Bedingungen für die Abwicklung von Bankgeschäften über das Berenberg Corporate Portal

1 Leistungsangebot

(1) Der Kunde kann mittels des Berenberg Corporate Portal Bankgeschäfte in dem von der Bank angebotenen Umfang abwickeln. Für die Abwicklung gelten die Bedingungen für die jeweiligen Bankgeschäfte (z. B. Sonderbedingungen für den Überweisungsverkehr). Zudem kann er Informationen der Bank über das Berenberg Corporate Portal abrufen.

(2) Soweit bei anderen Kreditinstituten geführte Konten in das Berenberg Corporate Portal einbezogen werden sollen, wird der Kunde diese Kreditinstitute zur Übermittlung von Kontoinformationen an die Bank beauftragen und zur Entgegennahme von Auftragsdatensätzen berechtigen, die diesen von der Bank übermittelt worden sind. Die Bank wird hierbei als Bote tätig. Der Kunde wird der Bank die hierzu jeweils erforderlichen Angaben rechtzeitig mitteilen.

(3) Kunde und Bevollmächtigte werden im Folgenden einheitlich als »Teilnehmer« bezeichnet. Konto und Depot werden im Folgenden einheitlich als »Konto« bezeichnet.

(4) Zur Nutzung des Berenberg Corporate Portal gelten die mit der Bank gesondert vereinbarten Verfügungslimite für die vereinbarte Serviceart.

2 Voraussetzungen zur Nutzung des Berenberg Corporate Portal

Um sich gegenüber der Bank als berechtigter Teilnehmer auszuweisen (siehe Nummer 3) und Aufträge zu autorisieren (siehe Nummer 4) authentifiziert die Bank den Teilnehmer mit den hierfür vereinbarten Authentifizierungselementen und prüft hierdurch die Identität des Teilnehmers.

2.1 Authentifizierungselemente

Authentifizierungselemente sind

- Wissenselemente, also etwas, das nur der Teilnehmer weiß (z.B. persönliche Identifikationsnummer [„PIN"]),
- Besitzelemente, also etwas, das nur der Teilnehmer besitzt (z.B. Gerät zur Erzeugung oder zum Empfang von einmal verwendbaren Transaktionsnummern [TAN], die den Besitz des Teilnehmers nachweisen, wie mobile Endgeräte) oder,
- Seinselemente, also etwas, das der Teilnehmer ist (Inhärenz, z.B. Fingerabdruck als biometrisches Merkmal des Teilnehmers).

Die Authentifizierung des Teilnehmers erfolgt, indem der Teilnehmer gemäß der Anforderung der Bank das Wissenselement, den Nachweis des Besitzelements und/oder den Nachweis des Seinselements an die Bank übermittelt.

3 Zugang zum Berenberg Corporate Portal

Der Teilnehmer erhält Zugang zum Berenberg Corporate Portal, wenn

- dieser die Teilnehmernummer auf der dafür vorgesehenen Eingabemaske angibt und sich mittels Verwendung des oder der von der Bank angeforderten Authentifizierungselemente(s) ausweist,
- die Prüfung dieser Daten bei der Bank eine Zugangsberechtigung des Teilnehmers ergeben hat und
- keine Sperre des Zugangs (siehe Nummern 9.1 und 10) vorliegt.

Nach Gewährung des Zugangs zum Berenberg Corporate Portal kann der Teilnehmer Informationen abrufen oder Aufträge erteilen.

4 Auftragsabwicklung im Rahmen des Berenberg Corporate Portal

4.1 Auftragserteilung und Autorisierung

Die Autorisierung zur Durchführung einzelner Geschäfte (z. B. Überweisung) erfolgt – abhängig von der gewählten Serviceart – mittels Eingabe der von der Bank angeforderten Authentifizierungselemente.

4.2 Meldung nach AWV

Bei Zahlungen zugunsten Gebietsfremder ist vom Teilnehmer die Meldung gemäß Außenwirtschaftsverordnung (AWV) zu beachten.

