COMMERZBANK
Die Bank an Ihrer Seite

Bedingungen für die Abwicklung von Bankgeschäften über das Firmenkundenportal

Stand: Juni 2018, Commerzbank AG Niederlassung Wien, Österreich

1. Leistungsumfang

(1) Der Kunde (Kontoinhaber, der Nicht-Verbraucher im Sinne des ZaDiG 2018 ist) kann das Firmenkundenportal nutzen und Bankgeschäfte über das Firmenkundenportal in dem der Bank angebotenen Umfang abwickeln. Für die Abwicklung gelten die Bedingungen für die jeweiligen Bankgeschäfte (z. B. allgemeine Geschäftsbedingungen, Sonderbedingungen für Commerzbank Online Banking Wertpapiergeschäft, Main Funders). Zudem kann der Kunde Informationen der Bank über das Firmenkundenportal abrufen. Der Kunde ist zusätzlich berechtigt für die Auslösung eines Zahlungsauftrages einen Zahlungsauslösedienst gemäß § 1 Absatz 2 Ziffer 7 ZaDiG 2018 und für die Mitteilung von Informationen über ein Zahlungskonto einen Kontoinformationsdienstleister gemäß § 1 Absatz 2 Ziffer 8 ZaDiG 2018 zu nutzen.

(2) Kunde und Bevollmächtigte werden im Folgenden einheitlich als "Teilnehmer" oder "Nutzer" bezeichnet. Hierunter fallen auch "Nutzer" gemäß den Bedingungen für die Datenfernübertragung, der die Datenfernübertragung im Rahmen des Firmenkundenportals nutzt. Konto und Depot werden im Folgenden einheitlich als "Konto" bezeichnet.

(3) Kunde und Bank können Verfügungslimits für bestimmte Servicearten gesondert vereinbaren.

2. Voraussetzungen zur Nutzung des Firmenkundenportals

Der Teilnehmer/Nutzer benötigt für die Nutzung des Firmenkundenportals die mit der Bank vereinbarten, personalisierten Sicherheitsmerkmale und Authentifizierungsinstrumente, um sich gegenüber der Bank als berechtigter Teilnehmer/Nutzer auszuweisen (siehe Nummer 3) und Aufträge zu autorisieren/rechtsgeschäftliche Erklärungen abzugeben (siehe Nummer 4). Statt eines personalisierten Sicherheitsmerkmals kann auch ein biometrisches Merkmal des Teilnehmers/Nutzers zum Zwecke der Authentifizierung bzw. Autorisierung vereinbart werden.

Die Bank wird Authentifizierungsinstrumente ab 1.12.2019 nur auf der Grundlage einer starken Authentifizierung im Sinne des § 4 Z 28 ZaDiG 2018 für Autorisierungszwecke von Zahlungsvorgängen nach § 87 ZaDiG 2018 zulassen.

2.1. Personalisierte Sicherheitsmerkmale

Personalisierte Sicherheitsmerkmale, die auch alphanumerisch sein können, sind personalisierte Merkmale, die die Bank dem Teilnehmer zum Zwecke der Authentifizierung bereitstellt. Dies sind beispielsweise:

- die Persönliche Identifikationsnummer (PIN),
- einmal verwendbare Transaktionsnummern (photoTAN) und
- die Signatur-PIN/das Kennwort und die Daten des persönlichen elektronischen Schlüssels für die elektronische Signatur.

2.2. Authentifizierungsinstrumente

Die photoTAN kann für den Teilnehmer/Nutzer mittels eines mobilen End- oder Lesegeräts generiert und ihm zur Verfügung gestellt werden. Der Teilnehmer/Nutzer kann weitere Authentifizierungsinstrumente zur Freigabe von Transaktionen nutzen:

- eine Chipkarte mit Signaturfunktion oder
- ein sonstiges Authentifizierungsinstrument, auf dem sich der Signaturschlüssel befindet einschließlich einer Speicherung der elektronischen Schlüssel in einer von der Bank (oder einem von der Bank zugelassenen Dienstleister) zur Verfügung gestellten technischen Umgebung, die vor unautorisiertem Zugriff geschützt ist,
- eine von der Bank im Initialisierungsprozess für den Teilnehmer/Nutzer personalisierte App.

