Allgemeine Bedingungen für die Teilnahme am Onlinebanking (Onlineservice)

1 Leistungsangebot

1.1 Im Onlineservice der Ikano Bank AB (publ), Zweigniederlassung Deutschland (im Folgenden Ikano Bank genannt) kann der Kunde in dem von der Ikano Bank angebotenen Umfang Bankgeschäfte abwickeln und Informationen abrufen. Er kann zusätzlich für berechtigte Produkte für die Mitteilung von Informationen über ein Zahlungskonto einen Kontoinformationsdienst gemäß §1 Abs. 34 ZAG nutzen.

1.2 Zur Nutzung des Onlineservice gelten die mit der Ikano Bank gesondert vereinbarten Verfügungslimits.

2 Voraussetzungen zur Nutzung des Onlineservice

Um den Onlineservice der Ikano Bank in vollem Umfang nutzen zu können, benötigt der Kunde die mit der Ikano Bank vereinbarten personalisierten Sicherheitsmerkmale und Authentifizierungsinstrumente. Mit diesen kann der Kunde sich gegenüber der Ikano Bank als berechtigter Teilnehmer ausweisen (authentifizieren) und Aufträge autorisieren.

2.1 Zwei-Faktor-Authentifizierung

Für bestimmte Produkte benötigt der Kunde für die Authentifizierung eine sogenannte Zwei-Faktor-Authentifizierung. Hierfür muss der Kunde zwei von den folgenden drei Faktoren zur Authentifizierung erfüllen:

- Wissenselement - etwas, das nur der Kunde weiß (z. B. die persönliche Identifikationsnummer [PIN] oder das persönliche Passwort),
- Besitzelement, etwas, was nur der Kunde besitzt (z. B. das mobile Endgerät), oder
- Seinselement, etwas, das der Kunde ist (Inhärenz, z. B. Fingerabdruck als biometrisches Merkmal des Kunden).

Der Kunde benötigt für eine Zwei-Faktor-Authentifizierung zwingend ein mobiles Endgerät, das zunächst bei der Bank über eine Anmeldung zu authentifizieren ist. Der Kunde hat hierzu zur Verwendung des mobilen Endgeräts auf diesem eine Ikano-Anwendung (Ikano Bank Secure App) herunterzuladen. Für diese gelten eigene Geschäfts- und Nutzungsbedingungen. Der Kunde ist selbst für die Beschaffung, Installation, Wartung und Pflege des mobilen Endgerätes und der Anwendung verantwortlich. Für die Authentifizierung seines mobilen Endgerätes wird dem Kunden ein Freischalt-Code (Initialcode) übermittelt. Dieses kann auf jede Weise erfolgen, die eine sichere Datenübermittlung zulässt, z.B. per Post.

2.2 Authentifizierungsinstrumente

Authentifizierung ist das mit der Bank vereinbarte Verfahren, mit dessen Hilfe die Bank die Identität des Kunden oder die berechtigte Verwendung eines bestimmten Zahlungsinstruments, einschließlich der Verwendung des personalisierten Sicherheitsmerkmals des Kunden überprüfen kann. Der Kunde kann sich mit den hierfür vereinbarten Authentifizierungselementen gegenüber der Bank als berechtigt ausweisen und sofern möglich auf Informationen zugreifen oder Aufträge erteilen. Authentifizierungsinstrumente sind personalisierte Instrumente oder Verfahren, deren Verwendung zwischen der Ikano Bank und dem Kunden vereinbart wurde und die vom Teilnehmer zur Erteilung eines Online-Service-Auftrags verwendet werden. Insbesondere mittels folgender Authentifizierungsinstrumente kann das personalisierte Sicherheitsmerkmal dem Teilnehmer zur Verfügung gestellt wer- den, wobei nicht alle Authentifizierungsinstrumente jederzeit von der Ikano Bank angeboten werden müssen:

- PIN Brief
- Online Service App auf einem mobilen Endgerät (z.B. Mobiltelefon) zur Erzeugung eines Einmalpasswortes oder zur Freigabe mittels biometrischer Kennzeichen.
- ein sonstiges Authentifizierungsinstrument, auf dem sich Signaturschlüssel befinden.

