HypoVereinsbank Member of UniCredit

BEDINGUNGEN ZUR ONLINEVEREINBARUNG FÜR FIRMENKUNDEN[1]

Stand: 11. März 2022

I. Datenfernübertragung

1. Leistungsangebot
Die Bank steht ihrem Kunden für die Datenfernübertragung auf elektronischem Wege (DFÜ) zur Verfügung. Insoweit gelten die »Bedingungen für Datenfernübertragung«, soweit diese »Bedingungen zur Onlinevereinbarung für Firmenkunden« keine abweichenden Regelungen treffen.

2. Definitionen
Sofern sich aus diesen »Bedingungen zur Onlinevereinbarung für Firmenkunden« nichts Gegenteiliges ergibt, haben die darin verwendeten Begriffe dieselbe Bedeutung wie die definierten Begriffe in den »Bedingungen für Datenfernübertragung«.

Abweichend von den »Bedingungen für Datenfernübertragung« werden Kunde und Kontobevollmächtigte im Folgenden einheitlich nicht als »Nutzer«, sondern als »User« bezeichnet. »User« und »technischer Teilnehmer« werden im Folgenden unter dem Begriff »Teilnehmer« zusammengefasst.

3. Elektronische Zugangswege
Zur Nutzung der von der Bank angebotenen Zugangswege wird jeweils ein separater Vertrag geschlossen.

Die Bank ist berechtigt, die gesamten elektronischen Zugangswege eines Kunden und damit auch eines jeden von ihm benannten Teilnehmers zu löschen, wenn sich nicht innerhalb von 6 Monaten nach Erhalt des ersten Bestätigungsschreibens durch den Kunden mindestens ein Teilnehmer gemäß den »Bedingungen für Datenfernübertragung« mittels Initialisierungsprotokolls initialisiert hat. Die Bank wird den Kunden hierüber informieren.

4. Vertretungsberechtigung

4.1 User und Technische Teilnehmer [2]
Kunde und Bank legen die User und den Technischen Teilnehmer sowie deren Vertretungsberechtigung betreffend bestimmte Konten gesondert fest. Der Kunde wird den von ihm bevollmächtigten Personen den jeweiligen Umfang ihrer Vertretungsberechtigung mitteilen.

4.2 Umfang der Vertretungsberechtigung für künftige Bankprodukte
Die Vertretungsberechtigung der Teilnehmer gilt, sofern der Kunde der Bank nichts Abweichendes mitteilt, für den jeweiligen elektronischen Zugangsweg soweit die Teilnehmer für diesen angemeldet sind, in jeweils gleichem Umfang auch für alle künftigen Bankprodukte/-services. Die Mitteilung gem. Satz 1 sollte aus Beweisgründen schriftlich erfolgen.

4.3 Änderung/Erlöschen der Vertretungsberechtigung
Der Kunde hat das Erlöschen einer der Bank bekannt gegebenen Vertretungsberechtigung eines Teilnehmers unverzüglich und aus Beweisgründen möglichst in Schriftform der Bank mitzuteilen. Diese Mitteilungspflicht besteht auch dann, wenn die Vertretungsberechtigung in ein öffentliches Register (z. B. in das Handelsregister) eingetragen ist und ihr Erlöschen oder ihre Änderung in dieses Register eingetragen wird.

4.4 Automatisches Erlöschen der Vertretungsberechtigung
Die Bank ist berechtigt, sämtliche elektronischen Zugangswege eines seitens des Kunden angemeldeten Teilnehmers zu löschen, wenn sich der Teilnehmer nicht innerhalb von 12 Monaten nach Erhalt des Bestätigungsschreiben durch den Kunden, in dem der Teilnehmer erstmals als Vertretungsberechtigter aufgeführt ist, gemäß den vereinbarten »Bedingungen für Datenfernübertragung« mittels Initialisierungsprotokolls initialisiert hat. Die Bank wird den Kunden über die Löschung des Teilnehmers mittels Bestätigungsschreiben informieren.