2.3. Vereinbarung der personalisierten Sicherheitsmerkmale und Authentifizierungsinstrumente

Jeder Teilnehmer/Nutzer kann mit der Bank vereinbaren, welches personalisierte Sicherheitsmerkmal und Autorisierungsinstrument von ihm verwendet werden soll.

3. Zugang zum Firmenkundenportal

Der Teilnehmer/Nutzer erhält Zugang zum Firmenkundenportal, wenn

- dieser die Teilnehmernummer/den Anmeldenamen und die PIN übermittelt,
- die Prüfung dieser Daten bei der Bank eine Zugangsberechtigung des Teilnehmers/Nutzers ergeben hat und
- keine Sperre des Zugangs (siehe Nummern 9.1 und 10) vorliegt.

Nach Gewährung des Zugangs zum Firmenkundenportal kann der Teilnehmer/Nutzer Informationen abrufen oder Aufträge erteilen. Die Sätze 1 und 2 gelten auch, wenn der Teilnehmer Zahlungsaufträge über einen Zahlungsauslösedienst auslöst und Zahlungskontoinformationen über einen Kontoinformationsdienst anfordert (siehe Nummer 1 Absatz 1 Satz 4).

4. Auftragsabwicklung im Rahmen des Firmenkundenportals

4.1. Auftragserteilung und Autorisierung

Die Autorisierung zur Durchführung einzelner Geschäfte (z. B. Überweisung) erfolgt - abhängig von der gewählten Serviceart - mittels der vereinbarten personalisierten Sicherheitsmerkmale

- photoTAN
- PIN
- elektr. Signatur

- biometrische Signatur bzw.
- nach Anmeldung mit Teilnehmernummer bzw. Anmeldenamen und PIN durch einfache Freigabe.

Satz 1 gilt auch, wenn der Teilnehmer einen Zahlungsauftrag über einen Zahlungsauslösedienst (siehe Nummer 1 Absatz 4) auslöst und übermittelt.

4.2. Ergänzende Regelungen für die Datenfernübertragung im EBICS-Standard bei Einsatz des photoTAN-Verfahrens

4.2.1. Der Kunde beauftragt die Bank mit der Speicherung des persönlichen Schlüssels des Teilnehmers/Nutzers in einer technischen Umgebung, die vor unautorisiertem Zugriff geschützt ist. Die Bank ist berechtigt, hierfür auch einen zuverlässigen Dienstleister zu beauftragen. Das zur Freigabe des persönlichen Schlüssels erforderliche Kennwort wird durch die TAN im photoTAN-Verfahren ersetzt.

4.2.2. Die Bedingungen für die Datenfernübertragung werden wie folgt ergänzt:

- Ergänzend zu Ziffer 4(2) der Bedingungen für die Datenfernübertragung gilt, dass die Aufbewahrung der elektronischen Schlüssel in einer von der Bank (oder von einem von der Bank zugelassenen Dienstleister) zur Verfügung gestellten technischen Umgebung (vgl. Ziffer 2.2.1. (5) der Anlage 1a der Bedingungen für die Datenfernübertragung) erlaubt ist.

- Zu Ziffer 7(3) wird vereinbart, dass die Bank die Legitimation auch daraufhin prüft, ob die richtige photoTAN eingegeben wurde.

4.2.3. Die Anlage 1a der Bedingungen für die Datenfernübertragung wird wie folgt ergänzt:

- Die Authentifikationssignatur kann in Ziffer 1.2 beim photoTAN-verfahren auch in der technischen Umgebung der Bank oder des zugelassenen Dienstleisters geleistet werden. Diese nehmen für den Kunden die erforderliche Prüfung vor.
- zu Ziffer 2.2.1. (5) wird vereinbart, dass die photoTAN anstelle des Passwortes verwendet wird, wenn das Sicherungsmedium des Teilnehmers bankseitig in einer technischen Umgebung gespeichert ist, die vor unautorisiertem Zugriff geschützt ist.
- Die Autorisierung von Aufträgen gemäß Ziffer 3 kann auch durch Eingabe der auf dem mobilen End- oder Lesegerät angezeigten photoTAN und der daraufhin in der gesicherten technischen Umgebung erzeugten elektronischen Signatur erteilt werden.

