COMMERZBANK
Die Bank an Ihrer Seite

Bedingungen für die Abwicklung von Bankgeschäften über das Firmenkundenportal

Gegenüberstellung der geänderten Bestimmungen
Commerzbank AG Niederlassung Wien, Österreich

Stand Februar 2017	Stand: Juni 2018
1. Leistungsangebot (1) Der Kunde 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. Firmenkundenbedingungen für Zahlungsdienste, Sonderbedingungen für Commerzbank Online Banking Wertpapiergeschäft, Main Funders). Zudem kann er Informationen der Bank über das Firmenkundenportal abrufen. (3) Zur Nutzung des Firmenkundenportals gelten die Standardlimite oder die mit der Bank gesondert vereinbarten Verfügungslimite für die vereinbarte Serviceart.	**1. Leistungsangebot** (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. ~~Firmenkundenbedingungen für Zahlungsdienste~~ allgemeine Geschäftsbedingungen, Sonderbedingungen für Commerzbank Online Banking Wertpapiergeschäft, Main Funders). Zudem kann ~~er~~ 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. (3) ~~Zur Nutzung des Firmenkundenportals gelten die Standardlimite oder die mit der Bank gesondert vereinbarten Verfügungslimite für die vereinbarte Serviceart.~~ Kunde und Bank können Verfügungslimits für bestimmte Servicearten gesondert vereinbaren.
2. Voraussetzungen zur Nutzung des Firmenkundenportals Der Teilnehmer/Nutzer benötigt für die Abwicklung von Bankgeschäften 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). Jeder Teilnehmer/Nutzer kann mit der Bank vereinbaren, welches personalisierte Sicherheitsmerkmal und Autorisierungsinstrument von ihm verwendet werden soll. **2.1 Personalisierte Sicherheitsmerkmale** Personalisierte Sicherheitsmerkmale, die auch alphanumerisch sein können, sind: • 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. Voraussetzungen zur Nutzung des Firmenkundenportals** Der Teilnehmer/Nutzer benötigt für die Abwicklung von Bankgeschäften 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). ~~Jeder Teilnehmer/Nutzer kann mit der Bank vereinbaren, welches personalisierte Sicherheitsmerkmal und Autorisierungsinstrument von ihm verwendet werden soll.~~ 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.

	2.3 *(neu)* Vereinbarung der personalisierten Sicherheitsmerk-male 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.	**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. Unterschrift bzw. • nach Anmeldung mit Teilnehmernummer bzw. Anmeldenamen und PIN durch einfache Freigabe.	**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. ~~Unterschrift~~ Signatur ~~bzw.~~ • *(neu)* 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. *(neu)* Ergänzende Regelungen für die Datenfernübertragung im EBICS-Standard bei Einsatz des photoTAN-Verfahrens** 4.2.1. *(neu)* Der Kunde beauftragt die Bank mit der Speicherung des persönlichen Schlüssels des Teilnehmers/Benutzers 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. *(neu)* 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. *(neu)* 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.
4.2 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 Melde-verordnungen (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.	**~~4.2~~ 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.
4.3 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 Firmenkundenportals erfolgen, es sei denn, die Bank sieht eine Widerrufsmöglichkeit im Firmenkundenportal ausdrücklich vor.	**~~4.3~~ 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 (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 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. (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.	**5. Bearbeitung von Aufträgen durch die Bank** (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 ~~oder das Standardlimit~~ 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. (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.
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. Der Kunde ist dafür verantwortlich, dass er für seine eigenen Systeme eine angemessene Datensicherung unter-hält und stets nach dem Stand der Technik ausreichende Vorkehrungen gegen Viren und andere schädliche Programme (z. B. Trojaner, Würmer	**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

