Nutzungsbedingungen für das DHB Net- und Mobile-Banking

1. Leistungsumfang
Die DHB Bank N.V. (im folgenden „Bank“) bietet ihren Kunden verschiedene Möglichkeiten zur elektronischen Kontoführung an. Als Zugangsmedium steht das Net-Banking über die Homepage der Bank (www.dhbbank.de) und das Mobile-Banking über die DHB Bank App zur Verfügung. Der oder die Kontoinhaber:in und dessen oder deren Bevollmächtigte (im Folgenden beide einheitlich als „Kontoinhaber:in“ bezeichnet) können Bankgeschäfte in dem von der Bank angebotenen Umfang abwickeln.

2. Zugang
2.1. Mobile-Banking App herunterladen
Um die DHB Mobile-Banking App zu nutzen, benötigt der oder die Kontoinhaber:in bei der ersten Anmeldung den Benutzernamen und das Passwort. Nach der Registrierung kann die App mit einem individuell festgelegten Zugangscode verwendet werden. Es wird empfohlen, immer die neueste Version der App zu verwenden. Sobald eine neue Version der App verfügbar ist, wird diese in dem entsprechenden Online-Portal (Apple App Store oder Google Play Store) angezeigt.
2.2. Zugangsvoraussetzungen
Der oder die Kontoinhaber:in erhält Zugang zum Net- und Mobile-Banking der Bank, wenn die Benutzername und Kennwort bzw. der mobile PIN-Code richtig eingegeben werden und keine Nutzungssperre vorliegt. Für das Mobile-Banking kann der Zugriff auch über Fingerabdruck oder Gesichtserkennung erfolgen, sofern das Endgerät diese Funktionen unterstützt. Die Aktivierung dieser biometrischen Funktionen ist optional. Nach erfolgreichem Login können Informationen abgerufen und gemäß Abschnitt 3 Aufträge erteilt werden.

3. Aufträge
3.1 Auftragserteilung
Der oder die Kontoinhaber:in muss einem über das Net- oder Mobile-Banking erteilten Auftrag (z. B. einer Auszahlung) für dessen Wirksamkeit zustimmen (Autorisierung). Auf Aufforderung sind hierfür Authentifizierungselemente (z. B. die Eingabe einer MobileTIN) zu verwenden, um die Zustimmung zu erteilen. Die Bank bearbeitet die ihr mittels Net- oder Mobile-Banking ordnungsgemäß erteilten Aufträge im Rahmen des banküblichen Arbeitsablaufs. Erklärungen jeder Art (z. B. Kontostandsabfragen oder Überweisungsaufträge) gelten als abgegeben, wenn sie abschließend zur Übermittlung an die Bank freigegeben werden.
3.2 Widerrufbarkeit von Aufträgen
Die Bank führt keine manuelle Nachbearbeitung von fehlerhaften Aufträgen durch. Ein Widerruf oder eine Änderung von bereits final erteilten Aufträgen ist nicht möglich.

4. Finanzielle Nutzungsgrenze
Der oder die Kontoinhaber:in kann Verfügungen nur im Rahmen seines oder ihres Kontoguthabens vornehmen. Tägliche Verfügungen sind auf einen Höchstbetrag von € 25.000 begrenzt. Das Limit kann schriftlich mit dem Antrag "Änderung des Online-Überweisungslimits" auf bis zu € 50.000 erhöht oder bei Bedarf herabgesetzt werden.

5. Elektronisches Postfach
Die Bank stellt dem oder der Kontoinhaber:in ein elektronisches Postfach zur Verfügung. Über dieses Postfach übermittelt die Bank für die festgelegten Konten sämtliche Mitteilungen und Informationen, insbesondere Kontoauszüge, Rechnungsabschlüsse, Angebote zur Änderung der Allgemeinen Geschäftsbedingungen und Sonderbedingungen. Die Bank behält sich das Recht vor, Dokumente nicht nur durch Bereitstellung im elektronischen Postfach, sondern auch auf dem Postweg zu versenden, wenn dies im Interesse des Kunden sinnvoll erscheint oder aus rechtlichen Gründen erforderlich ist. Kontoauszüge der letzten 36 Monate sind im Net- und Mobile-Banking abrufbar, sofern Transaktionen erfolgt sind.

6. Datenaktualisierung
Der oder die Kontoinhaber:in ist dazu befugt, die E-Mail-Adresse, Mobilfunknummer, Festnetznummer, Anschrift sowie die Ausweisdaten eigenständig im Net- und Mobile-Banking zu ändern. Die Änderung der Mobilfunknummer erfolgt mittels einer TAN, welche dem oder der Kontoinhaber:in per SMS übermittelt wird. Für die Aktualisierung der Ausweisdaten ist eine Verifizierung durch das Hochladen eines Bildes oder einer PDF-Datei des Ausweisdokuments erforderlich.

7. Sorgfalts- und Mitwirkungspflichten
7.1 Schutz der Zugangsdaten
Der oder die Kontoinhaber:in hat alle zumutbaren Vorkehrungen zu treffen, um seine oder ihre Zugangsdaten vor unbefugtem Zugriff zu schützen. Andernfalls besteht die Gefahr eines Missbrauchs des Net- oder Mobile-Bankings. Zum Schutz der Zugangsdaten hat der oder die Kontoinhaber:in die Wissenselemente, wie beispielsweise die PIN oder das Passwort geheim zu halten. Sie dürfen insbesondere:

- nicht mündlich (z. B. telefonisch oder persönlich) mitgeteilt werden,
- nicht außerhalb des Net-Banking in Textform (z. B. per E-Mail, Messenger-Dienst) weitergegeben werden,
- nicht ungesichert elektronisch gespeichert (z. B. Speicherung der PIN im Klartext im Computer oder im mobilen Endgerät) werden und
- nicht auf einem Gerät notiert oder als Abschrift zusammen mit einem Gerät aufbewahrt werden, das als Besitzelement dient.