3 Zugang zum Online-Banking

Der Kunde erhält Zugang zum Onlineservice der Ikano Bank, wenn

- er sich mithilfe der relevanten Authentifizierungsinstrumente authentifiziert und Ikano das Online-Banking für den Kunden freigeschaltet hat,
- die Prüfung der Daten bei der Ikano Bank eine Zugangsberechtigung ergeben hat und
- keine Sperre des Zugangs (vgl. 8.1 und 9) vorliegt.
- Nach Gewährung des Zuganges kann der Kunde Informationen abrufen und Aufträge erteilen. Das gilt auch, wenn Du Zahlungskontoinfor- mationen über einen Kontoinformationsdienst anforderst.

4 Online-Service Aufträge

4.1 Auftragserteilung und Autorisierung

Bestimmte Transaktionen bedürfen zu ihrer Wirksamkeit einer Autorisierung mittels der von der Ikano Bank bereitgestellten Autorisierungsmethode. Die Ikano Bank bestätigt den Eingang des Auftrages mit einer Meldung im Onlineservice.

4.2 Widerruf von Aufträgen

Die Widerrufbarkeit eines erteilten Auftrages richtet sich nach den für die jeweilige Auftragsart geltenden Bedingungen (z. B. Bedingungen für den Überweisungsverkehr). Der Widerruf von Aufträgen kann nur außerhalb des Onlineservices erfolgen, es sei denn, die Ikano Bank sieht eine Widerrufsmöglichkeit im Onlineservice ausdrücklich vor.

5 Bearbeitung von Online-Banking- sowie Telefax-Aufträgen durch die Bank

5.1 Die Bearbeitung der Aufträge erfolgt an den für die Abwicklung der jeweiligen Auftragsart im „Preis und Leistungsverzeichnis" bekannt gegebenen Geschäftstagen im Rahmen des ordnungsgemäßen Arbeitsablaufes. Geht der Auftrag nach dem im „Preis- und Leistungsverzeichnis" bestimmten Zeitpunkt (Annahme-frist) ein oder fällt der Zeitpunkt des Eingangs nicht auf einen Geschäftstag gemäß „Preis und Leistungs-verzeichnis", so gilt der Auftrag als am darauffolgenden Geschäftstag zugegangen. Die Bearbeitung beginnt erst an diesem Tag.

5.2 Die Ikano Bank wird den Auftrag nach Maßgabe der Bestimmungen der für die jeweilige Auftragsart geltenden Bedingungen (z. B. Bedingungen für den Überweisungsverkehr) ausführen, wenn folgende Ausführungsbedingungen vorliegen:

- Der Kunde hat den Auftrag autorisiert und, sofern für den Auftrag erforderlich, die notwendige Authentifizierung mittels einer 2-Faktor-Authentifizierung vorgenommen.
- Eine Berechtigung für die jeweilige Auftragsart liegt vor.
- Das Datenformat für den Onlineservice ist eingehalten.
- Das vereinbarte Onlineservice -Verfügungslimit ist nicht überschritten.
- Die Ausführungsvoraussetzungen nach den für die jeweilige Auftragsart maßgeblichen Bedingungen (z. B. ausreichende Kontodeckung gemäß Bedingungen für den Überweisungsverkehr) liegen vor.

5.3 Liegen diese Ausführungsbedingungen nicht vor, wird die Ikano Bank den Auftrag nicht ausführen und im Onlineservice eine Information über die Nichtausführung anzeigen. Soweit möglich, wird die Ikano Bank auch Möglichkeiten aufzeigen, mit denen Fehler, die zur Ablehnung geführt haben, berichtigt werden können.

6 Informationen über Verfügungen per Onlineservice

Die Ikano Bank unterrichtet den Kunden mindestens einmal jährlich über die getätigten Verfügungen auf dem für Kontoinformationen vereinbarten Weg.

7 Sorgfaltspflicht

7.1 Technische Verbindung zum Onlineservice

Aus Sicherheitsgründen ist der Kunde verpflichtet, die technische Verbindung zum Onlineservice nur über die von der Ikano Bank gesondert mitgeteilten Onlineservice-Zugangskanäle (z.B. Internetadresse) herzustellen.

Zur Erteilung von Zahlungsaufträgen und zum Abruf von Informationen über ein Zahlungskonto kann der Kunde die Verbindung zum Online-Banking auch über einen Kontoin- formationsdienst herstellen.