etc.) trifft. Apps der Bank dürfen nur von App-Anbietern bezogen werden, die die Bank dem Kunden mitgeteilt hat. Der Kunde hat eigenverantwortlich die landes-spezifischen Regelungen für die Nutzung des Internets zu beachten.	(siehe Nummer 1 Absatz 1 Satz 4) herstellen. Der ~~Kunde~~ 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 ~~Kunde~~ Teilnehmer/Nutzer hat eigenverantwortlich die landesspezifischen Regelungen für die Nutzung des Internets zu beachten.
7.2 Geheimhaltung der personalisierten Sicherheitsmerk-male und sichere Aufbewahrung der Authentifizierungsinstrumente (1) Der Teilnehmer/Nutzer hat seine personalisierten Sicherheitsmerkmale (siehe Nummer 2.1) geheim zu halten und nur über die von der Bank gesondert für das Firmenkundenportal mitgeteilten Zugangskanäle oder über von der Bank herausgegebene Apps zu übermitteln 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.	**7.2. Geheimhaltung der personalisierten Sicherheitsmerk-male und sichere Aufbewahrung der Authentifizierungsinstrumente** (1) Der Teilnehmer/Nutzer hat • seine personalisierten Sicherheitsmerkmale (siehe Nummer 2.1) geheim zu halten ~~und nur über die von der Bank gesondert für das Firmenkundenportal mitgeteilten Zugangskanäle oder über von der Bank herausgegebene Apps zu übermitteln~~ 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. • Die personalisierten Sicherheitsmerkmale dürfen nicht außerhalb der gesondert vereinbarten Internetseiten eingegeben werden (z. B. nicht auf Online-Händlerseiten). • Die personalisierten Sicherheitsmerkmale dürfen nicht außerhalb des Firmenkundenportals weitergegeben werden, also beispielsweise nicht per E-Mail. • 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.	(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. • ~~Die personalisierten Sicherheitsmerkmale dürfen nicht außerhalb der gesondert vereinbarten Internetseiten eingegeben werden (z.B. nicht auf Online-Händlerseiten)~~ • ~~Die~~ Das personalisierte~~n~~ Sicherheitsmerkmal~~e dürfen nicht außerhalb des Firmenkundenportals weitergegeben werden, also beispielsweise per E-Mail.~~ 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.
10. Nutzungssperre 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 Auslands- und Transaktionsgeschäft 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 oder des personalisierten Sicherheitsmerkmals besteht.	**10. Nutzungssperre** **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 ~~Auslands- und Transaktionsgeschäft~~ Commerzbank Transaction Services 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 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 mittels Brief, postalischer Zusendung des Kontoauszuges oder – sofern der Kunde damit einverstanden ist – auf elektronischer Weise informieren.	(2) Die Bank wird den Kunden unter Angabe der hierfür maßgeblichen Gründe möglichst vor, spätestens jedoch unverzüglich nach der Sperre ~~mittels Brief, postalischer Zusendung des Kontoauszuges oder – sofern der Kunde damit einverstanden ist – auf elektronischer Weise informieren~~ in Textform (z.B. mittels Brief, Telefax oder E-Mail) oder telefonisch unterrichten. (3) *(neu)* Die Bank ist zudem berechtigt, einem Kontoinformationsdienstleister oder einem Kontoauslösedienstleister 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 Authentifizierungs-instrument austauschen, wenn die Gründe für die Sperre nicht mehr gegeben sind. Hierüber unterrichtet sie den Kunden mittels Brief, postalischer Zusendung des Kontoauszuges oder – sofern der Kunde damit einverstanden ist – auf elektronischer Weise unverzüglich.	**10.3 Aufhebung der Sperre** Die Bank wird eine Sperre aufheben oder das personalisierte Sicherheitsmerkmal beziehungsweise das Authentifizierungs-instrument austauschen, wenn die Gründe für die Sperre nicht mehr gegeben sind. Hierüber unterrichtet sie den Kunden ~~mittels Brief, postalischer Zusendung des Kontoauszuges oder – sofern der Kunde damit einverstanden ist – auf elektronischer Weise unverzüglich~~ in Textform (z.B. mittels Brief, Telefax oder E-Mail) oder telefonisch.
10.4 Automatische Sperre eines chip-basierten Authentifizierungsinstrument (1) Die Chipkarte mit Signaturfunktion wird gesperrt, wenn dreimal in Folge die Signatur-PIN/das Kennwort für die elektronische Signatur falsch eingegeben wurde. Eine Wiederfreischaltung bzw. Entsperrung der Chipkarte durch die Bank ist nicht möglich.	**10.4. Automatische Sperre ~~eines chip-basierten Authentifizierungsinstruments~~** (1) Die Chipkarte mit Signaturfunktion wird gesperrt, wenn dreimal in Folge ~~die Signatur-PIN/das Kennwort für die elektronische Signatur~~ der Nutzungscode falsch eingegeben wurde. Eine Wiederfreischaltung bzw. Entsperrung der Chipkarte durch die Bank ist nicht möglich.