4.5 Nicht ausreichende Vertretungsberechtigung bei übersandten Dateien (Verteilte elektronische Unterschrift)
Ist bei elektronisch übersandten Dateien die Vertretungsberechtigung nicht ausreichend (z. B. fehlende elektronische Unterschrift; fehlende Zweitunterschrift) wird die Datei – falls gemäß den »Bedingungen für Datenfernübertragungen (DFÜ-Bedingungen) die Möglichkeit zur verteilten elektronischen Unterschrift besteht – zur verteilten elektronischen Unterschrift weitergeleitet d. h. die Datei wird bei der Bank zunächst zwischengespeichert. Dies wird im Protokoll der Datenfernübertragung (DFÜ-Protokoll) vermerkt. Nach Ablauf der in den DFÜ-Bedingungen vereinbarten Zeit wird die Datei gelöscht.

Besteht die Möglichkeit zur verteilten elektronischen Unterschrift nicht, wird die Datei nicht ausgeführt. Auch dies wird im DFÜ-Protokoll vermerkt.

5. Urheberschutz
Die über die elektronischen Zugangswege zur Verfügung gestellten Inhalte, insbesondere die darin enthaltenen Informationen, Daten, Texte, Bildmaterialien sowie Funktionen unterliegen dem Urheberschutz. Der Teilnehmer erwirbt durch deren Nutzung daran keinerlei eigene Rechte. Er darf jedoch nach Maßgabe der jeweiligen Funktion hierfür bestimmte Inhalte für seine geschäftlichen Zwecke kopieren oder anderweitig nutzen, soweit er auf die Urheberrechte der Bank verweist. Der Teilnehmer wird die elektronischen Zugangswege und ihre Inhalte nur für eigene geschäftliche Zwecke verwenden und Dritten nicht zur Verfügung stellen, alle Inhalte vertraulich behandeln, Hinweise auf das Urheberrecht der Bank oder ihrer Zulieferer nicht entfernen oder unkenntlich machen sowie Marken, Domainnamen und andere Kennzeichen der Bank oder Dritter nicht ohne deren Einwilligung verwenden.

6. Länderspezifische Beschränkungen
Die Nutzung bestimmter Inhalte über die elektronischen Zugangswege ist in einigen Ländern nicht bzw. nur in eingeschränktem Umfang oder unter zusätzlichen Voraussetzungen erlaubt, so dass teilweise diese Inhalte in bestimmten Ländern nicht aufgerufen werden dürfen. Der Kunde wird sich deshalb vor Nutzung der Zugangswege selbst erkundigen, welche länderspezifischen Beschränkungen bestehen und der Sorge tragen, dass diese von den Usern eingehalten werden.

7. Devisenrechtliche Bestimmungen
Bei länderübergreifenden Zahlungsaufträgen wird sich der Kunde über die jeweils geltenden devisenrechtlichen Bestimmungen der betroffenen Länder selbst informieren.

8. Schlussbestimmungen
Für die »Onlinevereinbarung für Firmenkunden« gilt deutsches Recht.

Für alle außervertraglichen Ansprüche, die aus oder im Zusammenhang mit der »Onlinevereinbarung für Firmenkunden« entstehen könnten, gilt ebenfalls deutsches Recht.

Gerichtsstand für die »Onlinevereinbarung für Firmenkunden« und für alle außervertraglichen Ansprüche, die daraus oder im Zusammenhang damit entstehen könnten, ist München, Deutschland.

Hinweise:
[1] Bedingungen für Kunden, die keine Verbraucher sind
[2] Gegenwärtig oder künftig erteilte Kontovollmachten bleiben neben der Vertretungsberechtigung für elektronische Zugangswege bestehen.

Ab dem 14.09.2019 erfolgt der Zugang zu UC eBanking Global ausschließlich über das Corporate Portal unter https://corporateportal.unicreditgroup.eu/portal/germany

II. CORPORATE PORTAL

1. Leistungsangebot

1.1 Der Kunde und dessen Bevollmächtigte können über das Corporate Portal webbasiert auf ausgewählte Bankprodukte sowie die integrierte persönliche Communication Suite (nachfolgend als »Postfach" bezeichnet) zugreifen und Bankgeschäfte in dem von der Bank angebotenen Umfang abwickeln, z. B. bei bestimmten Bankprodukten Aufträge unmittelbar online über das Corporate Portal erteilen.