4.3 Widerruf von Aufträgen

Die Widerrufbarkeit eines Auftrags richtet sich nach den für die jeweilige Auftragsart geltenden Sonderbedingungen. Der Widerruf von Aufträgen kann nur außerhalb des Berenberg Corporate Portal erfolgen, es sei denn, die Bank sieht eine Widerrufsmöglichkeit im Berenberg Corporate Portal ausdrücklich vor.

5 Bearbeitung von Aufträgen durch die Bank

(1) Die Bearbeitung der im Rahmen des Berenberg Corporate Portal erteilten Aufträge erfolgt nach den für die Abwicklung der jeweiligen Auftragsart geltenden Regelungen der vereinbarten Serviceart.

(2) Für Aufträge, insbesondere Zahlungsaufträge (Überweisung, Lastschrift) gelten folgende Sonderregelungen:

Die Bank wird den Auftrag ausführen, wenn folgende Ausführungsbedingungen vorliegen:

- Der Teilnehmer hat den Auftrag autorisiert (vgl. Nummer 4.1).
- Die Berechtigung des Teilnehmers für die jeweilige Auftragsart liegt vor.
- Das für die vereinbarte Serviceart erforderliche Datenformat ist eingehalten.
- Das für die Serviceart gesondert vereinbarte Verfügungslimit oder das Standardlimit ist nicht überschritten.
- Die Ausführungsvoraussetzungen nach den für die jeweilige Auftragsart maßgeblichen Sonderbedingungen liegen vor.
- Es ist eine ausreichende Kontodeckung (Guthaben oder eingeräumter Kredit) vorhanden.

Liegen die vorgenannten Ausführungsbedingungen vor, führt die Bank den Auftrag aus. Die Ausführung darf nicht gegen sonstige Rechtsvorschriften verstoßen.

BeGo 2024-08
Form SB-41 DE

(3) Liegen die Ausführungsbedingungen nach Absatz (2) Satz 1 Spiegelstrich 1–6 nicht vor, wird die Bank den Auftrag nicht ausführen. Die Bank wird den Teilnehmer über die Nichtausführung und soweit möglich, über deren Gründe und die Möglichkeiten, mit denen Fehler, die zur Ablehnung geführt haben, berichtigt werden können, online oder auf anderem Weg eine Information zur Verfügung stellen. Dies gilt nicht, wenn die Angabe von Gründen gegen sonstige Rechtsvorschriften verstößt. Führt die Bank den Auftrag aus, obwohl keine Kontodeckung vorhanden ist, entsteht eine geduldete Kontoüberziehung, für die ein erhöhter Zins zu zahlen ist.

6 Information des Kunden über im Rahmen des Berenberg Corporate Portal erteilte Verfügungen

Die Bank unterrichtet den Kunden über die im Rahmen des Berenberg Corporate Portal getätigten Verfügungen auf dem für Kontoinformationen vereinbarten Weg und gemäß den für den Auftrag geltenden Bedingungen.

7 Sorgfaltspflichten des Teilnehmers

7.1 Technische Verbindung zum Berenberg Corporate Portal

Der Teilnehmer ist verpflichtet, die technische Verbindung zum Berenberg Corporate Portal nur über die von der Bank gesondert mitgeteilten Zugangskanäle (z. B. Internetadresse) herzustellen. Der Kunde ist dafür verantwortlich, dass er für seine eigenen Systeme eine angemessene Datensicherung unterhält und stets nach dem Stand der Technik ausreichende Vorkehrungen gegen Viren und andere schädliche Programme (z. B. Trojaner, Würmer etc.) trifft. Der Kunde hat eigenverantwortlich die landesspezifischen Regelungen für die Nutzung des Internets zu beachten.

