мобільному пристрої, на якому встановлено Мобільний додаток з функцією входу за відбитком пальців.
14. Про зміну номера мобільного телефону Користувач зобов'язаний повідомити Банк у письмовій або електронній формі, як тільки виникає така ситуація. Користувач несе відповідальність за негативні наслідки у разі відсутності такої актуалізації.
15. У разі запитань/занепокоєння щодо безпеки послуг банку або повідомлення про інцидент безпеки, зверніться до Контакт-центру або будь-якого відділення Alior Bank.
16. У разі виникнення сумнівів щодо достовірності повідомлень безпеки, отриманих електронною поштою чи іншим каналом, їх необхідно порівняти з інформацією на сайті Банку в розділі Безпека.
17. Будь-яка інформація про інциденти безпеки (не стосується індивідуальних випадків) розміщується на веб-сайтах Банку в розділі Безпека.

БЛОКУВАННЯ ТА ВІДМОВА ВІД ЕЛЕКТРОННИХ КАНАЛІВ ЗВ'ЯЗКУ

§ 30

1. Під блокуванням слід розуміти неможливість Користувача використовувати даний Електронний канал.
2. Блокування Інтернет-банкінгу та блокування Мобільного банкінгу можуть відбуватися як спільно, так і незалежно один від одного.

§31

1. Кожен з електронних каналів може бути заблокований Користувачем:
   a. шляхом надання Розпоряджень консультанту Контакт-центру,
   b. в Установі Банку,
   c. в результаті перевищення ліміту неправильних спроб входу, встановленого для даного Електронного каналу.
2. Інтернет-банкінг може бути заблокований в результаті:
   a. перевищення ліміту 5 неправильних послідовних спроб входу,
   b. перевищення ліміту 5 неправильних послідовних спроб авторизації Розпорядження.
3. Блокування Мобільного додатка може статися в результаті:
   a. перевищення ліміту 5 неправильних послідовних спроб входу,
   b. перевищення ліміту 5 неправильних послідовних спроб авторизації Розпорядження.
4. Кожен з електронних каналів може бути заблокований Банком на підставі аналізу даних системи у разі:
   a. загрози перехоплення даних доступу Користувача зловмисним програмним забезпеченням,
   b. використання даних доступу Користувача програмним забезпеченням, яке автоматично входить в систему з високою частотою,
   c. використання систем або рахунків у спосіб, що не відповідає чинному законодавству,
   d. здійснення дій, які можуть загрожувати безпеці системи та даних, що обробляються в ній,
   e. підозри Банку в тому, що третя особа отримала доступ до Електронних каналів Користувача,
   f. відсутність активації Користувачем Електронного каналу протягом трьох місяців з моменту підписання Договору,
   g. перенесення Користувача в іншу систему Інтернет-банкінгу, коли доступ у вихідній системі був заблокований.
5. Одразу після блокування Банк запускає процедуру оповіщення, яка полягає в спробі зв'язатися з Користувачем через доступні канали зв'язку для

з’ясування ситуації. Це не стосується ситуації, описаної в п 4 літ. f.

§32

Користувач може розблокувати:

1. Телефонний банкінг – шляхом Розпорядження, поданого консультанту Контакт-центру, в Установі Банку або самостійно в Інтернет-банкінгу, якщо цей канал активний,
2. Інтернет-банкінг та Мобільний банкінг:
   a. в Установі Банку,
   b. шляхом надання Розпорядження консультанту Контакт-центру,
   c. через форму, доступну на сторінці входу в Інтернет-банкінг (дійсна з моменту надання форми Банком, після повідомлення Користувача не пізніше ніж за 7 днів до дати надання форми, через Електронні канали {2]).

