



Sonderbedingungen für das eBanking/Telefon-Banking

Stand: November 2011

1. Leistungsangebot

(1) Der Kontoinhaber kann Bankgeschäfte ausschließlich mittels Onlinebanking („eBanking“) oder Telefon-Banking („Telefon-Banking“) in dem von der Bank angebotenen Umfang abwickeln. Zudem kann er Informationen der Bank mittels eBanking abrufen bzw. mittels Telefon-Banking abfragen.

(2) Nutzungsberechtigter des eBanking/Telefon-Banking-Angebots der Bank ist ausschließlich der Kontoinhaber. Eine Berechtigung weiterer Personen, das eBanking/Telefon-Banking-Angebot anstelle des Kontoinhabers zu nutzen, ist nicht möglich.

2. Voraussetzungen zur Nutzung des eBanking

(1) Der Kontoinhaber benötigt für die Abwicklung von Bankgeschäften mittels eBanking die mit der Bank vereinbarten Personalisierten Sicherheitsmerkmale (GE NetKey, PIN, TAN) und Authentifizierungsinstrumente (mobilen Transaktionsnummern ("mobileTAN") und ein zum Empfang von mobileTAN registriertes Empfangsgerät, z.B. Mobiltelefon), um sich gegenüber der Bank als berechtigter Kontoinhaber auszuweisen (siehe Nummer 3 und 4) und Aufträge zu autorisieren (siehe Nummer 5).

(2) Für die Abwicklung von Bankgeschäften mittels eBanking sind die mit der Bank vereinbarten personalisierten Sicherheitsmerkmale und Authentifizierungsinstrument erforderlich, um sich gegenüber der Bank als berechtigter Kontoinhaber auszuweisen (siehe Nr. 3) und Aufträge zu autorisieren (siehe Nr. 4).

- Personalisierte Sicherheitsmerkmale sind der Benutzername, das persönliche Kennwort, die drei vom Kontoinhaber festzulegenden Sicherheitsfragen nebst Antworten für das Onlinebanking sowie die einmal verwendbaren mobileTAN.
- Als Authentifizierungsinstrument dient ein zum Empfang von mobileTAN per Textnachricht (SMS) geeignetes Empfangsgerät (z.B. Mobiltelefon).

(3) Für die Nutzung des eBanking benötigt der Kontoinhaber einen Internetzugang. Dieser wird nicht von der Bank bereitgestellt. Um das eBanking nutzen zu können, benötigt der Kontoinhaber zurzeit einen Browser, der eine 128-Bit-SSL-Verschlüsselung unterstützt. Die Bank behält sich vor, den Verschlüsselungsstandard und/oder die technischen Anforderungen jederzeit zu ändern, um die notwendige Sicherheit des eBanking zu gewährleisten. Über eine Änderung des Verschlüsselungsstandards und/oder der technischen Anforderungen wird die Bank den Kontoinhaber über sein elektronisches Postfach durch eine vorherige Mitteilung rechtzeitig informieren.

(4) Die sonstigen technischen Anforderungen auf Seiten des Kontoinhabers für die Nutzung des eBanking sind auf der Internetseite der Bank unter www.gecapitaldirekt.de beschrieben.





3. GE NetKey-Verfahren

(1) Für die Teilnahme am GE Netkey-Verfahren übersendet die Bank dem Kontoinhaber einen persönlichen GE NetKey, eine PIN, sowie über ein registriertes Empfangsgerät mobileTAN. Der Kontoinhaber muss seine persönliche PIN nach Erhalt von der Bank ändern.

(2) Bei der Abgabe von Willenserklärungen, Änderungen oder Überweisungen muss der Kontoinhaber neben seinem GE NetKey und seiner PIN jeweils eine mobileTAN eingeben.

(3) Die Willenserklärung des Kontoinhabers ist wirksam abgegeben, wenn er die in der Benutzerführung vorgeschriebene Freigabe zur Übermittlung vorgenommen hat. Bei Willenserklärungen, die die Eingabe einer TAN vorsehen, gilt die Willenserklärung mit Eingabe der mobileTAN als abgegeben.

4. mobileTAN-Verfahren

(1) Für die Teilnahme am mobileTAN-Verfahren ist ein Mobiltelefon mit einem Mobilfunk-Netzzugang eines deutschen Mobilfunk-Netzbetreibers erforderlich, das bei der Bank registriert wird. Mobiltelefone mit ausländischer Rufnummer können aus Sicherheitsgründen nicht verwendet werden.

