Bedingungen für die Abwicklung von Bankgeschäften über das Firmenkundenportal

Gegenüberstellung der geänderten Bestimmungen

Fassung 2009	Fassung 2017
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 Wertpapierbedingungen, Sonderbedingungen für Wertpapiergeschäfte). Zudem kann er Informationen der Bank über das Firmenkundenportal abrufen. (2) Kunde und Bevollmächtigte werden im Folgenden einheitlich als "Teilnehmer" oder "User" bezeichnet Konto und Depot werden im Folgenden einheitlich als "Konto" bezeichnet	**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 Firmenkun-denportal abrufen. (2) Kunde und Bevollmächtigte werden im Fol-genden 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.
2. Voraussetzungen zur Nutzung des Firmenkundenportals Der Teilnehmer/ User benötigt für die Abwicklung von Bankgeschäften die mit der Bank vereinbarten, personalisierten Sicherheitsmerkmale und Authentifizierungsinstrumente, um sich gegenüber der Bank als berechtigter Teilnehmer/User auszuweisen (siehe Nummer 3) und Aufträge zu autorisieren (siehe Nummer 4). **2.1 Personalisierte Sicherheitsmerkmale** Personalisierte Sicherheitsmerkmale, die auch alphanumerisch sein können, sind: – die Persönliche Identifikationsnummer (PIN), – einmal verwendbare Transaktionsnummern (iTAN/TAN) und – die Signatur-PIN/das Kennwort und die Daten des persönlichen elektronischen Schlüssels für die elektronische Signatur. **2.2 Authentifizierungsinstrumente** Die TAN können dem Teilnehmer/User auf einer Liste mit einmal verwendbaren TAN zur Verfügung gestellt werden. Die Teilnehmer/User können weitere Authentifizierungsinstrumente zur Speicherung der elektronischen Signaturdaten nutzen:	**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. **2.2 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 Authentifzierungsinstrument, auf dem sich der Signaturschlüssel befindet.	– eine Chipkarte mit Signaturfunktion oder – ein sonstiges Authentifzierungsinstrument, 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.
3. Zugang zum Firmenkundenportal Der Teilnehmer/User 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/Users ergeben hat und – keine Sperre des Zugangs (siehe Nummern 9.1 und 10) vorliegt. Nach Gewährung des Zugangs zum Firmenkundenportal kann der Teilnehmer/User 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.
4. Auftragsabwickung 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 – iTAN – PIN – elektr. Unterschrift bzw. – nach Anmeldung mit Teilnehmernummer bzw. Anmeldenamen und PIN durch einfache Freigabe. **4.2 Einhaltung von Meldeverordnungen** Bei Zahlungen zugunsten Gebietsfremder ist vom Teilnehmer/User die Meldepflicht nach den auf § 6 Abs 2 und 3 Devisengesetz 2004 von der OeNB erlassenen Meldeverordnungen (derzeit „ZABIL 1/2009“ und „ZABIL 2/2009“, sowie die Verordnung betreffend statistische Erhebungen über die Importe und Exporte von Dienstleistungen und grenzüberschreitende Finanzbeziehungen) zu beachten.	**4. Auftragsabwickung 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. **4.2 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 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.
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/User hat sich mit seinem	**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 per-

personalisierten Sicherheitsmerkmal legitimiert. – Die Berechtigung des Teilnehmer/Users für die jeweilige Auftragsart liegt vor. (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/User über die Nichtausführung und soweit möglich, über deren Gründe und die Möglichkeiten, mit denen Fehler, die zur Ablehnung geführt haben, berichtigt werden können, online oder auf anderem Weg eine Information zur Verfügung stellen. Dies gilt nicht, wenn die Angabe von Gründen gegen sonstige Rechtsvorschriften verstößt. Führt die Bank den Auftrag aus, obwohl keine Kontodeckung vorhanden ist, entsteht eine geduldete Kontoüberziehung. für die ein erhöhter Zins zu zahlen ist.	sonalisierten Sicherheitsmerkmal legitimiert. – Die Berechtigung des Teilnehmer/Nutzers für die jeweilige Auftragsart liegt vor. *(Rest unverändert)* (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 erhöhter Zins zu zahlen ist.~~
7. Sorgfaltspflichten des Teilnehmers/Users **7.1 Technische Verbindung zum Firmenkundenportal** Der Teilnehmer/User 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 unterhält und stets nach dem Stand der Technik ausreichende Vorkehrungen gegen Viren und andere schädliche Programme (z. B. Trojaner, Würmer etc.) trifft. Der Kunde hat eigenverantwortlich die landesspezifischen Regelungen für die Nutzung des Internets zu beachten. **7.2 Geheimhaltung der personalisierten Sicherheitsmerkmale und sichere Aufbewahrung der Authentifizierungsinstrumente** (1) Der Teilnehmer/User hat • seine personalisierten Sicherheitsmerkmale (siehe Nummer 2.1) geheim zu halten und nur über die von der Bank gesondert für das Firmenkundenportal mitgeteilten Zugangskanäle 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. (2) Insbesondere ist Folgendes zum Schutz des personalisierten Sicherheitsmerkmals sowie des Authentifizierungsinstruments zu beachten:	**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 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 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 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. (2) Insbesondere ist Folgendes zum Schutz des personalisierten Sicherheitsmerkmals sowie des Authentifizierungsinstruments zu beachten:

- Die personalisierten Sicherheitsmerkmale PIN und iTAN sowie die Signatur-PIN/das Kennwort dürfen bei einem Teilnehmer/User nicht elektronisch gespeichert werden (z.B. im Kundensystem). Der vom Teilnehmer/User erzeugte persönliche elektronische Schlüssel darf sich nur in der alleinigen Verfügungsgewalt des Teilnehmers/Users befinden
- Wird im Rahmen einer vollautomatisierten Übertragung ein sog. "Technischer User" eingesetzt, ist die elektronisch gespeicherte Signatur in einer sicheren und entsprechend geeigneten technischen Umgebung zu speichern. Der "Technische User" 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/User darf zur Autorisierung eines Auftrags nicht mehr als eine iTAN verwenden. Zwei TANs zu einem Vorgang werden von der Bank nur im Rahmen der Aktivierung einer neuen TAN-Liste erfragt (letzte TAN des alten TAN-Briefs und erste TAN des neuen TAN- Briefs).

- 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.

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/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.
7.3 Kontrolle der Auftragsdaten mit von der Bank angezeigten Daten Soweit die Bank dem Teilnehmer/User Daten aus seinem über das Firmenkundenportal erteilten Auftrag (z. B. Betrag, Kontonummer des Zahlungsempfängers, Wertpapierkennnummer) im Kundensystem oder über ein anderes Gerät des Teilnehmers/Users (z. B. Chipkartenlesegerät mit Display) zur Bestätigung anzeigt, ist der Teilnehmer/User verpflichtet, vor der Bestätigung die Übereinstimmung der angezeigten Daten mit den für die Transaktion vorgesehenen Daten zu prüfen.	**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.
7.4 Weitere Sorgfaltspflichten des Kunden Der Kunde trägt dafür Sorge, dass die Sorgfaltspflichten aus diesem Vertrag auch von dem Bevollmächtigten (also von allen Teilnehmern/Usern) eingehalten werden.	**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.
9. Anzeige- und Unterrichtungspflichten **9.1 Sperranzeige** (1) Stellt der Teilnehmer/User • 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/User die Bank hierüber unverzüglich unterrichten (Sperranzeige). Der Teilnehmer/User kann der Bank eine Sperranzeige jederzeit auch über die gesondert mitgeteilte Sperrhotline abgeben. (2) Der Teilnehmer/User hat jeden Diebstahl oder Missbrauch unverzüglich bei der Polizei zur Anzeige zu bringen. (3) Hat der Teilnehmer/User 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. 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.
10. Nutzungssperre **10.1 Sperre auf Veranlassung des Teilnehmers/Users**	**10. Nutzungssperre** **10.1 Sperre auf Veranlassung des Teilnehmers/Nutzers**