4.3. Einhaltung von Meldeverordnungen

Bei Zahlungen zugunsten Gebietsfremder ist vom Teilnehmer/Nutzer die Meldepflicht nach den auf § 6 Abs. 2 und Abs. 3 Devisengesetz 2004 von der OeNB erlassenen Meldeverordnungen (derzeit "ZABIL 1/2013" in der novellierten Form 1/2016, sowie die Verordnung betreffend statistische Erhebungen über die Importe und Exporte von Dienstleistungen und grenzüberschreitende Finanzbeziehungen) zu beachten.

4.4. 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 Firmenkundenportals erfolgen, es sei denn, die Bank sieht eine Widerrufsmöglichkeit im Firmenkundenportal ausdrücklich vor.

5. Bearbeitung von Aufträgen durch die Bank

(1) Die Bearbeitung der im Rahmen des Firmenkundenportals erteilten Aufträge erfolgt nach den für die Abwicklung der jeweiligen Auftragsart (z. B. Überweisung oder Wertpapierauftrag) geltenden Regelungen der vereinbarten Serviceart.

(2) Für Zahlungsaufträge (Überweisung, Lastschrift) gelten folgende Sonderregelungen:
Die Bank wird den Zahlungsauftrag ausführen, wenn folgende Ausführungsbedingungen vorliegen:
- Der Teilnehmer/Nutzer hat sich mit seinem personalisierten Sicherheitsmerkmal legitimiert.
- Die Berechtigung des Teilnehmer/Nutzers für die jeweilige Auftragsart liegt vor.
- Das für die vereinbarte Serviceart erforderliche Datenformat ist eingehalten.
- Das für die Serviceart gesondert vereinbarte Verfügungslimit ist nicht überschritten.
- Die weiteren Ausführungsvoraussetzungen nach den für die jeweilige Auftragsart maßgeblichen Sonderbedingungen liegen vor.
- Es ist eine ausreichende Kontodeckung (Guthaben oder eingeräumter Kredit) vorhanden.

Liegen die Ausführungsbedingungen nach Satz 1 vor, führt die Bank den Zahlungsauftrag aus. Die Ausführung darf nicht gegen sonstige Rechtsvorschriften verstoßen.

(3) Liegen die Ausführungsbedingungen nach Absatz (2) Satz 1 Spiegelstrich 1-5 nicht vor, wird die Bank den Zahlungsauftrag nicht ausführen Die Bank wird den Teilnehmer/Nutzer 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 vereinbarter Zins zu zahlen ist.

6. Information des Kunden über im Rahmen des Firmenkundenportals erteilte Verfügungen

Die Bank unterrichtet den Kunden über die im Rahmen des Firmenkundenportals getätigten Verfügungen auf dem für Konto- und Depotinformationen vereinbarten Weg und gemäß den für den Auftrag geltenden Bedingungen.

7. Sorgfaltspflichten des Teilnehmers/Nutzers

7.1. Technische Verbindung zum Firmenkundenportal

Der Teilnehmer/Nutzer ist verpflichtet, die technische Verbindung zum Firmenkundenportal nur über die von der Bank gesondert mitgeteilten Zugangskanäle (z. B. Internetadresse) herzustellen. Zur Auslösung eines Zahlungsauftrags und zum Abruf von Informationen über ein Zahlungskonto kann der Teilnehmer die technische Verbindung zum Firmenkundenportal auch über einen Zahlungsauslösedienst bzw. einen Kontoinformationsdienst (siehe Nummer 1 Absatz 1 Satz 4) herstellen. Der Teilnehmer/Nutzer 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. Apps der Bank dürfen nur von App-Anbietern bezogen werden, die die Bank dem Kunden mitgeteilt hat. Der Teilnehmer/Nutzer hat eigenverantwortlich die landesspezifischen Regelungen für die Nutzung des Internets zu beachten.