§33

1. Для укладення Договору необхідна письмова форма або інша форма, рівна письмовій.
2. Договір укладається на невизначений строк і може бути розірваний будь-якою із сторін у письмовій формі. Розірвання договору не впливає на дію укладених на його основі Договорів продуктів, що пропонуються Банком для фізичних осіб.
3. Після припинення дії Договору Користувач більше не зможе використовувати Електронні канали зв'язку.
4. Якщо Договір укладено за межами Установи Банку, Користувач може розірвати його протягом 14 днів з дня його укладення без пояснення причин шляхом подання відповідної заяви до Банку.

§34

Банк має право тимчасово відключити Електронні канали після попереднього розміщення відповідного повідомлення на сайті Банку.

СИЛЬНА АВТЕНТИКАЦІЯ КОРИСТУВАЧА

§35

1. Банк застосовує Сильну автентифікацію, коли:
   a. Користувач отримує онлайн-доступ до свого рахунку за допомогою Інтернет-банкінгу або Мобільного банкінгу або
   b. Користувач ініціює платіжну операцію через Інтернет-банкінг або Мобільний банкінг або
   c. Користувач через Інтернет-банкінг або мобільний банкінг: ініціює створення або зміну шаблону платежу, зміну даних доступу до електронних каналів, зміну даних або методів, що використовуються в рамках Сильної автентифікації, зміну лімітів квоти в Електронних каналах зв'язку, зміну лімітів операцій для платіжної картки, активацію платіжної картки або токенізацію платіжної картки або
   d. Користувач платіжної картки, який також є Користувачем мобільного додатка, ініціює транзакцію типу e-commerce через Інтернет за допомогою платіжної картки на умовах, визначених Правилам про платіжні картки Alior Bank SA.
2. Для входу в Інтернет-банкінг Банк використовує застосовує Сильну автентифікацію за допомогою таких методів:
   a. Користувач подає Ідентифікатор доступу та Пароль, а потім:
      i. у разі входу за допомогою Коду авторизації – Користувач вводить Код авторизації в Інтернет-банкінг;
      ii. у разі входу за допомогою PUSH-повідомлення – Користувач підтверджує повідомлення на Пристрої за замовчуванням. Крім того, Користувач може відсканувати відображений QR-код за допомогою Пристрою за замовчуванням, а потім ввести отриманий одноразовий код в Інтернет-банкінг.
   b. Користувач може визначити пристрій, з якого здійснюється вхід, як виділений пристрій. У цьому випадку користувач вибирає в Інтернет-банкінгу даний пристрій як виділений пристрій і зобов'язується забезпечити, щоб він був єдиним користувачем цього виділеного пристрою. Потім при кожному вході в систему Банк перевіряє, чи Користувач входить за допомогою спеціального пристрою. Вхід в систему відбувається після введення Користувачем ідентифікатора та Пароля, а потім верифікації пристрою, виділеного Банком.
   c. Вхід за допомогою спеціального пристрою може відбуватися протягом періоду, визначеного Банком, але Банк може вимагати автентифікації з використанням коду авторизації або PUSH-повідомлення також з міркувань безпеки.
   d. Сильна автентифікація Користувача також може бути виконана після подачі Ідентифікатора та Пароля, а потім на основі його Поведінкового профілю.
3. Сильна автентифікація для входу в Мобільний додаток здійснюється через
   a. перевірку Банком пристрою з активним мобільним додатком, а потім:
      i. у разі входу за допомогою ПІН-коду авторизації – введення Користувачем ПІН-коду авторизації в Мобільному додатку;
      ii. у разі входу за допомогою біометричної автентифікації – автентифікація Користувача за допомогою Біометричного ідентифікатора.
      iii. Перевірка Банком користувача на основі його Поведінкового профілю.

§36

Користувач заявляє, що він є єдиним власником спеціального пристрою, зазначеного в §35 абз. 2b і абз 3., і зобов'язується не надавати цей пристрій третім особам.

§37

Банк надає постачальникам послуг доступ до інформації про рахунок, постачальникам послуг ініціювання платежів та постачальникам платіжних послуг, що випускають платіжні інструменти на основі картки – Банк надає спеціальний інтерфейс доступу для надання цих послуг.