7.2 Sicherheit des Kundensystems

Der Kunde muss die Sicherheitshinweise auf der Internetseite der Ikano Bank zum Onlineservice, insbesondere die Maßnahmen zum Schutz der eingesetzten Hard- und Software (Kundensystem) beachten. Hierzu gehören insbesondere die Installation und regelmäßige Aktualisierung einer handelsüblichen Antivirensoftware, die Installation einer Firewall sowie regelmäßige Sicherheits-Updates für den verwendeten Browser.

7.3 Geheimhaltung der personalisierten Sicherheitsmerkmale und sichere Aufbewahrung der Authentifizierungsinstrumente

7.3.1 Der Kunde muss

- seine Wissenselemente (personalisierten Sicherheitsmerkmale) geheim halten sowie
- seine Besitzelemente vor dem Zugriff anderer Personen sicher verwahren und vor Missbrauch schützen. Der Kunde hat insbesondere Sorge dafür zu tragen, dass kein Dritter auf sein mobiles Endgerät zugreifen oder Anwendungen auf dem mobilen Endgerät für das Online-Banking nutzen kann.
- Den Initialcode für die Aktivierung der Anwendung auf dem mobilen Endgerät geheimhalten.
- Dafür Sorge tragen, dass seine Seins-Elemente nur dann als Authentifizierungselement verwendet werden, sofern auf seinem mobilen Endgerät keine anderen Seins-Elemente anderer Personen gespeichert werden.

Die Geheimhaltungspflicht bezüglich der personalisierten Sicherheitsmerkmale wird nicht verletzt, wenn der Kunde diese zum Abruf von Informationen über ein Zahlungskonto an den von ihm ausgewählten Kontoinformations- dienst übermittelt.

7.3.2 Insbesondere ist Folgendes zum Schutz des personalisierten Sicherheitsmerkmals sowie des Authentifizierungsinstruments zu beachten:

- Personalisierte Sicherheitsmerkmale dürfen nicht ungesichert elektronisch gespeichert werden
- Bei Eingabe des personalisierten Sicherheitsmerkmals ist sicherzustellen, dass andere Personen dieses nicht ausspähen können.
- Das personalisierte Sicherheitsmerkmal darf nicht per E-Mail weitergegeben werden.
- Das personalisierte Sicherheitsmerkmal (z.B. PIN) darf nicht zusammen mit dem Authentifizierungsinstrument verwahrt werden.
- Für die Nutzung des Onlineservice und für die Freigabe mittels biometrischer Kennzeichen oder die Erzeugung eines Einmalpasswortes müssen unterschiedliche Geräte verwendet werden.

7.4 Kontrolle der Auftragsdaten mit den von der Ikano Bank angezeigten Daten

Soweit die Ikano Bank dem Teilnehmer Daten aus seinem Online-Service-Auftrag im Kundensystem oder über ein anderes Gerät des Teilnehmers (z.B. Mobiltelefon) zur Bestätigung anzeigt, ist der Teilnehmer verpflichtet, vor der Bestätigung die Übereinstimmung der angezeigten Daten mit den für die Transaktion vorgesehenen Daten zu prüfen.

8 Anzeige- und Unterrichtungspflichten

8.1 Sperranzeige

8.1.1 Stellt der Kunde den Verlust oder den Diebstahl des Authentifizierungsinstruments, die missbräuchliche Verwendung oder die sonstige nicht autorisierte Nutzung des Authentifizierungsinstruments oder seiner personalisierten Sicherheitsmerkmale fest, musst er die Ikano Bank hierüber unverzüglich unterrichten (Sperranzeige). Eine Sperranzeige kann jederzeit auch über eine gesondert mitgeteilte Telefonnummer aufgegeben werden.

8.1.2 Der Kunde muss jeden Diebstahl oder Missbrauch unverzüglich bei der Polizei zur Anzeige bringen.

8.1.3 Besteht Verdacht, dass eine andere Person unberechtigt - den Besitz am Authentifizierungsinstrument oder die Kenntnis des personalisierten Sicherheitsmerkmals erlangt hat oder das Authentifi- zierungsinstrument oder das personalisierte Sicherheitsmerkmal verwendet, ist ebenfalls eine Sperranzeige abzugeben.