1.2 Kunde und Bevollmächtigte werden einheitlich als »User« bezeichnet.

1.3 Die Bank wählt die Bankprodukte und Services, auf die mittels Corporate Portal zugegriffen werden kann, im eigenen Ermessen aus.

2. Voraussetzungen zur Nutzung des Corporate Portals

2.1 Der User kann das Corporate Portal nutzen, wenn die Bank ihn authentifiziert hat.

2.2 Authentifizierung ist das mit der Bank gesondert vereinbarte Verfahren, mit dessen Hilfe die Bank die Identität des Users oder die berechtigte Verwendung eines vereinbarten Zahlungsinstruments, einschließlich der Verwendung des personalisierten Sicherheitsmerkmals des Users überprüfen kann. Mit den hierfür vereinbarten Authentifizierungselementen kann der User sich gegenüber der Bank als berechtigter User ausweisen, auf Informationen zugreifen (siehe Ziffer 3 dieser Bedingungen) sowie Aufträge erteilen (siehe Ziffer 4 dieser Bedingungen).

2.3 Authentifizierungselemente sind:
- Wissenselemente, also etwas, das nur der User weiß (z. B. persönliche Identifikationsnummer (PIN),
- Besitzelemente, also etwas, das nur der User besitzt (z. B. Gerät zur Erzeugung oder zum Empfang von einmal verwendbaren Transaktionsnummern (TAN), die den Besitz des Users nachweisen, wie das mobile Endgerät), oder
- Seinselemente, also etwas, das der User ist (Inhärenz, z. B. Fingerabdruck als biometrisches Merkmal des Users).

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

3. Zugang zum Corporate Portal
Der User erhält Zugang zum Corporate Portal der Bank, wenn
- er seine individuelle Userkennung (z. B. Kontonummer, Anmeldename) angibt und
- er sich unter Verwendung des oder der von der Bank angeforderten Authentifizierungselemente(s) ausweist und
- keine Sperre des Zugangs (siehe Ziffern 8.1 und 9 dieser Bedingungen) vorliegt.

Nach Gewährung des Zugangs zum Corporate Portal kann jeweils in dem von der Bank angebotenen Umfang auf Bankprodukte und Services sowie Informationen zugegriffen werden und können nach Ziffer 4 dieser Bedingungen bei bestimmten Bankprodukten Aufträge unmittelbar online über das Corporate Portal erteilt werden.

4. Aufträge

4.1 Auftragserteilung
Der User muss einem Auftrag, den er unmittelbar online über das Corporate Portal erteilt zu dessen Wirksamkeit zustimmen (Autorisierung). Auf Anforderung hat er hierzu Authentifizierungselemente (zum Beispiel Eingabe einer TAN als Nachweis des Besitzelements) zu verwenden. Die Anforderungen an einen Auftrag, der nicht unmittelbar online über das Corporate Portal erteilt wird (zum Beispiel die Übermittlung von Auftragsdaten an die Bank im Wege der Datenfernübertragung) richten sich nach den für das jeweilige Bankprodukt oder für eine der darin jeweils enthaltenen Auftragsart geltenden Verträgen und Sonderbedingungen (z. B. Bedingungen für die Datenfernübertragung).

4.2 Widerruf von Aufträgen
Die Widerrufbarkeit eines Auftrags richtet sich nach den für das jeweilige Bankprodukt oder für eine der darin jeweils enthaltenen Auftragsart geltenden Verträgen und Sonderbedingungen. Der Widerruf von Aufträgen kann nur außerhalb des Corporate Portals erfolgen, es sei denn, die Bank sieht eine Widerrufmöglichkeit im Corporate Portal ausdrücklich vor.

5. Bearbeitung von Aufträgen durch die Bank

5.1 Die Bearbeitung der Aufträge erfolgt an den für die Abwicklung der jeweiligen Auftragsart im Corporate Portal der Bank, in den für das jeweilige Bankprodukt geltenden Verträgen und Sonderbedingungen oder im »Preis- und Leistungsverzeichnis« bekannt gegebenen Geschäftstagen im Rahmen des ordnungsgemäßen Arbeitsablaufes. Geht der Auftrag nach dem im Corporate Portal der Bank, in den für das jeweilige Bankprodukt geltenden Verträgen und Sonderbedingungen oder im »Preis- und Leistungsverzeichnis« angegebenen Zeitpunkt (Annahmefrist) ein oder fällt der Zeitpunkt des Eingangs nicht auf einen Geschäftstag der Bank, so gilt der Auftrag als am darauf folgenden Geschäftstag zugegangen. Die Bearbeitung beginnt erst an diesem Geschäftstag.