Скарги (Рекламації)

§38

1. Банк розглядає скарги/рекламації негайно, не пізніше 15 робочих днів (стосується надання платіжних послуг) або 30 календарних днів (в інших випадках) з дня отримання скарги/рекламації.
   У разі платіжних послуг – в особливо складних випадках, які унеможливлюють розгляд скарги/рекламації та відповіді протягом вищезазначеного терміну Банк:
   1) пояснює причину затримки;
   2) зазначає обставини, які необхідно встановити для розгляду справи;
   3) вказує передбачуваний термін розгляду скарги/рекламації та відповіді на неї, який не може перевищувати 35 робочих днів з дня отримання скарги/рекламації.

   В інших особливо складних випадках (не пов'язаних з платіжними послугами) цей строк може бути продовжений, але не більше ніж на 60 календарних днів з дня надходження скарги/рекламації. Користувачу буде повідомлено про причини затримки, обставини, які потребують з'ясування, та

очікувану дату розгляду скарги/рекламації та реагування на неї.
2. Користувач зобов’язаний надати Банку всю інформацію та документацію щодо скарги/рекламації та співпрацювати з Банком до розгляду скарги.
3. Скаргу/рекламацію можна подати:
   a. безпосередньо в Установі Банку,
   b. по телефону Контакт-центру,
   c. через систему Інтернет-банкінгу (для авторизованого Користувача),
   d. через Мобільний додаток (для авторизованого Користувача),
   e. листом – на адресу для кореспонденції Банку.
4. Відповідь на скаргу може бути надана:
   a. листом,
   b. через систему Інтернет-банкінгу (для авторизованого Користувача),
   c. через Мобільний додаток (для авторизованого Користувача),
   d. за допомогою SMS-повідомлення,

   а в обґрунтованих випадках додатково:
   e. телефоном,
   f. в Установі Банку.
5. Користувач, який не задоволений способом розгляду скарги/рекламації, має право звернутися у справі спору що стосується відносин з Банком:
   a. до Банківського арбітра – у позасудовому порядку для вирішення спору (детальна інформація про Банківський споживчий арбітраж розміщена на сайті Банку, в реєстрі уповноважених суб’єктів, який ведеться Президентом УОКіК та на веб-сайті www. zbp.pl);
   b. до Фінансового Омбудсмена – у порядку оскарження або позасудового вирішення спорів (детальна інформація доступна на сайті www.rf.gov.pl).

Прикінцеві Правила
§39

1. За діяльність, пов’язану з наданням та обслуговуванням Електронних каналів зв’язку, Банк стягує збори і комісії згідно з чинним Тарифом зборів і комісій Alior Bank S.A. для Індивідуальних клієнтів або Брокерського дому, де вказано:
   1) суму і правила справляння плати і комісії за дії, пов'язані з обслуговуванням і зміною договору,
   2) терміни, розміри та правила зміни зборів і комісій,
   3) правила і порядок інформування про зміни Тарифу зборів і комісій.
2. Банк залишає за собою право відмовитися від стягування зборів і комісій.
3. Діючий Тариф зборів і комісій доступний на веб-сайті Банку та в Установах Банку.

§40

1. Банк залишає за собою право вносити зміни до Правил, якщо виникає хоча б одна з наступних причин:
   a. зміна функціонування продуктів і послуг, які пропонує Банк; включаючи відкликання продукту або послуги, до яких застосовуються Правила,
   b. введення Банком нових продуктів або послуг, до яких застосовуватимуться положення Правил;
   c. зміна інформаційних систем, що використовуються для обслуговування пропонованих Банком продуктів і послуг, до яких застосовуються Правила;
   d. зміна законодавства:
      1) регулювання продуктів або послуг, що пропонуються Банком; на які поширюються Правила;
      2) що впливають на виконання договору або Правил;
   e. зміна або винесення нових судових рішень, ухвал адміністративних органів, наказів чи рекомендацій уповноважених органів, у тому числі Комісії фінансового нагляду – в обсязі, пов'язаному з виконанням договору або Регламенту.