8.2 Unterrichtung über nicht autorisierte oder fehlerhaft ausgeführte Aufträge

Nach Feststellung eines nicht autorisierten oder fehlerhaft ausgeführten Auftrages ist die Ikano Bank unverzüglich hierüber zu unterrichten.

9 Nutzungssperre

9.1 Sperre auf Veranlassung des Teilnehmers

Die Ikano Bank sperrt auf Veranlassung des Kunden, insbesondere im Fall der Sperranzeige nach Nummer 9.1, den Onlineservice-Zugang für den Kunden oder alle Teilnehmer oder sein Authentifizierungsinstrument.

9.2 Sperre auf Veranlassung der Ikano Bank

Die Ikano Bank wird den Zugang zum Onlineservice sperren, wenn

- sie berechtigt ist, den Vertrag zum Onlineservice aus wichtigem Grund zu kündigen,
- sachliche Gründe im Zusammenhang mit der Sicherheit des Authentifizierungsinstruments oder des personalisierten Sicherheitsmerkmals dies rechtfertigen oder
- der Verdacht einer nicht autorisierten oder einer betrügerischen Verwendung des Authentifizierungsinstruments besteht.

Die Ikano Bank wird den Kunden unter Angabe der hierfür maßgeblichen Gründe möglichst vor, spätestens jedoch unverzüglich nach der Sperre auf dem vereinbarten Weg informieren.

9.3 Aufhebung der Sperre

Die Ikano Bank hebt eine Sperre auf oder tauscht das personalisierte Sicherheitsmerkmal aus, wenn die Gründe für die Sperre nicht mehr gegeben sind. Hierüber wird der Kunde unverzüglich informiert.

10 Haftung

10.1 Die Haftung der Ikano Bank bei nicht autorisierten, nicht oder fehlerhaft oder verspätet ausgeführten Onlineservice-Verfügungen

Die Haftung der Ikano Bank bei nicht autorisierten, nicht oder fehlerhaft oder verspätet ausgeführten Onlineservice-Verfügungen richtet sich nach den für die jeweilige Auftragsart vereinbarten Sonderbedingungen(z. B. Sonderbedingungen für den Überweisungsverkehr).

10.2 Haftung des Kunden bei missbräuchlicher Nutzung seiner Authentifizierungsinstrumente

10.2.1 Haftung des Kunden für nicht autorisierte Zahlungsvorgänge vor der Sperranzeige

10.2.1.1 Beruht ein nicht autorisierter Zahlungsvorgang vor der Sperranzeige auf der Nutzung eines verloren gegangenen oder gestohlenen oder sonst abhanden gekommenen Authentifizierungsinstruments oder auf der sonstigen missbräuchlichen Verwendung eines Authentifizierungsinstruments, haftet der Kunde für den hierdurch entstehenden Schaden bis zu einem Betrag von 50 Euro, ohne dass es darauf ankommt, ob den Kunden ein Verschulden trifft.

10.2.1.2 Der Kunde ist nicht zum Ersatz des Schadens nach 10.2.1.1 verpflichtet, wenn es ihm nicht möglich war, (i) den Verlust, Diebstahl, das Abhandenkommen oder eine sonstige missbräuchliche Verwendung des Authentifizierungsinstruments vor dem nicht autorisierten Zahlungsvorgang zu bemerken oder (ii) der Verlust des Authentifizierungsinstruments durch einen Angestellten, Agenten, eine Zweigniederlassung eines Zahlungsdienstleisters oder eine sonstige Stelle, an die Tätigkeiten des Zahlungsdienstleisters ausgelagert wurden, verursacht worden ist.

10.2.1.3 Kommt es vor der Sperranzeige zu nicht autorisierten Zahlungsvorgängen und hat der Kunde in betrügerischer Absicht gehandelt oder seine Anzeige- und Sorgfaltspflichten nach diesen Bedingungen vorsätzlich oder grob fahrlässig verletzt, trägt er abweichend von 10.1.2.1 und 10.1.2.2 gehandelt den hierdurch entstandenen Schaden in vollem Umfang. Grobe Fahrlässigkeit kann insbesondere dann vorliegen, wenn er

