

Sonderbedingungen für das Online-Banking

1. Leistungsangebot

1.1 Die GarantiBank und der Kontoinhaber vereinbaren, dass die Kontoführung sowie die Abwicklung von Bankgeschäften per Online-Banking mit elektronischem Postfach („ePostfach“) erfolgen.

1.2 Der Kontoinhaber und etwaige gesetzliche Vertreter („Teilnehmer“), können Bankgeschäfte mittels Online-Banking in dem von der GarantiBank angebotenen Umfang abwickeln. Zudem können Teilnehmer Informationen der GarantiBank mittels Online-Banking über das ePostfach abrufen (siehe Nummer 10). Darüber hinaus können Teilnehmer von ihnen ausgewählte sonstige Drittdienste nutzen.

2. Voraussetzungen für die Nutzung des Online-Banking

2.1 Teilnehmer können das Online-Banking nutzen, wenn die GarantiBank sie authentifiziert hat.

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

2.3 Authentifizierungselemente sind

- Wissenselemente, also etwas, das nur der Teilnehmer weiß (z. B. Passwort, persönliche Identifikationsnummer (PIN)),
- Besitzelemente, also etwas, das nur der Teilnehmer besitzt (z. B. mobiles Endgerät, das für den Empfang einer einmal verwendbaren Transaktionsnummer, der so genannten MobilTAN, durch den Kontoinhaber registriert ist) oder
- Seinselemente, also etwas, das der Teilnehmer ist (Inhärenz, z. B. Fingerabdruck als biometrisches Merkmal des Teilnehmers).

2.4 Die Authentifizierung des Teilnehmers erfolgt, indem der Teilnehmer gemäß den Anforderungen der GarantiBank das Wissenselement und/oder den Nachweis des Besitzelements und/oder den Nachweis des Seinselements an die GarantiBank übermittelt.

3. Zugang zum Online-Banking

Der Teilnehmer erhält Zugang zum Online-Banking der GarantiBank, wenn

- er seine individuellen Zugangsdaten (z.B. Kontonummer, PIN, Benutzername) angibt und
- er sich unter Verwendung des oder der von der GarantiBank angeforderten Authentifizierungselemente ausweist und
- keine Nutzungssperre vorliegt.

Nach Gewährung des Zugangs zum Online-Banking kann auf Informationen zugegriffen oder können Aufträge (siehe Nummer 4) erteilt werden.

4. Auftragserteilung

4.1 Der Teilnehmer muss einem über das Online-Banking erteilten Auftrag (z. B. eine Auszahlung) zu dessen Wirksamkeit zustimmen (Autorisierung). Auf Anforderung hat der Teilnehmer hierzu Authentifizierungselemente (z. B. die Eingabe einer MobilTAN) zu verwenden. Die GarantiBank bestätigt über das Online-Banking den Eingang des Auftrags.

4.2 Die Widerrufbarkeit eines Auftrags richtet sich nach den für die jeweilige Auftragsart geltenden Sonderbedingungen (z. B. Besondere Bedingungen für Kleeblatt-Sparkonto).

5. Bearbeitung von Aufträgen durch die GarantiBank

5.1 Die Bearbeitung der Aufträge erfolgt an den für die Abwicklung der jeweiligen Auftragsart (z. B. Überweisung, Festgeldaufträge, Freistellungsaufträge) auf der Online-Banking-Internetseite der GarantiBank oder im Preis-/Leistungsverzeichnis der GarantiBank bekannt gegebenen Geschäftstagen im Rahmen des ordnungsgemäßen Arbeitsablaufs. Geht der Auftrag nach dem auf der Online-Banking-Internetseite der GarantiBank oder im Preis-/Leistungsverzeichnis der GarantiBank angegebenen Zeitpunkt (Annahmefrist) ein oder fällt der Zeitpunkt des Eingangs nicht auf einen Geschäftstag gemäß Preis-/Leistungsverzeichnis, so gilt der Auftrag als am darauf folgenden Geschäftstag zugegangen. Die Bearbeitung beginnt erst an diesem Geschäftstag.