7.2. Geheimhaltung der personalisierten Sicherheitsmerkmale und sichere Aufbewahrung der Authentifizierungsinstrumente

(1) Der Teilnehmer/Nutzer hat

- seine personalisierten Sicherheitsmerkmale (siehe Nummer 2.1) geheim zu halten sowie
- sein Authentifizierungsinstrument (siehe Nummer 2.2) vor dem Zugriff anderer Personen sicher zu verwahren.

Denn jede andere Person, die im Besitz des Authentifizierungsinstruments ist, kann in Verbindung mit dem dazugehörigen personalisierten Sicherheitsmerkmal das Verfahren missbräuchlich nutzen. Die Geheimhaltungspflicht bezüglich der personalisierten Sicherheitsmerkmale nach Satz 1 gilt nicht, wenn der Teilnehmer diese zur Erteilung eines Zahlungsauftrags oder zum Abruf von Informationen über ein Zahlungskonto an den von ihm ausgewählten Zahlungsauslösedienst beziehungsweise Kontoinformationsdienst übermittelt (siehe Nummer 1 Absatz 1 Satz 4).

(2) Insbesondere ist Folgendes zum Schutz des personalisierten Sicherheitsmerkmals sowie des Authentifizierungsinstruments zu beachten:

- Die personalisierten Sicherheitsmerkmale PIN und die Signatur-PIN/das Kennwort dürfen bei einem Teilnehmer/Nutzer nicht elektronisch gespeichert werden (z.B. im Kundensystem). Der vom Teilnehmer/Nutzer erzeugte persönliche elektronische Schlüssel darf sich nur in der alleinigen Verfügungsgewalt des Teilnehmers/Nutzers befinden 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 Nutzer" eingesetzt, ist die elektronisch gespeicherte Signatur in einer sicheren und entsprechend geeigneten technischen Umgebung zu speichern. Der "Technische Nutzer" ist nicht berechtigt, die Auftragserteilung selbst vorzunehmen. Er übermittelt lediglich die Auftragsdaten.
- Bei Eingabe des personalisierten Sicherheitsmerkmals ist sicherzustellen, dass andere Personen diese nicht ausspähen können.
- Das personalisierte Sicherheitsmerkmal darf nicht per E-Mail weitergegeben werden.
- Die Signatur-PIN/das Kennwort für die elektronische Signatur dürfen nicht zusammen mit dem Authentifizierungsinstrument verwahrt werden.
- Der Teilnehmer/Nutzer darf zur Autorisierung eines Auftrags nicht mehr als eine photoTAN verwenden.

7.3. Obliegenheit des Kunden zur Sicherheit des Kundensystems

Der Teilnehmer/Nutzer muss die Sicherheitshinweise auf der Internetseite der Bank unter https://www.firmenkunden.commerzbank.de/portal/de/cb/de/footer/sicherheit/home.html, insbesondere die Maßnahmen zum Schutz der eingesetzten Hard- und Software, beachten und aktuelle, dem Stand der Technik entsprechende Virenschutz- und Firewall-Systeme installieren. Insbesondere dürfen das Betriebssystem und die Sicherheitsvorkehrungen des mobilen Endgerätes nicht modifiziert oder deaktiviert werden.

7.4. Kontrolle der Auftragsdaten mit von der Bank angezeigten Daten

Soweit die Bank dem Teilnehmer/Nutzer Daten aus seinem über das Firmenkundenportal erteilten Auftrag (z. B. Betrag, Kontonummer des Zahlungsempfängers, Wertpapierkennnummer) im Kundensystem oder über ein anderes Gerät des Teilnehmers/Nutzers (z.B. photoTAN-Lesegerät, photoTAN-App, Chipkartenlesegerät mit Display) zur Bestätigung anzeigt, ist der Teilnehmer/Nutzer verpflichtet, vor der Bestätigung die Übereinstimmung der angezeigten Daten mit den für die Transaktion vorgesehenen Daten zu prüfen.