- der Ikano Bank den Verlust oder Diebstahl oder die missbräuchliche Nutzung des Authentifizierungsinstruments oder des personalisierten Sicherheitsmerkmals nicht unverzüglich anzeigt, nachdem er hiervon Kenntnis erlangt hat (vgl. Nummer 8.1),
- das personalisierte Sicherheitsmerkmal ungesichert elektronisch gespeichert hat (vgl. Nummer 7.3.2, 1. Spiegelstrich),
- das personalisierte Sicherheitsmerkmal nicht geheim gehalten hat und der Missbrauch dadurch verursacht wurde (vgl. Nummer 7.3.1, 2. Spiegelstrich),
- das personalisierte Sicherheitsmerkmal per E-Mail, weitergegeben hat (vgl. Nummer 7.3.2, 3. Spiegelstrich),
- das personalisierte Sicherheitsmerkmal auf dem Authentifizierungsinstrument vermerkt oder zusammen mit diesem verwahrt hat (vgl. Nummer 7.3.2, 4. Spiegelstrich),
- für das Online-Banking und das Authentifizierungsinstrument das gleiche mobile Endgerät genutzt hat (vgl. Nummer 7.3.2, 5. Spiegelstrich).

10.2.1.4 Abweichend von 9.2.1.1 und 9.2.1.3 ist der Kunde nicht zum Schadenersatz verpflichtet, wenn die Ikano Bank von ihm eine starke Kundenauthentifizierung nach §1 Abs. 24 Zahlungsdiensteaufsichtsgesetz (ZAG) nicht verlangt hat, obwohl die Ikano Bank zur starken Kundenauthentifizierung nach §68 Abs. 4 ZAG verpflichtet war. Eine starke Kundenauthentifizierung erfordert insbesondere die Verwendung von zwei voneinander unabhängigen Elementen aus den Kategorien Wissen (etwas, das der Kunde weiß, z.B. Online-Kennwort), Besitz (etwas, das der Kunde besitzt, z.B. TAN-Generator) oder Inhärenz (etwas, das von dem Kunden selbst ist, z.B. Fingerabdruck).

10.2.1.5 Die Haftung für Schäden, die innerhalb des Zeitraums, für den der Verfügungsrahmen gilt, verursacht werden, beschränkt sich jeweils auf den vereinbarten Verfügungsrahmen.

10.2.1.6 Der Kunde ist nicht zum Ersatz des Schadens nach 10.2.1.1 bzw. 10.2.1.3 verpflichtet, wenn er die Sperranzeige nach nicht abgeben konnte, weil die Ikano Bank nicht die Möglichkeit zur Entgegennahme der Sperranzeige sichergestellt hatte und der Schaden hierdurch eingetreten ist.

10.2.1.7 Die 10.2.1.2 und 10.2.1.4 bis 6 finden keine Anwendung, wenn der Kunde in betrügerischer Absicht gehandelt hat.

10.2.2 Haftung der Ikano Bank ab der Sperranzeige

Sobald die Ikano Bank eine Sperranzeige erhalten hat, übernimmt sie alle danach durch nicht autorisierte Verfügungen über ihren Onlineservice entstehenden Schäden. Dies gilt nicht, wenn der Kunde in betrügerischer Absicht gehandelt hat.

10.2.3 Haftungsausschluss

Haftungsansprüche sind ausgeschlossen, wenn die einen Anspruch begründenden Umstände auf einem ungewöhnlichen und unvorhersehbaren Ereignis beruhen, auf das der, der sich auf dieses Ereignis beruft, keinen Einfluss hat, und dessen Folgen trotz Anwendung der gebotenen Sorgfalt von ihm nicht hätten vermieden werden können.

Stand: 01.11.2024

Ikano Bank AB (publ), Zweigniederlassung Deutschland, Wettinerstraße 5, 65189 Wiesbaden, Deutschland, Telefon 06122 999 0, Fax 06122 999 799, E-Mail service@ikano.de, Amtsgericht Wiesbaden, HRB 28399;
Eingetragener Sitz der Ikano Bank AB (publ) - Aktiengesellschaft schwedischen Rechts: Älmhult, Schweden, Schwedisches Gesellschaftsregister (Bolagsverket) 516406-0922; Mitglieder des Vorstands (Styrelse): Mikael Palmquist, Peter van der Poel, Lars Ljungälv, Viveka Strangert, Diederick van Thiel, Heather Jackson; Vorstandsvorsitzende (Styrelseordförande): Lone Fønss Schrøder; Geschäftsführer (Verkställande Direktör): Niclas Olsson