5.2 Die GarantiBank wird den Auftrag ausführen, wenn folgende Ausführungsbedingungen vorliegen:

- Der Teilnehmer hat den Auftrag autorisiert (vgl. Nummer 4 Absatz 1).
- Die Berechtigung des Teilnehmers für die jeweilige Auftragsart liegt vor.
- Das Internetbanking-Datenformat ist eingehalten.
- Die weiteren Ausführungsbedingungen nach den für die jeweilige Auftragsart maßgeblichen Sonderbedingungen (z. B. Auszahlungen vom Kleeblatt-Sparkonto nur zu Gunsten des hinterlegten Gegenkontos gemäß den Besondere Bedingungen für das Kleeblatt-Sparkonto) liegen vor.

Liegen die vorstehenden Ausführungsbedingungen vor, führt die GarantiBank die Aufträge nach Maßgabe der Bestimmungen der für die jeweilige Auftragsart geltenden Sonderbedingungen (z. B. Besonderen Bedingungen für das Kleeblatt-Sparkonto) aus.

5.3 Liegen die Ausführungsbedingungen nach Absatz 2 nicht vor, wird die GarantiBank den Auftrag nicht ausführen. Sie wird dem Teilnehmer mittels Internetbanking eine Information zur Verfügung stellen und soweit möglich dabei die Gründe und die Möglichkeiten nennen, mit denen Fehler, die zur Ablehnung geführt haben, berichtigt werden können.

6. Information des Kontoinhabers über Online-Banking-Verfügungen

6.1 Die GarantiBank unterrichtet den Kontoinhaber über die mittels Online-Banking getätigten Verfügungen auf dem für Kontoinformationen vereinbarten Weg. Inhalt und Häufigkeit der Kontoinformationen richten sich nach den für die jeweilige Auftragsart geltenden Sonderbedingungen.

6.2 Der Kontoinhaber hat die ihm im Online-Banking mitgeteilten Umsatzinformationen und Ausführungsdaten auf ihre Vollständigkeit und Richtigkeit zu überprüfen.

6.3 Der Kontoinhaber ist verpflichtet, sich unverzüglich nach Erteilung von Aufträgen von der Ausführung des Auftrags durch die GarantiBank zu vergewissern. Nicht autorisierte oder fehlerhaft ausgeführte Aufträge hat der Kontoinhaber der GarantiBank unverzüglich anzuzeigen.

7. Sorgfaltspflichten des Teilnehmers

7.1 Schutz der Authentifizierungselemente

(1) Der Teilnehmer hat alle zumutbaren Vorkehrungen zu treffen, um seine Authentifizierungselemente (siehe Nummer 2) vor unbefugtem Zugriff zu schützen. Ansonsten besteht die Gefahr, dass das Online-Banking missbräuchlich verwendet oder in sonstiger Weise nicht autorisiert genutzt wird (siehe Nummer 3 und Nummer 4).

(2) Zum Schutz der einzelnen Authentifizierungselemente hat der Teilnehmer vor allem Folgendes zu beachten:

(a) Wissenselemente, wie z. B. die PIN, sind geheim zu halten; sie dürfen insbesondere

- nicht mündlich (z. B. telefonisch oder persönlich) mitgeteilt werden,
- nicht außerhalb des Internetbanking in Textform (z. B. per E-Mail, Messenger-Dienst) weitergegeben werden,
- nicht ungesichert elektronisch gespeichert (z. B. Speicherung der PIN im Klartext im Computer oder mobilen Endgerät) werden und
- nicht auf einem Gerät notiert oder als Abschrift zusammen mit einem Gerät aufbewahrt werden, das als Besitzelement (z. B. mobiles Endgerät) oder zur Prüfung des Seinslements (z. B. mobiles Endgerät mit Fingerabdrucksensor) dient.

(b) Besitzelemente, wie z. B. ein mobiles Endgerät, sind vor Missbrauch zu schützen, insbesondere

- ist das mobile Endgerät vor dem unbefugten Zugriff anderer Personen sicher zu verwahren,
- ist sicherzustellen, dass unberechtigte Personen auf das mobile Endgerät des Teilnehmers nicht zugreifen können,
- dürfen die Nachweise des Besitzelements (z. B. MobilTAN) nicht außerhalb des Online-Banking mündlich (z. B. per Telefon) oder in Textform (z. B. per E-Mail, Messenger-Dienst) weitergegeben werden und
- hat der Teilnehmer von der GarantiBank einen Code zur Aktivierung des Besitzelements erhalten, muss er diesen vor dem unbefugten Zugriff anderer Personen sicher verwahren.