Stellt der Kontoinhaber den Verlust dieses Mobiltelefons oder der SIM-Karte fest oder besteht der Verdacht einer missbräuchlichen Nutzung, ist er verpflichtet, die Bank unverzüglich hiervon zu benachrichtigen und das Mobiltelefon beim jeweiligen Mobilfunknetzbetreiber unverzüglich sperren zu lassen. Eventuelle Schäden, welche dem Kunden oder Bank durch unterlassenes Sperren entstehen, sind vom Kunden zu tragen; Ziffer 8 und 9 bleiben unberührt.

(2) Sofern eBanking-Vorgänge der Eingabe einer mobileTAN bedürfen, wird dem Kontoinhaber von der Bank auf Anforderung durch eine entsprechende Online-Anwendung für jede Transaktion eine Textmeldung (SMS) mit einer mobileTAN auf das registrierte Mobiltelefon übermittelt. Die in der SMS angegebene mobileTAN ist nur für die Transaktion gültig, für die sie angefordert wurde. Eine nicht genutzte mobileTAN verliert nach einer bestimmten Zeit nach deren Absendung durch die Bank ihre Gültigkeit.

5. eBanking-Aufträge

(1) Der Kontoinhaber muss eBanking-Aufträge (z. B. Überweisungen) zu deren Wirksamkeit gemäß dem GE NetKey-Verfahren (Nummer 3) oder dem mobileTAN-Verfahren (Nummer 4) autorisieren und der Bank mittels eBanking übermitteln. Die Bank bestätigt mittels eBanking den Eingang des Auftrags. Erklärungen, die keiner Autorisierung bedürfen, sind gegenüber der Bank wirksam abgegeben, wenn der Nutzungsberechtigte die in der Benutzerführung vorgeschriebene Freigabe zur Übermittlung an die Bank vorgenommen hat.

(2) Die Widerrufbarkeit eines eBanking-Auftrages richtet sich nach den für die jeweilige Auftragsart geltenden Sonderbedingungen (z. B. Sonderbedingungen für den Überweisungsverkehr). Der Widerruf von Aufträgen kann nur außerhalb des eBanking erfolgen, es sei denn, die Bank sieht eine Widerrufsmöglichkeit im eBanking ausdrücklich vor.



6. Bearbeitung der eBanking-Aufträge durch die Bank

(1) Die Bearbeitung der im Rahmen des eBankings erteilten Aufträge erfolgt nach den für die Abwicklung der jeweiligen Auftragsart (z. B. Überweisung) geltenden Regelungen, insbesondere den Ausführungsfristen gemäß Preis- und Leistungsverzeichnis. Aus Sicherheitsgründen ist die Bank berechtigt, eine Betragsobergrenze für Aufträge im eBanking festzusetzen.

(2) Zahlungsaufträge (Überweisung) führt die Bank unter folgenden Bedingungen aus:

- Der Kontoinhaber hat sich mit seinem personalisierten Sicherheitsmerkmal gemäß dem GE NetKey-Verfahren oder dem mobileTAN-Verfahren legitimiert.
- Das eBanking Datenformat ist eingehalten.
- Eine etwaige Betragsobergrenze für Aufträge im eBanking ist nicht überschritten.
- Es ist eine ausreichende Kontodeckung (ein ausreichendes Guthaben) vorhanden.

Liegen die vorstehenden Auszahlungsbedingungen vor, führt die Bank den eBanking-Auftrag nach Maßgabe der für die jeweilige Auftragsart geltenden Sonderbedingungen (z. B. Überweisungen) aus, sofern die Ausführung nicht gegen sonstige Rechtsvorschriften verstößt.

(3) Liegen die Ausführungsbedingungen nach Absatz 2 Satz 1 nicht vor, wird die Bank den eBanking-Auftrag nicht ausführen. Sie wird dem Kontoinhaber mittels eBanking eine Information über die Nichtausführung und – soweit möglich – über deren Gründe und die Möglichkeiten, mit denen Fehler, die zur Ablehnung geführt haben, berichtigt werden können, zur Verfügung stellen. Dies gilt nicht, wenn die Angabe von Gründen gegen sonstige Rechtsvorschriften verstößt.