7.5. Weitere Sorgfaltspflichten des Kunden

Der Kunde trägt dafür Sorge, dass die Sorgfaltspflichten aus diesem Vertrag auch von dem Bevollmächtigten (also von allen Teilnehmern/Nutzern) 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/Nutzer

- den Verlust oder den Diebstahl des Authentifizierungsinstruments,
- die missbräuchliche Verwendung oder
- die sonstige nicht autorisierte Nutzung seines Authentifizierungsinstruments oder seines persönlichen Sicherheitsmerkmals

fest, muss der Teilnehmer/Nutzer die Bank hierüber unverzüglich unterrichten (Sperranzeige). Der Teilnehmer/Nutzer kann der Bank eine Sperranzeige jederzeit auch über die gesondert mitgeteilte Sperrhotline abgeben. Bei Nichtzustandekommen des Leitungsaufbaues oder bei Störungen ist der Kunde verpflichtet - zur Schadensminderung - umgehend die anderen Kommunikationsmittel auszuschöpfen (z. B. Telefonanruf bei dem Kundenbetreuer).

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

(3) Hat der Teilnehmer/Nutzer den Verdacht, dass eine andere Person unberechtigt

- den Besitz an seinem Authentifizierungsinstrument oder die Kenntnis seines personalisierten Sicherheitsmerkmals erlangt hat oder
- das Authentifizierungsinstrument oder das personalisierte Sicherheitsmerkmal verwendet, muss er 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.

9.3. Beweismittel

Die Bank hat dem Kunden auf Anfrage Beweismittel zur Verfügung zu stellen, mit denen der Kunde bis zu 18 Monate nach der Anzeige beweisen kann, ob er seiner Anzeigepflicht gemäß den Nummern 9.1 und 9.2 nachgekommen ist.

10. Nutzungssperre

10.1. Sperre auf Veranlassung des Teilnehmers/Nutzers

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

- den Zugang zum Firmenkundenportal für ihn und, falls der Teilnehmer/Nutzer dies verlangt, den Zugang für alle Teilnehmer/Nutzer des Kunden oder
- sein Authentifizierungsinstrument.

10.2. Sperre auf Veranlassung der Bank

(1) Die Bank darf den Zugang zum Firmenkundenportal für einen Teilnehmer/Nutzer sperren, wenn
- sie berechtigt ist, den Vertrag über die Zusammenarbeit im Bereich Commerzbank Transaction Services aus wichtigem Grund zu kündigen,
- sachliche Gründe im Zusammenhang mit der Sicherheit des Authentifizierungsinstruments oder des personalisierten Sicherheitsmerkmals dies rechtfertigen,
- der Verdacht einer nicht autorisierten oder einer betrügerischen Verwendung des Authentifizierungsinstruments oder des personalisierten Sicherheitsmerkmals besteht oder
- wenn der Kontoinhaber seinen Zahlungspflichten im Zusammenhang mit einer mit dem eBanking im Firmenkundenportal verbundenen Kreditlinie (Überschreitung oder Überziehung) nicht nachgekommen ist, und entweder die Erfüllung dieser Zahlungspflichten aufgrund einer Verschlechterung oder Gefährdung der Vermögensverhältnisse des Kunden oder eines Mitverpflichteten gefährdet ist; oder beim Kunden die Zahlungsunfähigkeit eingetreten ist oder diese unmittelbar droht.

(2) Die Bank wird den Kunden unter Angabe der hierfür maßgeblichen Gründe möglichst vor, spätestens jedoch unverzüglich nach der Sperre in Textform (z.B. mittels Brief, Telefax oder E-Mail) oder telefonisch unterrichten.

(3) Die Bank ist zudem berechtigt, einem Kontoinformationsdienstleister oder einem Zahlungsauslösedienstleister den Zugang zum Zahlungskonto des Kunden zu verweigern, wenn der begründete Verdacht eines nicht autorisierten Zugangs oder einer betrügerischen Auslösung eines Zahlungsvorgangs besteht. Die Bank wird den Kunden – soweit eine Bekanntgabe der Verweigerung oder der Gründe der Verweigerung nicht österreichischen oder gemeinschaftsrechtlichen Rechtsnormen oder objektiven Sicherheitserwägungen zuwiderlaufen würde – über eine solche Verweigerung des Zugangs zum Zahlungskonto des Kunden in einer mit dem Kunden vereinbarten Form möglichst vor, spätestens aber unverzüglich nach der Verweigerung des Zugangs informieren.