(c) Seinslemente, wie z. B. der Fingerabdruck des Teilnehmers, dürfen auf einem mobilen Endgerät des Teilnehmers für das Internetbanking nur dann als Authentifizierungselement verwendet werden, wenn auf dem mobilen Endgerät keine Seinslemente anderer Personen gespeichert sind. Sind auf dem mobilen Endgerät, das für das Internetbanking genutzt wird, Seinslemente anderer Personen gespeichert, ist für das Internetbanking das von der GarantiBank ausgegebene Wissenselement (z. B. PIN) zu nutzen und nicht das auf dem mobilen Endgerät gespeicherte Seinslement (z. B. Fingerabdruck).

(3) Ungeachtet der Schutzpflichten nach den Absätzen 1 bis 2 darf der Teilnehmer seine Authentifizierungselemente gegenüber einem von ihm ausgewählten sonstigen Drittdienst verwenden (siehe Nummer 1.2). Sonstige Drittdienste hat der Kunde mit der im Verkehr erforderlichen Sorgfalt auszuwählen.

7.2 Sicherheitshinweise der GarantiBank

Der Teilnehmer muss die Sicherheitshinweise zum Online-Banking auf der Internetseite der GarantiBank, insbesondere auch die Maßnahmen zum Schutz der von ihm eingesetzten Hard- und Software (Kundensystem), beachten. Der Kontoinhaber ist verpflichtet, die technische Verbindung zum Online-Banking nur über die von der Bank gesondert mitgeteilten Online-Banking-Zugangskanäle (z. B. Internetadresse) herzustellen.

7.3 Prüfung der Auftragsdaten mit von der GarantiBank angezeigten Daten

Die GarantiBank zeigt dem Teilnehmer die von ihr von dem Teilnehmer empfangenen Auftragsdaten (z. B. Betrag, IBAN) an. Der Teilnehmer ist verpflichtet, vor der Bestätigung die Übereinstimmung der angezeigten Daten mit den für den Auftrag vorgesehenen Daten zu prüfen.

7.4 Allgemeine Sorgfaltspflichten des Teilnehmers

Der Teilnehmer hat die ihm während des Online-Bankings angezeigten Verfahrens- und Benutzungshinweise zu beachten und alle von ihm eingegebenen oder die von einer Anwendung ermittelten und ausgelesenen Daten auf Vollständigkeit und Richtigkeit zu überprüfen. Aufträge jeder Art müssen ihren Inhalt zweifelsfrei erkennen lassen. Nicht eindeutig formulierte Aufträge und insbesondere nicht oder nicht richtig ausgefüllte Felder können Rückfragen und Missverständnisse zur Folge haben, die zu Verzögerungen der Ausführung führen können. Die GarantiBank überprüft nicht die formale und inhaltliche Richtigkeit der erteilten Aufträge.

8. Anzeige und Unterrichtungspflichten

8.1 Sperranzeige

(1) Stellt der Teilnehmer

- den Verlust oder den Diebstahl eines Besitzelements zur Authentifizierung (z. B. mobiles Endgerät) oder
- die missbräuchliche Verwendung oder die sonstige nicht autorisierte Nutzung eines Authentifizierungselements fest, oder hat er einen entsprechenden Verdacht, muss der Teilnehmer die GarantiBank hierüber unverzüglich unterrichten (Sperranzeige).

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

(3) Das für die Nutzung des GarantiBank-Online-Banking registrierte mobile Endgerät ist im GarantiBank-Online-Banking zu löschen oder ändern, wenn der Teilnehmer das mobile Endgerät nicht mehr nutzt oder die Telefonnummer ändert.

8.2 Unterrichtung über nicht autorisierte oder fehlerhaft ausgeführte Aufträge

Der Kunde hat die GarantiBank unverzüglich nach Feststellung eines nicht autorisierten oder fehlerhaft ausgeführten Auftrags hierüber zu unterrichten.

9. Nutzungssperre

9.1 Sperre auf Veranlassung des Teilnehmers

Die GarantiBank sperrt auf Veranlassung des Teilnehmers, insbesondere im Fall der Sperranzeige nach Nummer 8.1

- den Online-Banking-Zugang für ihn oder alle Teilnehmer oder
- seine Authentifizierungselemente zur Nutzung des Online-Banking.