(2) Die übermittelte Signatur wird gesperrt, wenn dreimal in Folge der Signatur-PIN/das Kennwort zur Freigabe der Signatur falsch eingegeben wurde. 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 übermittelte Signatur wird gesperrt, wenn dreimal in Folge der Signatur-PIN/das Kennwort zur Freigabe der Signatur falsch eingegeben wurde.~~ 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.
(3) Die PIN wird gesperrt, wenn dreimal in Folge die PIN falsch eingegeben wurde. Der TAN-Brief wird gesperrt, wenn dreimal in Folge eine TAN falsch eingegeben wurde.	~~(3)~~ (2) Die PIN wird gesperrt, wenn dreimal in Folge die PIN falsch eingegeben wurde. ~~Der TAN-Brief wird gesperrt, wenn dreimal in Folge eine TAN falsch eingegeben wurde.~~
(4) Der Teilnehmer/Nutzer wird für das photoTAN-Verfahren gesperrt, wenn fünfmal hintereinander die TAN falsch eingegeben wird.	~~(4)~~ (3) Der Teilnehmer/Nutzer wird für das photoTAN-Verfahren gesperrt, wenn fünfmal hintereinander die TAN falsch eingegeben wird.
(5) Der Teilnehmer/Nutzer kann sich mit der Bank in Verbindung setzen, um die Nutzungsmöglichkeiten des Firmenkunden-portals 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.	~~(5)~~ (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. 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. 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.
(3) Die Haftung für Schäden, die innerhalb des Zeitraums, für den das Standardlimit oder das mit dem Kunden für das Firmenkundenportal vereinbarte Verfügungslimit gilt, verursacht werden, beschränkt sich jeweils auf diese Limite.	(3) Die Haftung für Schäden, die innerhalb des Zeitraums, für den ~~das Standardlimit oder~~ das mit dem Kunden für das Firmenkundenportal vereinbarte Verfügungslimit gilt, verursacht werden, beschränkt sich jeweils auf dieses Limit~~e~~. (4) *(neu)* Die Absätze 2 und 3 finden keine Anwendung, wenn der Teilnehmer in betrügerischer Absicht gehandelt hat.
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 geltende Bankarbeitstage zu finden unter	**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. Telefonnummern und Geschäftszeiten werden in den Zugangswegen (z. B. https://www.firmenkunden.commerzbank.de/portal/) kommuniziert	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.firmenkunden.commerzbank.de/portal/~~ www.commerzbank.at) kommuniziert
16. Abbedingung von §§ 9, 10 ECG Die Vorschriften der §§ 9, 10 ECG (E-Commerce-Gesetz) finden keine Anwendung, sofern es sich bei dem Kunden nicht um einen Verbraucher handelt.	**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) ~~finden keine Anwendung, sofern es sich bei dem Kunden nicht um einen Verbraucher handelt~~ 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 Zahlungsvorgängen], § 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“.