10.3. Aufhebung der Sperre

Die Bank wird eine Sperre aufheben oder das personalisierte Sicherheitsmerkmal beziehungsweise das Authentifizierungsinstrument austauschen, wenn die Gründe für die Sperre nicht mehr gegeben sind. Hierüber unterrichtet sie den Kunden in Textform (z.B. mittels Brief, Telefax oder E-Mail) oder telefonisch.

10.4. Automatische Sperre

(1) Die Chipkarte mit Signaturfunktion wird gesperrt, wenn dreimal in Folge der Nutzungscode falsch eingegeben wurde. Eine Wiederfreischaltung bzw. Entsperrung der Chipkarte durch die Bank ist nicht möglich. Der Teilnehmer/Nutzer muss eine neue elektronische Signatur erstellen und diese erneut an die Bank übermitteln sowie mittels eines INI-Briefes bei der Bank freigeben.

(2) Die PIN wird gesperrt, wenn dreimal in Folge die PIN falsch eingegeben wurde.

(3) Der Teilnehmer/Nutzer wird für das photoTAN-Verfahren gesperrt, wenn fünfmal hintereinander die TAN falsch eingegeben wird.

(4) Der Teilnehmer/Nutzer kann sich mit der Bank in Verbindung setzen, um die Nutzungsmöglichkeiten des Firmenkundenportals wiederherzustellen. Die Bank hat den Kunden unverzüglich nach der Sperrung von der Sperrung und den Gründen in der mit dem Kunden vereinbarten Form unterrichten, außer dies würde objektiven Sicherheitserwägungen oder gemeinschaftsrechtlichen oder innerstaatlichen Regelungen zuwiderlaufen oder gerichtliche oder verwaltungsbehördliche Anordnungen verletzen.

11. Haftung beim Einsatz von Personalisierten Sicherheitsmerkmalen und/oder Authentifizierungsinstrumenten

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 abhandengekommenen Authentifizierungsinstruments oder auf der sonstigen missbräuchlichen Nutzung des personalisierten Sicherheitsmerkmals oder des Authentifizierungsinstruments, haftet der Kunde für den der Bank hierdurch entstehenden Schaden, wenn dem Teilnehmer/Nutzer an dem Verlust, Diebstahl, sonstigem Abhandenkommen oder der sonstigen missbräuchlichen Nutzung des personalisierten Sicherheitsmerkmals oder des Authentifizierungsinstruments 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. Auch wenn der Kunde seine Sorgfaltspflichten nach § 63 ZaDiG 2018 schuldhaft verletzt hat, haftet er gegenüber der Bank. 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.

(2) Der Kunde ist nicht zum Ersatz des Schadens nach den Absätzen 1 verpflichtet, wenn der Teilnehmer/Nutzer 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 mit dem Kunden für das Firmenkundenportal vereinbarte Verfügungslimit gilt, verursacht werden, beschränkt sich jeweils auf dieses Limit.

(4) Die Absätze 2 und 3 finden keine Anwendung, wenn der Teilnehmer in betrügerischer Absicht gehandelt hat.

11.2. Haftung bei nicht autorisierten Wertpapiertransaktionen oder bei anderen Servicearten vor der Sperranzeige

Beruhen nicht autorisierte Wertpapiertransaktionen oder nicht autorisierte Transaktionen bei den vereinbarten Servicearten vor der Sperranzeige auf der Nutzung eines verlorengegangenen, gestohlenen oder sonst abhanden gekommenen Authentifizierungsinstruments oder auf der sonstigen missbräuchlichen Nutzung des personalisierten Sicherheitsmerkmals oder des Authentifizierungsinstruments und ist der Bank hierdurch ein Schaden entstanden, haftet der Kunde für den der Bank hierdurch entstandenen Schaden, wenn dem Teilnehmer/Nutzer an dem Verlust, Diebstahl, sonstigen Abhandenkommen oder der sonstigen missbräuchlichen Nutzung des personalisierten Sicherheitsmerkmals oder des Authentifizierungsinstruments 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.