7. Voraussetzungen zur Nutzung des Telefon-Banking

(1) Der Kontoinhaber benötigt für die Abwicklung von Bankgeschäften mittels Telefon-Banking die mit der Bank vereinbarten personalisierten Sicherheitsmerkmale (GE NetKey, Alias, Kunden- oder Kontonummer und PIN), um sich gegenüber der Bank als berechtigter Kontoinhaber auszuweisen.

(2) Für die Abwicklung von Bankgeschäften mittels Telefon-Banking wird der Kunde persönlich begrüßt, mittels GE NetKey, Alias, Kunden- oder Kontonummer vorlegitimiert und zur Eingabe der zugehörigen PIN in einen Sprachcomputer vermittelt. Die PIN muss zwingend numerisch sein und kann 5 bis 20 Stellen haben. Nach Eingabe der PIN wird der Kontoinhaber wieder mit dem Sachbearbeiter verbunden und kann legitimierungspflichtige Aufträge erteilen. Für die Eingabe von Aufträgen und Transaktionen ist keine Eingabe einer Transaktionsnummer (TAN) pro Geschäftsvorfall erforderlich.

(3) Für die Nutzung des Telefon-Banking benötigt der Kontoinhaber einen Telefon- oder Mobilfunkanschluss. Dieser wird nicht von der Bank bereitgestellt.

(4) Die mit dem Kontoinhaber geführten Gespräche werden – nach der Einwilligung durch den Kontoinhaber – aus Sicherheitsgründen aufgezeichnet. Die Sprachaufzeichnungen werden für 120 Tage gespeichert und danach gelöscht.



8. Sorgfaltspflichten des Kontoinhabers

(1) Der Kontoinhaber wird seine personalisierten Sicherheitsmerkmale (GE NetKey, PIN, TAN) geheim halten und nur über die von der Bank gesondert mitgeteilten eBanking/Telefon-Banking Zugangskanäle (z.B. Internetadresse, Telefonnummer) an diese übermitteln. Er wird sein Authentifizierungsinstrument (mobileTAN, mobiles Endgerät im mobileTAN-Verfahren bzw. GE NetKey, Alias, Kunden- oder Kontonummer und PIN) vor dem Zugriff anderer Personen sicher verwahren.

(2) Da jeder Dritte, der im Besitz des Authentifizierungsinstruments ist, in Verbindung mit dem dazugehörigen personalisierten Sicherheitsmerkmalen das eBanking/Telefon-Banking verfahrensmisbräuchlich nutzen kann, hat der Kontoinhaber insbesondere Folgendes zu beachten:

- Die personalisierten Sicherheitsmerkmale PIN und gegebenenfalls mobileTAN sowie der GE NetKey dürfen nicht elektronisch gespeichert werden (z.B. im Kundensystem).
- Bei Eingabe des personalisierten Sicherheitsmerkmals ist sicher zu stellen, dass andere Personen dies nicht ausspähen können.
- Die personalisierten Sicherheitsmerkmale dürfen nicht außerhalb der gesondert vereinbarten Internetseiten eingegeben bzw. bei anderen als den vereinbarten Telefon-Banking-Nummern mitgeteilt werden (z.B. nicht auf Online-Händlerseiten).
- Die personalisierten Sicherheitsmerkmale dürfen nicht außerhalb des eBanking/Telefon-Banking Verfahrens weiter gegeben werden, so beispielsweise nicht per E-Mail.
- Der GE NetKey, die PIN und gegebenenfalls mobileTAN dürfen nicht zusammen mit dem Authentifizierungsinstrument verwahrt werden.
- Der Kontoinhaber darf zur Autorisierung eines Auftrages beim eBanking nicht mehr als eine mobileTAN verwenden.
- Beim mobileTAN-Verfahren darf das Gerät, mit dem die mobileTAN empfangen werden (z.B. Mobiltelefon), nicht gleichzeitig für das eBanking genutzt werden.

(3) Der Kontoinhaber muss die Sicherheitshinweise auf der Internetseite der Bank unter www.gecapitaldirekt.de zum eBanking/Telefon-Banking, insbesondere die Maßnahmen zum Schutz der eingesetzten Hard- und Software, beachten. Hierzu gehören insbesondere die Installation und regelmäßige Aktualisierung einer handelsüblichen Antivirensoftware, die Installation einer Firewall sowie regelmäßige Sicherheits-Updates für den vom Kontoinhaber verwendeten Browser.