7.2 Schutz der Authentifizierungselemente

Der Teilnehmer hat alle zumutbaren Vorkehrungen zu treffen, um seine Authentifizierungselemente (siehe Nummer 2.1) vor unbefugtem Zugriff zu schützen. Ansonsten besteht die Gefahr, dass das Verfahren missbräuchlich verwendet oder in sonstiger Weise nicht autorisiert genutzt wird (vergleiche Nummer 3 und 4 dieser Bedingungen).

(1) Zum Schutz der einzelnen Authentifizierungselemente hat der Teilnehmer vor allem Folgendes zu beachten:

(a) Wissenselemente, wie z.B. die PIN, sind geheim zu halten; sie dürfe insbesondere

- nicht mündlich (z.B. telefonisch oder persönlich) mitgeteilt werden,
- nicht außerhalb des Verfahrens 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 (z.B. mobiles Endgerät, Signaturkarte) oder zur Prüfung des Seinselements (z.B. mobiles Endgerät mit Anwendung für das Online Banking und Fingerabdrucksensor) dient.

(b) Besitzelemente, wie z.B. ein mobiles Endgerät, sind vor Missbrauch zu schützen, insbesondere

- sind die Signaturkarte vor dem unbefugten Zugriff anderer Personen sicher zu verwahren,
- ist sicherzustellen, dass unberechtigte Personen auf das mobile Endgerät des Teilnehmers (z.B. Mobiltelefon) nicht zugreifen können,
- ist dafür Sorge zu tragen, dass andere Personen die auf dem mobilen Endgerät (z.B. Mobiltelefon) befindliche Anwendung für das Berenberg Corporate Portal (z.B. Anwendungs-App, Authentifizierungs-App) nicht nutzen können,
- ist die Anwendung für das Berenberg Corporate Portal (z.B. Anwendungs-App, Authentifizierungs-App) auf dem mobilen Endgerät des Teilnehmers zu deaktivieren, bevor der Teilnehmer den Besitz an diesem mobilen Endgerät aufgibt (z.B. durch Verkauf oder Entsorgung des Mobiltelefons),
- dürfen die Nachweise des Besitzelements (z.B. TAN) nicht außerhalb des Verfahrens mündlich (z.B. per Telefon) oder in Textform (z.B. per E-Mail, Messenger-Dienst) weitergegeben werden und
- muss der Teilnehmer, der von der Bank einen Code zur Aktivierung des Besitzelements (z.B. Mobiltelefon mit Anwendung für das Berenberg Corporate Portal) erhalten hat, diesen vor dem unbefugten Zugriff anderer Personen sicher verwahren; ansonsten besteht die Gefahr, dass andere Personen ihr Gerät als Besitzelement für das Berenberg Corporate Portal des Teilnehmers aktivieren.

(c) Seinselemente, wie z.B. Fingerabdruck des Teilnehmers, dürfen auf einem mobilen Endgerät des Teilnehmers für das Berenberg Corporate Portal nur dann als Authentifizierungselement verwendet werden, wenn auf dem mobilen Endgerät keine Seinselemente anderer Personen gespeichert sind. Sind auf dem mobilen Endgerät, das für das Berenberg Corporate Portal genutzt wird, Seinselemente anderer Personen gespeichert, ist für das Berenberg Corporate Portal das von der Bank ausgegebene Wissenselement (z.B. PIN) zu nutzen und nicht das auf dem mobilen Endgerät gespeicherte Seinselement.

(d) Des Weiteren ist zu beachten:

- Das Kennwort für die elektronische Signatur darf nicht zusammen mit dem Authentifizierungselement verwahrt werden.
- Der vom Teilnehmer erzeugte elektronische Schlüssel darf bei einem Teilnehmer nicht ungesichert elektronisch gespeichert werden (z. B. im Kundensystem oder auf einem mobilen Endgerät). Der vom Teilnehmer erzeugte persönliche elektronische Schlüssel darf sich nur in der alleinigen Verfügungsgewalt des Teilnehmers oder in einer von der Bank (oder von einem von der Bank

zugelassenen Dienstleister) zur Verfügung gestellten technischen Umgebung, die vor unautorisiertem Zugriff geschützt ist, befinden.