Die Bank sperrt auf Veranlassung des Teilnehmers/Users, insbesondere im Fall der Sperranzeige nach Nummer 9.1, • den Zugang zum Firmenkundenportal für ihn und, falls der Teilnehmer/User dies verlangt, den Zugang für alle Teilnehmer/User des Kunden, oder • sein Authentifizierungsinstrument.	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/Nutzers dies verlangt, den Zugang für alle Teilnehmer/Nutzer des Kunden, oder • sein Authentifizierungsinstrument.
10.2 Sperre auf Veranlassung der Bank	**10.2 Sperre auf Veranlassung der Bank**
(1) Die Bank darf den Zugang zum Firmenkundenportal für einen Teilnehmer/User 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. (2) Die Bank wird den Kunden unter Angabe der hierfür maßgeblichen Gründe möglichst vor, spätestens jedoch unverzüglich nach der Sperre unterrichten.	(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. (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 elektronische Weise informieren.
10.3 Aufhebung der Sperre	**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 unverzüglich.	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 mittels Brief, postalischer Zusendung des Kontoauszuges oder – sofern der Kunde damit einverstanden ist – auf elektronische Weise unverzüglich.
10.4 Automatische Sperre eines chip-basierten Authentifizierungsinstrument	**10.4 Automatische Sperre eines chip-basierten Authentifizierungsinstrument**
(2) Die übermittelte Signatur wird gesperrt, wenn dreimal in Folge der Signatur-PIN/das Kennwort zur Freigabe der Signatur falsch eingegeben wurde. Der Teilnehmer/User 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) 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) Das im Absatz 1 genannte Authentifizierungsinstrument kann dann nicht mehr für das Firmenkundenportal genutzt werden. Der Teilnehmer/User 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 hierfür zu unterrichten, außer dies würde objektiven Sicherheitserwägungen oder gemeinschaftsrechtlichen oder innerstaatlichen Regelungen zuwiderlaufen oder gerichtliche oder verwaltungsbehördliche Anordnungen verletzen.	(4) ~~Das im Absatz 1 genannte Authentifizierungsinstrument kann dann nicht mehr für das Firmenkundenportal genutzt werden.~~ 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 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 abhanden gekommenen 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/User 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. (2) Der Kunde ist nicht zum Ersatz des Schadens nach den Absätzen 1 und 2 verpflichtet, wenn der Teilnehmer/User 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.	**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 abhanden gekommenen 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. (2) Der Kunde ist nicht zum Ersatz des Schadens nach den Absätzen 1 und 2 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.
11.2 Haftung bei nicht autorisierten Wertpapiertransaktionen oder bei anderen Servicearten vor	**11.2 Haftung bei nicht autorisierten Wertpapiertransaktionen oder bei anderen Servicearten vor der**

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/User 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/Users erhalten hat, übernimmt sie alle danach durch nicht autorisierte Verfügungen entstehenden Schäden. Dies gilt nicht, wenn der Teilnehmer/User in betrügerischer Absicht gehandelt hat.	**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 durch nicht autorisierte Verfügungen entstehenden Schäden. Dies gilt nicht, wenn der Teilnehmer/Nutzer in betrügerischer Absicht gehandelt hat.
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 User einen leichteren Zugriff auf das Informationsangebot im Internet zu ermöglichen. Die Inhalte der Seiten dieser Anbieter stellen nicht eigene Aussagen der Bank dar. Sie werden von der Bank auch nicht überprüft.	**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 einen leichteren Zugriff auf das Informationsangebot im Internet zu ermöglichen. Die Inhalte der Seiten dieser Anbieter stellen nicht eigene Aussagen der Bank dar. Sie werden von der Bank auch nicht überprüft.
15. Hotline ("Helpdesk") Die Bank bietet eine telefonische Hotline (sog. "Helpdesk") für die Bearbeitung von Fragen zu Technik, Bedienung und Funktionalitäten der im Firmenkundenportal angebotenen Services an. Die Bank besetzt die Hotline während der für das deutsche Bankgewerbe geltenden Bankarbeitstage. Telefonnummern und Geschäftszeiten werden in den Zugangswegen (z. B. firmenkundenportal.de/kontakt) kommuniziert.	**15. Hotline ("Helpdesk")** Die Bank bietet eine telefonische Hotline (sog. "Helpdesk") für die Bearbeitung von Fragen zu 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.
16. Abbedingung von §§ 9, 10 ECG	**16. Abbedingung von §§ 9, 10 ECG**

Die Vorschriften der §§ 9, 10 ECG (E-Commerce-Gesetz) werden hiermit abbedungen.	Die Vorschriften der §§ 9, 10 ECG (E-Commerce-Gesetz) finden keine Anwendung, sofern es sich bei dem Kunden nicht um einen Verbraucher handelt.
	17. Änderungsklausel Diese Bedingungen über für die Abwicklung von Bankgeschäften über das Firmenkundenportal (im Folgenden "Bedingungen") sind im Internet abrufbar unter https://www.firmenkunden.commerzbank.de/portal/. 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 Gegenüberstellung 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.