5.2 Die Bank wird den Auftrag ausführen, wenn folgende Ausführungsbedingungen vorliegen:
- Der User hat den Auftrag autorisiert (vgl. Ziffer 4.1 dieser Bedingungen).
- Die Berechtigung des Users für das jeweilige Bankprodukt oder eine der darin jeweils enthaltenen Auftragsart (z. B. Wertpapierorder) liegt vor.
- Das jeweils vorausgesetzte Datenformat ist eingehalten.
- Ein etwaiges, gesondert vereinbartes Verfügungslimit ist nicht überschritten.
- Die weiteren Ausführungsvoraussetzungen nach den für das jeweilige Bankprodukt oder für eine der darin jeweils enthaltenen Auftragsart maßgeblichen Verträgen und Sonderbedingungen liegen vor.

Liegen die Ausführungsbedingungen nach Satz 1 vor, führt die Bank die Aufträge nach Maßgabe der Bestimmungen der für das jeweilige Bankprodukt oder den jeweiligen Geschäftsvorfall geltenden Verträgen und Sonderbedingungen (z. B. Bedingungen für das Wertpapiergeschäft) aus.

5.3. Liegen die Ausführungsbedingungen nach Ziffer 5.2 nicht vor, wird die Bank den Auftrag nicht ausführen. Sie wird dem User hierüber eine Information zur Verfügung stellen und soweit möglich dabei die Gründe und die Möglichkeiten nennen, mit denen Fehler, die zur Ablehnung geführt haben, berichtigt werden können.

6. Informationen

Die Bank kann verschiedene Informationen zur Geschäftsverbindung mittels Corporate Portal zur Verfügung stellen.

7. Sorgfaltspflichten des Users

7.1 Schutz der Authentifizierungselemente
(1) Der User hat alle zumutbaren Vorkehrungen zu treffen, um seine Authentifizierungselemente (siehe Ziffer 2 dieser Bedingungen) vor unbefugtem Zugriff zu schützen. Ansonsten besteht die Gefahr, dass das Corporate Portal missbräuchlich verwendet oder in sonstiger Weise nicht autorisiert genutzt wird (vergleiche Ziffer 3 und 4 dieser Bedingungen).
(2) Zum Schutz der einzelnen Authentifizierungselemente hat der User vor allem Folgendes zu beachten:
(a) Wissenselemente, wie z. B. die PIN, sind geheim zu halten; sie dürfen insbesondere
- nicht mündlich (z. B. telefonisch oder persönlich) mitgeteilt werden,
- nicht außerhalb des Corporate Portals in Textform (z. B. per E-Mail, Messenger-Dienst) weiter gegeben 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 Corporate Portal und Fingerabdrucksensor) dient.

(b) Besitzelemente, wie z. B. ein mobiles Endgerät, sind vor Missbrauch zu schützen, insbesondere
- ist sicherzustellen, dass unberechtigte Personen auf das mobile Endgerät des Users (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 Corporate Portal (z. B. Authentifizierungs-App) nicht nutzen können,
- ist die Anwendung für das Corporate Portal (z. B. Authentifizierungs-App) auf dem mobilen Endgerät des Users zu deaktivieren, bevor der User 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 Corporate Portal mündlich (z. B. per Telefon) oder in Textform (z. B. per E-Mail, Messenger-Dienst) weiter gegeben werden und
- muss der User, der von der Bank einen Code zur Aktivierung des Besitzelements (z. B. Mobiltelefon mit Anwendung für das 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 Corporate Portal des Users aktivieren
- ist die Signaturkarte vor dem unbefugten Zugriff anderer Personen sicher zu verwahren