11.3. Haftung der Bank ab der Sperranzeige

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

12. Verfügbarkeit

Die Bank strebt an, die im Firmenkundenportal 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 Kunden und dem Nutzer eine 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 Funktionalitäten der im Firmenkundenportal angebotenen Services an. Die Bank besetzt die Hotline während der für das österreichische Bankgewerbe geltenden Bankarbeitstage zu finden unter https://www.oenb.at/Service/Bankfeiertage.html (Montag bis Freitag, ausgenommen gesetzliche Feiertage, 24.12. und Karfreitag).
Telefonnummern und Geschäftszeiten werden in den Zugangswegen (z.B. https://www.commerzbank.at) kommuniziert.

16. Abbedingung von §§ 9, 10 ECG der dispositiven Bestimmungen des E-Commerce-Gesetzes und des ZaDiG 2018

Die Vorschriften der §§ 9, 10 ECG (E–Commerce–Gesetz) werden hiermit abbedungen.
Gegenüber dem Kunden werden folgende Bestimmungen des Zahlungsdienstegesetzes 2018 (ZaDiG) nicht Vertragsbestandteil: die Bestimmungen des 3 Hauptstückes des ZaDiG 2018 (Zahlungsdienstegesetzes 2018), somit §§ 32-54 (Informationspflichten), §§ 32 bis 54, § 56 (1) [Entgeltverbot für die Erfüllung der Informationspflichten oder für Berichtigungs-und Schutzmaßnahmen], § 58 (3) [Widerruf der Autorisierung], § 66 (1) und (3) [Nachweis der Authentifizierung und Ausführung von Zahlungsvor-gängen], § 68 (2),(5)und (6) [Haftung für nicht autorisierte Zahlungsvorgänge],§ 70 (1) und (3) [Erstattung eines vom Zahlungsempfänger ausgelösten Zahlungsvorganges], § 80 [Haftung der Zahlungsdienstleister für nicht erfolgte, fehlerhafte oder verspätete Ausführung von Zahlungsvorgängen]. In § 68 (1) entfällt gegenüber Unternehmern die Wortfolge „bis zu einem Betrag von 50 Euro“.

17. Änderungsklausel

Diese Bedingungen über für die Abwicklung von Bankgeschäften über das Firmenkundenportal (im Folgenden "Bedingungen") sind im Internet abrufbar unter
https://www.commerzbank.at. Die Bank stellt diese Geschäftsbedingungen dem Kunden auch auf Wunsch jederzeit zur Verfügung.
Änderungen dieser Bedingungen über für die Abwicklung von Bankgeschäften über das Firmenkundenportal - mit Ausnahme von Hauptleistungen der Bank oder von Entgelten - werden dem Kunden vom Kreditinstitut spätestens zwei Monate vor dem vorgeschlagenen Zeitpunkt ihres Inkrafttretens angeboten. Dabei werden die vom Änderungsangebot betroffenen Bestimmungen und die vorgeschlagenen Änderungen in einer Gegen-

überstellung dieser Bestimmungen dargestellt. Die Zustimmung des Kunden gilt als erteilt, wenn bei der Bank vor dem vorgeschlagenen Zeitpunkt des Inkrafttretens kein Widerspruch des Kunden einlangt. Darauf wird die Bank den Kunden im Änderungsangebot hinweisen. Außerdem wird die Bank eine Gegenüberstellung über die von der Änderung der Bedingungen betroffenen Bestimmungen sowie die vollständige Fassung der neuen Bedingungen auf seiner Internetseite veröffentlichen. Auch darauf wird die Bank im Änderungsangebot hinweisen. Die Mitteilung an den Kunden kann in Papierform oder, sofern mit dem Kunden vereinbart, in elektronischer Form erfolgen oder kann auf eine mit dem Kunden vereinbarte Weise zum Abruf bereit zu halten.

Änderungen der vorgenannten Geschäftsbedingungen müssen unter Berücksichtigung aller Umstände (gesetzliche, aufsichtsbehördliche und sonstige behördliche Anforderungen, Gerichtsurteile, die Sicherheit des Bankbetriebs, die technische Entwicklung, Änderung der vorherrschenden Kundenbedürfnisse oder des erheblich gesunkenen Nutzungsgrads der Leistung, der die Kostendeckung wesentlich beeinträchtigt) sachlich gerechtfertigt sein.