- Wird im Rahmen einer vollautomatisierten Übertragung ein sog. Technischer Teilnehmer eingesetzt, ist die elektronisch gespeicherte Signatur in einer sicheren und entsprechend geeigneten technischen Umgebung zu speichern. Der »Technische Teilnehmer« ist nicht berechtigt, die Auftragserteilung selbst vorzunehmen. Er übermittelt lediglich die Auftragsdaten.
- Bei Eingabe eines Authentifizierungselements ist sicherzustellen, dass andere Personen diese nicht ausspähen können.
- Authentifizierungselemente dürfen nicht außerhalb des Berenberg Corporate Portal weitergegeben werden, also beispielsweise nicht per E-Mail.
- Im Falle der Speicherung des elektronischen Schlüssels auf einem mobilen Endgerät (z.B. Smartphone) des Teilnehmers ist sicherzustellen, dass unberechtigte Personen auf dieses Endgerät nicht zugreifen und es nicht nutzen können.
- Es ist dafür Sorge zu tragen, dass andere Personen die auf dem mobilen Endgerät befindliche Authentifizierungselemente nicht nutzen können.

(2) Die App der Bank zur Teilnahme am Berenberg Corporate Portal oder zur Autorisierung von Aufträgen ist direkt von der Bank oder von einem dem Kunden von der Bank benannten Anbieter zu beziehen.

7.3 Kontrolle der Auftragsdaten mit von der Bank angezeigten Daten

Soweit die Bank dem Teilnehmer Daten aus seinem über das Berenberg Corporate Portal erteilten Auftrag (z. B. Betrag, Kontonummer des Zahlungsempfängers) im Kundensystem zur Bestätigung anzeigt, ist der Teilnehmer verpflichtet, vor der Bestätigung die Übereinstimmung der angezeigten Daten mit den für die Transaktion vorgesehenen Daten zu prüfen.

7.4 Weitere Sorgfaltspflichten des Kunden

Der Kunde trägt dafür Sorge, dass die Sorgfaltspflichten aus diesem Vertrag auch von dem Bevollmächtigten (also von allen Teilnehmern) eingehalten werden.

8 Verschlüsselungstechnik im Ausland

In den Ländern, in denen Nutzungs-, Einfuhr-, und/oder Ausfuhrbeschränkungen für Verschlüsselungstechniken bestehen, darf der von der Bank zur Verfügung gestellte Online-Zugang nicht genutzt werden. Gegebenenfalls hat der Teilnehmer die erforderlichen Genehmigungen, Anzeigen oder sonst erforderlichen Maßnahmen zu veranlassen. Der Teilnehmer hat die Bank über ihm bekannt gewordene Verbote, Genehmigungs- und Anzeigepflichten zu informieren.

9 Anzeige- und Unterrichtungspflichten

9.1 Sperranzeige

(1) Stellt der Teilnehmer

- den Verlust oder den Diebstahl eines Besitzelements zur Authentifizierung (z.B. eines Mobilen Endgeräts),
- die missbräuchliche Verwendung oder
- die sonstige nicht autorisierte Nutzung seines Authentifizierungselements,

muss der Teilnehmer die Bank hierüber unverzüglich unterrichten (Sperranzeige). Der Teilnehmer kann der Bank eine Sperranzeige jederzeit auch telefonisch unter +49 40 350 60-0 abgeben.

(2) Der Teilnehmer hat jeden Diebstahl oder Missbrauch unverzüglich bei der Polizei zur Anzeige zu bringen.

(3) Hat der Teilnehmer den Verdacht einer nicht autorisierten oder betrügerischen Verwendung eines seiner Authentifizierungselemente, muss er unverzüglich ebenfalls eine Sperranzeige abgeben.

9.2 Unterrichtung über nicht autorisierte oder fehlerhaft ausgeführte Aufträge

Der Kunde hat die Bank unverzüglich nach Feststellung eines nicht autorisierten oder fehlerhaft ausgeführten Auftrags hierüber zu unterrichten.