(c) Seinselemente wie z. B. Fingerabdruck des Users dürfen auf einem mobilen Endgerät des Users für das 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 Corporate Portal genutzt wird, Seinselemente anderer Personen gespeichert, ist für das Corporate Portal das von der Bank ausgegebene Wissenselement (z. B. PIN) zu nutzen und nicht das auf dem mobilen Endgerät gespeicherte Seinselement.
(3) Ungeachtet der Schutzpflichten nach den Absätzen 1 bis 2 darf der User seine Authentifizierungselemente gegenüber einem von ihm ausgewählten Zahlungsauslösedienst und Kontoinformationsdienst sowie einem sonstigen Drittdienst verwenden. Sonstige Drittdienste hat der User mit der im Verkehr erforderlichen Sorgfalt auszuwählen.
(4) Nutzt der User die in den Bedingungen für die Datenfernübertragung genannten Legitimations- und Sicherheitsverfahren, (z. B. individuelles Schlüsselpaar), um sich für den Zugang zum Corporate Portal gegenüber der Bank zu authentifizieren, gelten für den Umgang mit diesen besonderen Authentifizierungselementen die Regelungen über die Verhaltens- und Sorgfaltspflichten im Umgang mit den Legitimationsmedien für die Autorisierung des Auftrags (gem. Ziffer IV), die Verhaltens- und Sorgfaltspflichten im Umgang mit den Sicherungsmedien für den Datenaustausch (gem. Ziffer V), der Sicherheit des Kundensystems (gem. Ziffer VI) und die Sperre der Legitimations- und Sicherungsmedien (gem. Ziffer VII) der Bedingungen für die Datenfernübertragung einschließlich derer Anlagen entsprechend.

7.2 Sicherheitshinweise der Bank
Der User muss die Sicherheitshinweise im Corporate Portal, insbesondere die Maßnahmen zur technischen Verbindung mit der Bank und zum Schutz der eingesetzten Hard- und Software (Kundensystem), beachten.

7.3 Prüfung der Auftragsdaten mit von der Bank angezeigten Daten
Zeigt die Bank dem User die von ihr empfangenen Auftragsdaten (zum Beispiel Betrag, IBAN des Zahlungsempfängers) über das gesondert vereinbarte Gerät des Users an (zum Beispiel mittels mobilem Endgerät), ist der User verpflichtet, vor der Bestätigung die Übereinstimmung der angezeigten Daten mit den für den Auftrag vorgesehenen Daten zu prüfen.

7.4 Informationspflicht des Kunden
Der Kunde ist verpflichtet seine User über die Bedingungen zur Nutzung des Corporate Portals und insbesondere die Sorgfaltspflichten des Users in dieser Ziffer 7 sowie die Anzeigepflichten und Unterrichtungspflicht in Ziffer 8 zu informieren und deren Einhaltung zu gewährleisten.

8. Anzeigepflichten und Unterrichtungspflichten

8.1 Sperranzeige
(1) Stellt der User
- den Verlust oder den Diebstahl eines Besitzelements zur Authentifizierung (z. B. mobiles Endgerät, Signaturkarte) oder
- die missbräuchliche Verwendung oder die sonstige nicht autorisierte Nutzung eines Authentifizierungselements

fest, muss der User die Bank hierüber unverzüglich unterrichten (Sperranzeige). Der User kann eine solche Sperranzeige jederzeit auch über die gesondert mitgeteilten Kommunikationskanäle abgeben.
(2) Der User hat jeden Diebstahl oder Missbrauch eines Authentifizierungselements unverzüglich bei der Polizei zur Anzeige zu bringen.
(3) Hat der User den Verdacht einer nicht autorisierten oder betrügerischen Verwendung eines seiner Authentifizierungselemente, muss er ebenfalls eine Sperranzeige abgeben.

8.2 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.

9. Nutzungssperre

9.1 Sperre auf Veranlassung des Users
Die Bank sperrt auf Veranlassung des Users, insbesondere im Fall der Sperranzeige nach Ziffer 8.1 dieser Bedingungen
- den Zugang zum Corporate Portal für ihn oder alle User oder
- seine Authentifizierungselemente zur Nutzung des Corporate Portal.

9.2 Sperre auf Veranlassung der Bank
(1) Die Bank darf den Zugang zum Corporate Portal für einen User sperren, wenn
- sie berechtigt ist, einen Vertrag über die Nutzung eines in das Corporate Portal eingebundenes Bankprodukt aus wichtigem Grund zu kündigen,
- sachliche Gründe im Zusammenhang mit der Sicherheit der Authentifizierungselemente des Users 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. Die Angabe von Gründen darf unterbleiben, soweit die Bank hierdurch gegen gesetzliche Verpflichtungen verstoßen würde.