   У разі внесення змін до Правила, Банк надає Користувачеві зведений текст Правил. Правила або перелік змін до Правила будуть передані тільки в електронному вигляді (в електронній формі на адресу електронної пошти, надану Власником, або через веб-сайт у вигляді електронного файлу, наданого на ньому та збереженого на жорсткому носії після попереднього повідомлення, зокрема листом, SMS, електронною поштою, про наявність інформації про зміни до цих Правил на цьому веб-сайті. Крім того, Банк також може надавати інформацію про внесення змін до цих Правил в Інтернет-банкінгу) не пізніше ніж за 2 місяці до запропонованої дати набрання ними чинності, з урахуванням абз. 5. Відсутність заперечення Користувача щодо запропонованих змін рівносильна згоді на них.
2. Правила, надані в порядку, зазначеному в абз. 1, вважаються наданими.
3. Користувач має право розірвати Договір негайно до дати набуття чинності запропонованих змін. З цього приводу з нього не будуть стягуватися жодні збори, пов’язані із розірванням Договору, або збори, що випливають із запропонованих змін.
4. Якщо Користувач не дасть своєї згоди, відповідно до абз. 1, але не повідомить про намір розірвати Договір, Договір закінчить свою дію з днем, що передує даті набрання чинності пропонованих змін, без сплати зборів, пов'язаних із заявленим запереченням або зборів, що випливають із пропонованих змін.
5. У разі зміни Правил з приводу розширення діапазону дій, які можливі до виконання Власником, Банк інформує Користувача про зміну Правил у загальноприйнятому порядку в Установі Банку, на сайтах Банку або через Електронні канали, а при відсутності можливості використання Електронних каналів – поштою або на електронну адресу, вказану Користувачем. Змінені Правила набувають чинності з моменту їх введення.

§41

1. Банк залишає за собою право надавати певні послуги в рамках Електронних каналів зв’язку через зовнішні організації, зокрема дочірні компанії. Дані, передані цим особам, є об’єктами банківської таємниці та положень нормативно-правових актів про захист даних і захищені в тому ж обсязі, що й у випадку Банку. Банк несе повну відповідальність за операції, що здійснюються за посередництвом цих суб’єктів.
2. Застосування поведінкового профілю спрямоване на забезпечення Користувачеві правил безпеки, зазначених у §22 цих Правил. Правовою основою обробки даних на основі Поведінкового профілю є ст. 9 абз. 2 літ. g Регламенту Європейського Парламенту та Ради (UE) 2016/679 від 27 квітня 2016 року «Про захист фізичних осіб у зв’язку з обробкою персональних даних та про вільне переміщення таких даних», а також про відхилення Директиви 95/46/WE (загального розпорядження про захист персональних даних), тобто «обробка необхідна з причин, пов’язаних із важливим суспільним інтересом на основі законодавства ЄС або законодавства держави-члена». Цим законом є законодавчі акти:

a. ст. 97 – 98 Директиви Європейського Парламенту та Ради (UE) 2015/2366 від 25 листопада 2015 року Про платіжні послуги на внутрішньому ринку та внесення змін до Директив 2002/65/WE, 2009/110/WE, 2013/36/UE та Регламенту (UE) № 1093/2010 та скасування Директиви 2007/64/WE (Директиви PSD2),
b. ст. 2 та ст. 18 Делегованого Регламенту Комісії (UE) 2018/389 від 27 листопада 2017 року, що доповнює Директиву Європейського Парламенту та Ради (UE) 2015/2366 «Щодо нормативних технічних стандартів для надійної автентифікації клієнтів і спільних та безпечних відкритих стандартів зв'язку»,
c. ст. 10 Закону від 19 серпня 2011 року «Про платіжні послуги».