10 Nutzungssperre

10.1 Sperre auf Veranlassung des Teilnehmers

Die Bank sperrt auf Veranlassung des Teilnehmers, insbesondere im Fall der Sperranzeige nach Nummer 9.1,

- den Zugang zum Berenberg Corporate Portal für ihn und, falls der Teilnehmer dies verlangt, den Zugang für alle Teilnehmer des Kunden, oder
- sein Authentifizierungselement.

10.2 Sperre auf Veranlassung der Bank

(1) Die Bank darf den Zugang zum Berenberg Corporate Portal für einen Teilnehmer sperren, wenn

- sie berechtigt ist, den Vertrag über die Zusammenarbeit im Bereich Auslands- und Transaktionsgeschäft aus wichtigem Grund zu kündigen,
- sachliche Gründe im Zusammenhang mit der Sicherheit eines Authentifizierungselements dies rechtfertigen oder
- der Verdacht einer nicht autorisierten oder einer betrügerischen Verwendung eines Authentifizierungselements besteht.

(2) Die Bank wird den Kunden unter Angabe der hierfür maßgeblichen Gründe möglichst vor, spätestens jedoch unverzüglich nach der Sperre unterrichten.

10.3 Aufhebung der Sperre

Die Bank wird eine Sperre aufheben oder die betroffenen Authentifizierungselemente austauschen, wenn die Gründe für die Sperre nicht mehr gegeben sind. Hierüber unterrichtet sie den Kunden unverzüglich.

10.4 Automatische Sperre

Das Wissenselement (z.B. PIN) wird gesperrt, wenn es dreimal in Folge falsch eingegeben wurde. Der Teilnehmer kann sich mit der Bank in Verbindung setzen, um die Nutzungsmöglichkeiten des Berenberg Corporate Portal wiederherzustellen.

11 Haftung beim Einsatz von Authentifizierungselementen

11.1 Haftung des Kunden für nicht autorisierte Zahlungsvorgänge vor der Sperranzeige

(1) Beruhen nicht autorisierte Zahlungsvorgänge vor der Sperranzeige auf der Nutzung eines verlorengegangenen, gestohlenen oder sonst abhanden gekommenen Authentifizierungselements oder auf der sonstigen missbräuchlichen Nutzung eines Authentifizierungselements, haftet der Kunde für den der Bank hierdurch entstehenden Schaden, wenn den Teilnehmer an dem Verlust, Diebstahl, sonstigem Abhandenkommen oder der sonstigen missbräuchlichen Nutzung des Authentifizierungselements ein Verschulden trifft. Der Kunde haftet auch, wenn er einen von ihm benannten Teilnehmer nicht sorgfältig ausgesucht und/oder die Beachtung der Verpflichtungen des Teilnehmers nach diesen Bedingungen nicht regelmäßig überprüft hat. Hat die Bank durch ein schuldhaftes Verhalten zu der Entstehung eines Schadens beigetragen, bestimmt sich nach den Grundsätzen des Mitverschuldens, in welchem Umfang Kunde und Bank den Schaden zu tragen haben. Die Haftungsbegrenzung gemäß § 675v Abs. 1 des Bürgerlichen Gesetzbuches findet keine Anwendung.

(2) Der Kunde ist nicht zum Ersatz des Schadens nach Absatz 1 und 2 verpflichtet, wenn der Teilnehmer die Sperranzeige nach Nummer 9.1 nicht abgeben konnte, weil die Bank nicht die Möglichkeit zur Entgegennahme der Sperranzeige sichergestellt hatte und der Schaden dadurch eingetreten ist.

(3) Die Haftung für Schäden, die innerhalb des Zeitraums, für den das Standardlimit oder das mit dem Kunden für das Berenberg Corporate Portal vereinbarte Verfügungslimit gilt, verursacht werden, beschränkt sich jeweils diese Limite.