9.3 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.

9.4 Automatische Sperre eines chip-basierten Authentifizierungsinstruments
(1) Eine Chipkarte mit Signaturfunktion sperrt sich selbst, wenn dreimal in Folge der Nutzungscode für die elektronische Signatur falsch eingegeben wird.
(2) Ein TAN-Generator als Bestandteil einer Chipkarte, der die Eingabe eines eigenen Nutzungscodes erfordert, sperrt sich selbst, wenn dieser dreimal in Folge falsch eingegeben wird.

(3) Die in Absätzen 1 und 2 genannten Besitzelemente können dann nicht mehr für das Corporate Portal genutzt werden. Der User kann sich mit der Bank in Verbindung setzen, um die Nutzungsmöglichkeiten des Corporate Portal wiederherzustellen.

9.5 Zugangssperre für Zahlungsauslösedienst und Kontoinformationsdienst
Die Bank kann Kontoinformationsdienstleistern oder Zahlungsauslösedienstleistern den Zugang zu einem Zahlungskonto des Kunden verweigern, wenn objektive und gebührend nachgewiesene Gründe im Zusammenhang mit einem nicht autorisierten oder betrügerischen Zugang des Kontoinformationsdienstleisters oder des Zahlungsauslösedienstleisters zum Zahlungskonto, einschließlich der nicht autorisierten oder betrügerischen Auslösung eines Zahlungsvorgangs, es rechtfertigen. Die Bank wird den Kunden über eine solche Zugangsverweigerung auf dem vereinbarten Weg unterrichten. Die Unterrichtung erfolgt möglichst vor, spätestens jedoch unverzüglich nach der Verweigerung des Zugangs. Die Angabe von Gründen darf unterbleiben, soweit die Bank hierdurch gegen gesetzliche Verpflichtungen verstoßen würde. Sobald die Gründe für die Verweigerung des Zugangs nicht mehr bestehen, hebt die Bank die Zugangssperre auf. Hierüber unterrichtet sie den Kunden unverzüglich.

10. Haftung

10.1 Haftung der Bank bei Ausführung eines nicht autorisierten Auftrags und eines nicht, fehlerhaft oder verspätetet ausgeführten Auftrags
Die Haftung der Bank bei einem nicht autorisierten Auftrag und einem nicht, fehlerhaft ausgeführten oder verspätetet Auftrag richtet sich nach den für das jeweilige Bankprodukt oder eine der darin jeweils enthaltenen Auftragsart maßgeblichen Verträgen oder Sonderbedingungen für den jeweiligen Geschäftsvorfall (z. B. Bedingungen für das Wertpapiergeschäft).

10.2 Haftung des Kunden bei missbräuchlicher Nutzung seiner Authentifizierungselemente

10.2.1 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 Verwendung eines Authentifizierungselements, haftet der Kunde bei schuldhaftem Handeln für den der Bank hierdurch entstehenden Schadens.
(2) Der Kunde ist nicht zum Ersatz des Schadens nach Absatz 1 verpflichtet, wenn der Verlust des Authentifizierungselements durch einen Angestellten, einen Agenten, eine Zweigniederlassung eines Zahlungsdienstleisters oder eine sonstige Stelle, an die Tätigkeiten des Zahlungsdienstleisters ausgelagert wurden, verursacht worden ist.
(3) Kommt es vor der Sperranzeige zu nicht autorisierten Zahlungsvorgängen und hat der User in betrügerischer Absicht gehandelt oder seine Sorgfalts- und Anzeigepflichten nach diesen Bedingungen vorsätzlich oder grob fahrlässig verletzt, trägt der Kunde abweichend von den Absätzen 1 und 2 den hierdurch entstandenen Schaden in vollem Umfang. Grobe Fahrlässigkeit des Users kann insbesondere vorliegen, wenn er eine seiner Sorgfaltspflichten nach
– Nummer 7.1 Absatz 2,
– Nummer 7.1 Absatz 4,
– Nummer 7.3 oder
– Nummer 8.1 Absatz 1