(4) Soweit die Bank dem Kontoinhaber Daten aus seinem eBanking-Auftrag (z.B. Betrag, Kontonummer des Zahlungsempfängers) im Kundensystem oder über ein anderes Gerät des Kontoinhabers (z.B. Mobiltelefon) zur Bestätigung anzeigt, ist der Kontoinhaber verpflichtet, vor der Autorisierung die Übereinstimmung der angezeigten Daten mit den für die Transaktion vorgesehenen Daten zu prüfen.



9. Anzeige- und Unterrichtungspflichten

(1) Stellt der Kontoinhaber den Verlust oder den Diebstahl des Authentifizierungsinstruments, die missbräuchliche Verwendung oder die sonstige nicht autorisierte Nutzung eines Authentifizierungsinstruments oder seines persönlichen Sicherheitsmerkmals fest, muss er die Bank hierüber unverzüglich unterrichten (Sperranzeige). Der Kontoinhaber kann der Bank eine Sperranzeige jederzeit auch über die auf der Internetseite der Bank unter www.gecapitaldirekt.de hierfür mitgeteilten Kontaktdaten abgeben.

(2) Der Kontoinhaber hat jeden Diebstahl oder Missbrauch unverzüglich bei der Polizei zur Anzeige zu bringen. Hat der Kontoinhaber 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. Der Kontoinhaber hat die Bank unverzüglich nach Feststellung eines nicht autorisierten oder fehlerhaft ausgeführten Auftrags hierüber zu unterrichten.

10. Sperren

(a) Sperre auf Veranlassung des Kontoinhabers

Die Bank sperrt auf Veranlassung des Kontoinhabers, insbesondere im Fall der Sperranzeige nach Nummer 9, seinen Online-Zugang und/oder sein Authentifizierungsinstrument. Diese Sperre kann per eBanking oder unter 01802 - 273 101 (EUR 0,06 / Anruf; Mobilfunkpreise können abweichen) veranlasst werden.

(b) Sperre auf Veranlassung der Bank

Die Bank darf den eBanking/Telefon-Banking Zugang für den Kontoinhaber sperren, wenn sie berechtigt ist, das Vertragsverhältnis 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 besteht. Die Bank wird den Kontoinhaber unter Angabe der hierfür maßgeblichen Gründe möglichst vor, spätestens jedoch unverzüglich nach der Sperre unterrichten, sofern nicht gesetzliche Vorschriften eine Unterrichtung verbieten.

(c) Aufhebung der Sperre

Die Bank wird die Sperre aufheben oder das personalisierte Sicherheitsmerkmal beziehungsweise das Authentifizierungsinstrument austauschen, wenn die Gründe für die Sperre nicht mehr gegeben sind. Hierüber unterrichtet sie den Kontoinhaber unverzüglich.

(d) Automatische Sperre des eBanking/Telefon-Banking Zugangs bei falscher Eingabe von PIN und mobileTAN

Wird dreimal hintereinander beim eBanking die falsche mobilePIN eingegeben, so sperrt die Bank den Online-Zugang zum Konto. Der Nutzer kann diese Sperre aufheben, indem er über die Service-Hotline unter 01802 - 273 101 (EUR 0,06 / Anruf; Mobilfunkpreise können abweichen) den Online-Zugang wieder freischalten lässt.



11. Haftung

(a) Haftung der Bank bei einer nicht autorisierten eBanking/Telefon-Banking Verfügung und einer nicht oder fehlerhaft ausgeführten eBanking/Telefon-Banking Verfügung

Die Haftung der Bank bei einer nicht autorisierten eBanking/Telefon-Banking Verfügung und einer nicht oder fehlerhaft ausgeführten eBanking/Telefon-Banking Verfügung richtet sich nach den für die jeweilige Ausführungsart vereinbarten Sonderbedingungen (z.B. Vereinbarungen über den Überweisungsverkehr).

(b) Haftung des Kontoinhabers für nicht autorisierte Zahlungsvorgänge vor der Sperranzeige

(1) Beruhen nicht autorisierte Zahlungsvorgänge vor der Sperranzeige auf der Nutzung eines verloren gegangenen, gestohlenen oder sonst abhanden gekommenen Authentifizierungsinstruments, haftet der Kontoinhaber für den Bank hierdurch entstehenden Schaden bis zu einem Betrag in Höhe von 150 EURO, ohne dass es darauf ankommt, ob den Kontoinhaber an dem Verlust, Diebstahl oder sonstigem Abhandenkommen des Authentifizierungsinstruments ein Verschulden trifft.