11.2 Haftung bei nicht autorisierten anderen Servicearten vor der Sperranzeige

Beruhen nicht autorisierte Transaktionen bei den vereinbarten Servicearten vor der Sperranzeige auf der Nutzung eines verlorengegangenen, gestohlenen oder sonst abhanden gekommenen Authentifizierungselements oder auf der sonstigen missbräuchlichen Nutzung des Authentifizierungselements und ist der Bank hierdurch ein Schaden entstanden, haftet der Kunde für den der Bank hierdurch entstandenen Schaden, wenn dem Teilnehmer an dem Verlust, Diebstahl, sonstigen Abhandenkommen oder der sonstigen missbräuchlichen Nutzung des Authentifizierungselements ein Verschulden trifft. Die Haftungsbegrenzung gemäß § 675v Abs. 1 des Bürgerlichen Gesetzbuches findet keine Anwendung. Der Kunde haftet auch, wenn er einen von ihm benannten Teilnehmer nicht sorgfältig ausgesucht und/oder die Beachtung der Verpflichtungen des Teilnehmers nach diesen Bedingungen nicht regelmäßig überprüft hat. Hat die Bank durch ein schuldhaftes Verhalten zu der Entstehung eines Schadens beigetragen, bestimmt sich nach den Grundsätzen des Mitverschuldens, in welchem Umfang Kunde und Bank den Schaden zu tragen haben.

11.3 Haftung der Bank ab der Sperranzeige

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

12 Verfügbarkeit

Die Bank strebt an, die im Berenberg Corporate Portal angebotenen Services möglichst umfassend verfügbar zu halten. Eine garantierte Verfügbarkeit ist damit nicht verbunden. Insbesondere aufgrund technischer Probleme, Wartungsarbeiten und aufgrund von Netzproblemen (z. B. Nichtverfügbarkeit von Servern Dritter), auf welche die Bank keinen Einfluss hat, kann es zu zeitweiligen Störungen kommen, die den Zugriff verhindern.

13 Verweis auf Internetseiten Dritter

Falls im Rahmen des Internetauftritts der Zugriff auf die Seiten Dritter ermöglicht wird, geschieht dies nur, um dem Teilnehmer einen leichteren Zugriff auf das Informationsangebot im Internet zu ermöglichen. Die Inhalte der Seiten dieser Anbieter stellen nicht eigene Aussagen der Bank dar. Sie werden von der Bank auch nicht überprüft.

14 Nutzungsrechte

Dem Kunden wird durch diesen Vertrag nicht gestattet, Links oder Framelinks auf seinen Webseiten ohne vorherige schriftliche Zustimmung der Bank zu setzen. Der Kunde verpflichtet sich, die Webseiten und deren Inhalt nur für eigene Zwecke zu verwenden. Insbesondere ist der Kunde nicht berechtigt, ohne Zustimmung der Bank die Inhalte Dritten zur Verfügung zu stellen, in andere Produkte oder Verfahren einzubetten oder den Quellcode der einzelnen Webseiten zu entschlüsseln. Hinweise auf Rechte der Bank oder Dritter dürfen nicht entfernt oder unkenntlich gemacht werden. Der Kunde wird Marken, Domainnamen und

andere Kennzeichen der Bank oder Dritter nicht ohne vorherige Zustimmung der Bank verwenden. Der Kunde erhält nach diesen Bedingungen keine unwiderruflichen, ausschließlichen und übertragbaren Nutzungsrechte.

15 Hotline (»Helpdesk«)

Die Bank bietet eine telefonische Hotline (sog. Helpdesk) für die Bearbeitung von Fragen zur Technik, Bedienung und zu Funktionalitäten der im Berenberg Corporate Portal angebotenen Services an. Die Hotline ist zu erreichen unter der Telefonnummer +49 40 350 60-788. Die Bank besetzt die Hotline während der für das deutsche Bankgewerbe geltenden Bankarbeitstage.