7.2 Schutz des Nutzersystems
Da Angriffe auf die Sicherheit der elektronischen Kontoführung möglich sind, obliegt es dem oder der Kontoinhaber:in im eigenen Interesse geeignete Schutzmaßnahmen zu ergreifen. Dazu gehört insbesondere:

- den Computer und das Mobilgerät frei von sicherheitsgefährdenden Programmen wie Computerviren und Trojanern zu halten.
- handelsübliche Virenschutzprogramme zu nutzen, die jedoch nur dann effektiv sind, wenn ihre regelmäßigen Updates genutzt werden.
- sicherzustellen, dass der verwendete Browser keine Sicherheitsmängel aufweist.
- sich regelmäßig über sicherheitsrelevante Aspekte des verwendeten Systems (Betriebssystem, Browser etc.) zu informieren. Informationen zur Systemsicherheit können beispielsweise vom Systemhersteller bezogen werden.
- regelmäßige Informationen über Sicherheitsbelange einzuholen, um Gefährdungen des Systems zu verhindern, einschließlich der Prävention böswilliger Manipulationen durch Fremdprogramme.
- Maßnahmen zu ergreifen, die die Systemsicherheit erhöhen, wie die Installation sicherheitsrelevanter Programmaktualisierungen.

Regelmäßige Updates und Informationen sind erforderlich, um die Sicherheit des Systems zu gewährleisten.

7.3 Sorgfaltspflicht bei der Transaktion
Beim Aufruf des Begrüßungsbildschirms sollte der oder die Kontoinhaber:in zunächst die Adresse der Webseite im Browser überprüfen, um sicherzustellen, dass tatsächlich eine Verbindung zur Bank besteht. Andernfalls besteht die Gefahr, dass Dritte Zugang zu den Zugangsdaten erlangen. Anschließend sind alle eingegebenen Daten auf Vollständigkeit und Richtigkeit zu überprüfen, insbesondere die IBAN des Empfängers.

8. Sperranzeige
Stellt der oder die Kontoinhaber:in Folgendes fest:

- den Verlust oder Diebstahl eines Besitzelements zur Authentifizierung (z. B. mobiles Endgerät) oder
- die missbräuchliche Verwendung oder sonstige nicht autorisierte Nutzung der Zugangsdaten

muss er oder sie die Bank unverzüglich darüber informieren (Sperranzeige). Zudem ist jeder Diebstahl oder Missbrauch der Zugangsdaten umgehend der Polizei zu melden. Bei Verdacht auf eine nicht autorisierte oder betrügerische Verwendung der Zugangsdaten ist ebenfalls eine Sperranzeige erforderlich.

9. Zugangssperrung
Die Bank sperrt auf Veranlassung des oder der Kontoinhaber:in den Net- und Mobile-Banking-Zugang. Bei dreimaliger Falscheingabe des Passwortes oder bei Verdacht auf missbräuchliche Kontonutzung über das Net- oder Mobile-Banking wird der Zugang zum Konto gesperrt. Die Aufhebung der Sperre erfolgt, sobald die Gründe für die Sperrung entfallen sind oder auf schriftlichen Antrag des oder der Kontoinhaber:in.

10. Haftung
Die Bank haftet für die Erfüllung ihrer Verpflichtungen aus diesem Vertrag. Trägt der oder die Kontoinhaber:in durch eigenes Verschulden, insbesondere durch Verletzung seiner oder ihrer Sorgfaltspflichten, zur Entstehung eines Schadens bei, wird die Haftung von Bank und Kontoinhaber:in nach den Grundsätzen des Mitverschuldens anteilig festgelegt.
Haftung ab Sperranzeige
Nach Eingang einer Sperranzeige übernimmt die Bank die Haftung für alle daraus folgenden Schäden, die durch unautorisierte Netbanking-Verfügungen entstehen. Eine Haftung entfällt jedoch, wenn der oder die Kontoinhaber:in in betrügerischer Absicht gehandelt hat.
Haftung für minderjährige Kontoinhaber:innen
Haften minderjährige Kontoinhaber:innen gemäß den beschriebenen Bestimmungen, so treten die gesetzlichen Vertreter gesamtschuldnerisch für die daraus entstehende Haftung ein.
Haftungsausschluss
Haftungsansprüche sind ausgeschlossen, wenn der Schaden auf einem ungewöhnlichen und unvorhersehbaren Ereignis beruht, das außerhalb der Kontrolle der haftenden Partei liegt und dessen Folgen trotz angemessener Sorgfalt nicht hätten vermieden werden können.

11. Datenschutz
Für die Nutzung von Net- und Mobile-Banking gelten die allgemeinen Datenschutzhinweise der Bank.

12. Verhältnis zu anderen Bedingungen der Bank
Die Nutzungsbedingungen für Net- und Mobile-Banking sind in Verbindung mit den Allgemeinen Geschäftsbedingungen sowie den Sonderbedingungen für die einzelnen Anlageprodukte der Bank zu betrachten.

13. Beendigung der Nutzung des Net- und Mobile-Banking
Die Nutzung des Net- und Mobile-Banking kann von dem oder der Kontoinhaber:in beendet werden. Dies hat jedoch keinen Einfluss auf die Vertragsbeziehung zwischen dem oder der Kontoinhaber:in und der Bank. Das Löschen der DHB Bank App führt nicht zur Beendigung der Nutzung des Net- und Mobile-Banking.

Stand: 1. Dezember 2024