9.2 Sperre auf Veranlassung der GarantiBank

(1) Die GarantiBank darf den Online-Banking-Zugang für einen Teilnehmer sperren, wenn

- sie berechtigt ist, den Online-Banking-Vertrag aus wichtigem Grund zu kündigen,
- sachliche Gründe im Zusammenhang mit der Sicherheit der Authentifizierungselemente des Teilnehmers dies rechtfertigen oder
- der Verdacht einer nicht autorisierten oder einer betrügerischen Verwendung des Authentifizierungselements besteht.

(2) Die GarantiBank wird den Kunden unter Angabe der hierfür maßgeblichen Gründe möglichst vor, spätestens jedoch unverzüglich nach der Sperre auf dem vereinbarten Weg unterrichten. Die Angabe von Gründen darf unterbleiben, soweit die GarantiBank hierdurch gegen gesetzliche Verpflichtungen verstoßen würde.

9.3 Aufhebung der Sperre

Die GarantiBank wird eine Sperre aufheben oder die betroffenen Authentifizierungselemente austauschen, wenn die Gründe für die Sperre nicht mehr gegeben sind. Hierüber unterrichtet sie den Kunden unverzüglich.

9.4 Zugangssperre für sonstige Drittdienste

Die GarantiBank kann sonstigen Drittdiensten den Zugang zu einem Konto des Kunden verweigern, wenn objektive und gebührend nachgewiesene Gründe im Zusammenhang mit einem nicht autorisierten oder betrügerischen Zugang des sonstigen Drittdienstes zum Konto es rechtfertigen. Die GarantiBank wird den Kunden über eine solche Zugangsverweigerung auf dem vereinbarten Weg unterrichten. Die Unterrichtung erfolgt möglichst vor, spätestens jedoch unverzüglich nach der Verweigerung des Zugangs. Die Angabe von Gründen darf unterbleiben, soweit die GarantiBank hierdurch gegen gesetzliche Verpflichtungen verstoßen würde. Sobald die Gründe für die Verweigerung des Zugangs nicht mehr bestehen, hebt die GarantiBank die Zugangssperre auf. Hierüber unterrichtet sie den Kunden unverzüglich.

10. ePostfach

10.1 Mit Vereinbarung der Nutzung von GarantiBank Online-Banking richtet die GarantiBank dem Nutzer ein elektronisches Postfach („ePostfach“) ein. Mit der Einrichtung des ePostfach verzichtet der Nutzer nach Maßgabe dieser Bedingungen auf den postalischen Versand der eingestellten Informationen. Die GarantiBank ist jedoch berechtigt, die eingestellten Informationen weiterhin postalisch oder auf andere Weise dem Nutzer zuzusenden, wenn dies gesetzliche Vorgaben erforderlich machen oder es aufgrund anderer Umstände (z. B. des vorübergehenden Ausfalls des ePostfach) zweckmäßig ist.

10.2 In das ePostfach werden für den Nutzer bestimmte persönliche Informationen der GarantiBank online eingestellt. Soweit die GarantiBank die betreffenden Informationen nicht nur zum Abruf durch den Nutzer bereitstellt (z. B. Kontoauszüge), sondern zur Mitteilung verpflichtet ist, wird sie den Nutzer zusätzlich per Nachricht an die hinterlegte E-Mail-Adresse oder auf sonstige Weise auf die Einstellung der Informationen in das ePostfach hinweisen. Der Kontoinhaber ist zu diesem Zweck verpflichtet, der GarantiBank eine E-Mail-Adresse mitzuteilen und auf dem aktuellen Stand zu halten, die er üblicherweise für die Kommunikation mit Dritten verwendet. Der Nutzer kann sich die Informationen online ansehen, diese herunterladen, ausdrucken und archivieren. Die Nutzung ist ausschließlich dem Nutzer vorbehalten.

10.3 Wenn Kontoumsätze vorliegen, werden dem Nutzer einmal im Quartal Kontoauszüge bereitgestellt. Etwas anderes gilt nur, wenn vertraglich mit dem Nutzer abweichende Vereinbarungen getroffen wurden. Im Zeitraum zwischen zwei Kontoauszügen kann der Nutzer seine Kontobewegungen durch eine Umsatzabfrage im Online-Banking einsehen.