(2) Kommt es vor der Sperranzeige zu nicht autorisierten Zahlungsvorgängen aufgrund einer missbräuchlichen Verwendung des Authentifizierungsinstruments, ohne dass dieses verloren gegangen, gestohlen oder sonst abhanden gekommen ist, haftet der Kontoinhaber für den der Bank hierdurch entstehenden Schaden bis zu einem Betrag von 150 EURO, wenn der Kontoinhaber seine Pflicht zur sicheren Aufbewahrung der personalisierten Sicherheitsmerkmale schuldhaft verletzt hat.

(3) Der Kontoinhaber ist nicht zum Ersatz des Schadens nach den Absätzen (1) und (2) verpflichtet, wenn er die Sperranzeige nach Nummer 9 nicht abgeben konnte, weil die Bank nicht die Möglichkeit zur Entgegennahme der Sperranzeige sichergestellt hatte und der Schaden dadurch eingetreten ist.

(4) Kommt es vor der Sperranzeige zu nicht autorisierten Zahlungsvorgängen und hat der Kontoinhaber seine Sorgfaltspflichten nach diesen Bedingungen vorsätzlich oder grob fahrlässig verletzt oder in betrügerischer Absicht gehandelt, trägt der Kontoinhaber den hierdurch entstandenen Schaden in vollem Umfang. Grobe Fahrlässigkeit des Kontoinhabers kann insbesondere vorliegen, wenn er die Regelungen in Nummer 8 und 9 verletzt.

(c) Haftung der Bank ab der Sperranzeige

Sobald die Bank eine Sperranzeige eines Kontoinhabers erhalten hat, übernimmt sie alle danach über das eBanking/Telefon-Banking durch nicht autorisierte Verfügungen entstehenden Schäden. Dies gilt nicht, wenn der Kontoinhaber in betrügerischer Absicht gehandelt hat.

(d) Haftungsausschluss

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



12. Elektronische Postbox

(1) Im Rahmen der Geschäftsbeziehung zwischen der Bank und dem Kontoinhaber gilt die elektronische Postbox („Postbox“) als vereinbarter Kommunikationsweg. Über die Postbox übermittelt die Bank dem Kunden Mitteilungen, Kontoauszüge, Rechnungsabschlüsse und sonstige Informationen (zusammen „Dokumente“) zu gegenwärtigen und künftigen Konten in elektronischer Form.

(2) Dokumente gelten an dem Tag als zugegangen, an dem sie in die elektronische Postbox eingestellt werden. Der Kunde ist verpflichtet, regelmäßig, mindestens aber alle 30 Tage zu prüfen, ob neue Dokumente in seiner Postbox hinterlegt sind. Einwendungen gegen den Inhalt oder die Richtigkeit der in die Postbox übermittelten Dokumente wird der Kontoinhaber der Bank unverzüglich, spätestens jedoch innerhalb von sechs Wochen schriftlich mitteilen; Ziffer 7.2 der Allgemeinen Geschäftsbedingungen gilt entsprechend.

(3) Der Kunde hat über das Internet mit seinem GE NetKey und seiner PIN Zugriff auf die Postbox. In die Postbox eingestellte Dokumente kann der Kunde ansehen, ausdrucken und herunterladen.

(4) Der Kunde verzichtet ausdrücklich auf den postalischen Versand von Dokumenten. Die Bank ist jedoch berechtigt, dem Kunden Dokumente in Papierform auf dem Postwege zu übersenden, z. B. um gesetzliche Pflichten zu erfüllen oder wenn sie dies – auch unter Abwägung der Interessen des Kunden – für zweckmäßig erachtet. Insbesondere kann die Bank dem Kunden den Rechnungsabschluss per Post zusenden, wenn sie feststellt, dass der elektronische Abruf des Rechnungsabschlusses nach Ablauf von 30 Tagen seit der Einstellung in die elektronische Postbox nicht erfolgt ist; die Kosten hierfür können dem Kunden gemäß dem „Preis- und Leistungsverzeichnis“ in Rechnung gestellt werden.