dieser Bedingungen verletzt hat.
(4) Abweichend von den Absätzen 1 und 3 ist der Kunde nicht zum Schadensersatz verpflichtet, wenn die Bank vom User eine starke Kundenauthentifizierung im Sinne des § 1 Absatz 24 ZAG nicht verlangt hat. Eine starke Kundenauthentifizierung erfordert insbesondere die Verwendung von zwei voneinander unabhängigen Authentifizierungselementen aus den Kategorien Wissen, Besitz oder Sein (siehe Ziffer 2 Absatz 3 dieser Bedingungen).
(5) Die Haftung für Schäden, die innerhalb des Zeitraums, für den der Verfügungsrahmen gilt, verursacht werden, beschränkt sich jeweils auf das vereinbarte Verfügungslimit.
(6) Der Kunde ist nicht zum Ersatz des Schadens nach den Absätzen 1 und 3 verpflichtet, wenn der User die Sperranzeige nach Ziffer 8.1 dieser Bedingungen nicht abgeben konnte, weil die Bank nicht die Möglichkeit zur Entgegennahme der Sperranzeige sichergestellt hatte und der Schaden dadurch eingetreten ist
(7) Die Absätze 2 und 4 bis 6 finden keine Anwendung, wenn der User in betrügerischer Absicht gehandelt hat.

10.2.2 Haftung des Kunden bei nicht autorisierten Verfügungen außerhalb von Zahlungsdiensten (z. B. Wertpapiertransaktionen) vor der Sperranzeige Beruhen nicht autorisierte Verfügungen außerhalb von Zahlungsdiensten (z. B. Wertpapiertransaktionen) vor der Sperranzeige auf der Nutzung eines verlorengegangenen oder gestohlenen Authentifizierungselements oder auf der sonstigen missbräuchlichen Nutzung eines Authentifizierungselements und ist der Bank hierdurch ein Schaden entstanden, haften der Kunde und die Bank nach den gesetzlichen Grundsätzen des Mitverschuldens.

10.2.3 Haftung der Bank ab der Sperranzeige
Sobald die Bank eine Sperranzeige erhalten hat, übernimmt sie alle danach durch im Corporate Portal erteilte nicht autorisierte Aufträge entstehenden Schäden. Dies gilt nicht, wenn der User in betrügerischer Absicht gehandelt hat.

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

11. Postfach

11.1 Leistungsangebot
(a) Die Bank stellt dem User ein Postfach im Corporate Portal als seinen elektronischen Briefkasten zur Verfügung.
(b) Die Bank ist berechtigt, dem User Mitteilungen und Informationen (im Folgenden einheitlich Dokumente), die die Geschäftsverbindung zwischen dem Kunden und der Bank betreffen, in einem lesbaren und speicherbaren Format (bspw. im pdf-Format) in sein Postfach einzustellen. Die Bank ist berechtigt, diese Dokumente dem Kunden ausschließlich auf elektronischem Wege im Postfach des Users zur Verfügung zu stellen.
(c) Die Bank ist jederzeit berechtigt, das Angebot der Einstellung von Dokumenten und in das Postfach zu erweitern oder einzuschränken. Hierüber wird die Bank den Kunden jeweils vorab unterrichten.

11.2 Unveränderbarkeit der Daten
Die Bank gewährleistet die Unveränderbarkeit der in das Postfach eingestellten und dort gespeicherten Dokumente.

11.3 Verzicht auf papierhafte Zurverfügungstellung
(1) Der Kunde verzichtet ausdrücklich nach Maßgabe dieser Bedingungen auf die papierhafte Zurverfügungstellung (z. B. durch Postversand) der in das Postfach einzustellenden bzw. eingestellten Dokumente. Die Bank kommt ihrer Verpflichtung zur Mitteilung, Übermittlung, Unterrichtung oder Zurverfügungstellung durch Einstellung der betreffenden Dokumente in das Postfach nach.
(2) Der Kunde stimmt der elektronischen Übermittlung von Rechnungen zu (§ 14 UStG).
(3) Hinweis für buchführungs bzw. aufbewahrungspflichtige Kunden: Die Anerkennung der im Postfach zur Verfügung gestellten Dokumente durch Finanz- oder Steuerbehörden insbesondere für buchführungs- und aufzeichnungspflichtige Personen kann durch die Bank nicht gewährleistet werden. Der Kunde sollte sich ggf. hierzu bei dem für ihn zuständigen Finanzamt informieren.