10.4 Der Nutzer ist verpflichtet, die eingestellten Informationen zeitnah abzurufen und sie unverzüglich auf ihre Richtigkeit zu überprüfen. Etwaige Einwendungen sind unverzüglich über das GarantiBank-Online-Banking zu erheben.

10.5 Die GarantiBank stellt die Unveränderbarkeit der in das ePostfach eingestellten Dokumente sicher, sofern diese innerhalb des ePostfachs gespeichert oder aufbewahrt werden.

10.6 Die in das ePostfach eingestellten Informationen stehen während der dort angezeigten Dauer zur Verfügung. Danach erfolgt eine automatische Löschung der Informationen ohne gesonderte Nachricht. Die GarantiBank ist innerhalb der gesetzlichen Aufbewahrungsfristen jederzeit in der Lage, dem Nutzer auf dessen Anforderung eine papierhafte Ausfertigung dieser Informationen zur Verfügung zu stellen. Nach Beendigung der Konto- und Depotbeziehung kann der Nutzer die im ePostfach gespeicherten Dokumente nicht mehr online ansehen.

11. Haftung

11.1 Haftung der GarantiBank bei einer nicht autorisierten Online-Banking-Verfügung und einer nicht oder fehlerhaft ausgeführten Online-Banking-Verfügung

Die Haftung der GarantiBank bei einer nicht autorisierten Online-Banking-Verfügung und einer nicht oder fehlerhaft ausgeführten Online-Banking Verfügung richtet sich nach den für die jeweilige Auftragsart

vereinbarten Sonderbedingungen (z.B. Besondere Bedingungen für Kleeblatt-Festgeldanlagen, Besondere Bedingungen für das Kleeblatt-Sparkonto).

11.2. Haftung des Kontoinhabers bei missbräuchlicher Nutzung seines Authentifizierungs-instruments

11.2.1 Haftung des Kontoinhabers für nicht autorisierte Zahlungsvorgänge vor der Sperranzeige

(1) Beruhen nicht autorisierte Zahlungsvorgänge vor der Sperranzeige auf der Nutzung eines verlorengegangenen, gestohlenen oder sonst abhanden gekommenen Authentifizierungselements oder auf der sonstigen missbräuchlichen Verwendung eines Authentifizierungselements, haftet der Kontoinhaber für den der GarantiBank hierdurch entstehenden Schaden bis zu einem Betrag von 50,00 Euro, ohne dass es darauf ankommt, ob den Teilnehmer ein Verschulden trifft.

(2) Kommt es vor der Sperranzeige zu nicht autorisierten Zahlungsvorgängen und hat der Kontoinhaber in betrügerischer Absicht gehandelt oder seine Sorgfalts- und Anzeigepflichten nach diesen Vereinbarungen vorsätzlich oder groß fahrlässig verletzt, trägt er abweichend von 11.2.1. (1) den hierdurch entstandenen Schaden in vollem Umfang. Grobe Fahrlässigkeit des Kontoinhabers kann insbesondere vorliegen, wenn er seine Sorgfaltspflichten nach Nummer 7.1 (2), Nummer 7.3 oder Nummer 8.1 (1) verletzt hat.

11.2.2 Haftung ab der Sperranzeige

Sobald die GarantiBank eine Sperranzeige eines Teilnehmers erhalten hat, übernimmt sie alle danach durch nicht autorisierte Onlinebanking-Verfügungen entstehenden Schäden. Dies gilt nicht, wenn der Teilnehmer in betrügerischer Absicht gehandelt hat.

11.2.3 Haftungsausschluss

(1) Kann das Online-Banking aufgrund technischer oder sonstiger Störungen vorübergehend nicht durchgeführt werden, haftet die GarantiBank nur im Fall eines von ihr zu vertretenden Verschuldens und nur in dem Maße, in dem sie im Verhältnis zu anderen Ursachen an der Entstehung des Schadens mitgewirkt hat. Der Nutzer ist verpflichtet, Störungen bei der Übertragung von Daten der GarantiBank unverzüglich mitzuteilen.

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

Stand: 12.10.2020. Alle Angaben gelten bis auf Weiteres.