11.4 Benachrichtigung und Zugang
(1) Die Bank wird den User auf dem vereinbarten Kommunikationsweg (z. B. EMail) über die Einstellung neuer Dokumente benachrichtigen.
(2) Die Dokumente gehen dem Kunden in dem Zeitpunkt zu, in dem sie jeweils in abruf und speicherbarer Form in dem Postfach des Users zur Verfügung gestellt worden sind, der User über die Einstellung benachrichtigt worden ist und der User die Dokumente unter gewöhnlichen Umständen zur Kenntnis nehmen konnte. Unbeschadet von Absatz 2 gehen die Dokumente dem Kunden jedoch spätestens zu dem Zeitpunkt zu, in dem der User diese abgerufen hat.

11.5 Mitwirkungs- und Sorgfaltspflichten des Users
(1) Über Änderungen seiner Kontaktdaten für die Benachrichtigung nach Ziffer 11.4 wird der User die Bank unverzüglich informieren.
(2) Soweit der Corporate Portal Zugang auf Veranlassung (siehe Ziffer 9.1) oder aufgrund einer Handlung des Users gesperrt worden ist, ist dieser verpflichtet, alle erforderlichen Maßnahmen zu unternehmen, die es der Bank ermöglichen die Funktionsfähigkeit des Corporate Portal Zugangs des Users wiederherzustellen.
(3) Der User ist verpflichtet, die in sein Postfach eingestellten Dokumente regelmäßig und zeitnah abzurufen.

11.6 Bereitstellung und Aufbewahrung
(1) Die Bank verpflichtet sich, dem Kunden die Dokumente in dem Postfach des Users für die Dauer von mindestens zehn Jahren nach deren Einstellung zur Verfügung zu stellen. Dies gilt, solange der Kunde zum Corporate Portal angemeldet ist. Unbeschadet von Satz 2 endet die Frist zur Verfügungstellung der Dokumente für User, die Bevollmächtigte und gesetzliche Vertreter des Kunden sind, mit Erlöschen der Vollmacht bzw. Vertretungsberechtigung. Der User hat innerhalb der in Satz 1 genannten Frist jederzeit die Möglichkeit, im Postfach vorhandene Dokumente anzusehen, auszudrucken, zu archivieren oder auf einem eigenen Datenträger zu speichern.
(2) Nach Ablauf der Frist nach Absatz (1) ist die Bank berechtigt, die Dokumente aus dem Postfach zu entfernen. Etwaige gesetzliche Aufbewahrungsfristen der Bank und das Recht des Kunden, eine Zweitschrift eines Dokuments zu verlangen, bleiben von den in Absatz 1 genannten Fristen unberührt.
(3) Die Bank ist jederzeit berechtigt, bei technischen Problemen einzelne oder auch alle Dokumente auf dem Postweg oder in sonstiger Weise an den User und den Kunden zu übermitteln, wenn dies von der Bank unter Berücksichtigung des User-/Kundeninteresses als zweckmäßig erachtet wird. Die Bank ist darüber hinaus jederzeit aufgrund von gesetzlichen oder aufsichtsrechtlichen Verpflichtungen berechtigt, einzelne oder alle Dokumente auf dem Postweg oder in sonstiger Weise an den User und den Kunden zu übermitteln.

11.7 Änderungen
Die Bank ist berechtigt, das Angebot des Postfachs teilweise oder ganz jederzeit einzustellen; eine Verpflichtung zur Aufrechterhaltung des Angebots des Postfachs im Corporate Portal besteht nicht. Über eine Einstellung wird die Bank rechtzeitig vorab informieren, so dass der Kunde ausreichend Zeit hat, sich seine im Postfach befindlichen Dokumente herunterzuladen und bei sich zu archivieren. Die Bank wird dem Kunden neue Dokumente ab dem Zeitpunkt der Einstellung des Postfachs in Papierform per Postversand, per Kontoauszugsdrucker oder auf elektronischem Wege zur Verfügung stellen.