Sonderbedingungen für das Online- und Mobile-Banking

1. Leistungsangebot
1.1 Kontoführung und ePostfach

Die GarantiBank und der oder die Kontoinhaber:in vereinbaren, dass die Kontoführung sowie die Abwicklung von Bankgeschäften auch per Online- oder Mobile-Banking über die Garanti App mit elektronischem Postfach (ePostfach) erfolgen kann. Voraussetzung hierfür ist, dass ein Kleeblatt-Sparkonto im Namen der Kontoinhaberin oder des Kontoinhabers geführt wird.

1.2 Abwicklung von Bankgeschäften

Der oder die Kontoinhaber:in und etwaige gesetzliche Vertreter:innen (zusammen Teilnehmer:in), können Bankgeschäfte mittels Online- oder Mobile-Banking in dem von der GarantiBank angebotenen Umfang abwickeln. Zudem können Teilnehmer:innen Informationen der GarantiBank mittels Online- oder Mobile-Banking über das ePostfach abrufen (siehe Nummer 10). Darüber hinaus können Teilnehmer:innen von ihnen ausgewählte sonstige Drittdienste nutzen. Andere bevollmächtigte Personen, die nicht gesetzliche Vertreter sind, sind keine Teilnehmer:innen im Sinne dieser Sonderbedingungen und können Bankgeschäfte nicht mittels Online- oder Mobile-Banking abwickeln.

1.3 Verhältnis zu anderen Bedingungen der GarantiBank

Die Sonderbedingungen für das Online- und Mobile Banking stehen im Zusammenhang mit den allgemeinen Geschäftsbedingungen und den Sonderbedingungen für das Kleeblatt-Sparkonto sowie etwaigen Sonderbedingungen für die einzelnen angebotenen Anlageprodukte.

2. Voraussetzungen für die Nutzung des Online-Banking
2.1 Notwendigkeit der Authentifizierung

Teilnehmer:innen können das Online- und Mobile-Banking Angebot nutzen, wenn die GarantiBank sie authentifiziert hat.

2.2 Authentifizierung

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

2.3 Authentifizierungselemente

Authentifizierungselemente sind
- Wissenselemente, also etwas, das nur der oder die Teilnehmer:in weiß (z. B. Passwort, persönliche Identifikationsnummer (PIN));
- Besitzelemente, also etwas, das nur der oder die Teilnehmer:in besitzt (z. B. mobiles Endgerät, das für den Empfang einer einmal verwendbaren Transaktionsnummer, der so genannten MobilTAN, durch den oder die Teilnehmer:in registriert ist);
- Seinselemente, also etwas, das der oder die Teilnehmer:in ist (Inhärenz, z. B. Fingerabdruck als biometrisches Merkmal des Teilnehmers oder der Teilnehmerin); oder
- Scan eines QR-Codes im Online-Banking Bereich mit der GarantiBank App.

2.4 Erfolgreiche Authentifizierung

Die Authentifizierung des Teilnehmers oder der Teilnehmerin erfolgt, indem der oder die Teilnehmer:in gemäß den gesetzlichen Anforderungen zwei voneinander unabhängige Authentifizierungselemente aus den vorgenannten Kategorien Wissen, Besitz und Sein verwendet.

2.5 Benötigte Soft- und Hardware

Je nach Authentifizierungsverfahren und -instrument benötigt der oder die Teilnehmer:in hierfür gegebenenfalls geeignete Hard- und Software. Über das Angebot der bankeigenen Anwendungen hinaus bleibt der oder die Teilnehmer:in selbst für die Beschaffung, Installation und Pflege dieser Hard- und Software verantwortlich.

2.6 Unterstützte Betriebssysteme und Endgeräte

Auf der Website der Garantibank können die jeweils derzeit unterstützten Betriebssysteme und Geräte eingesehen werden.

3. Zugang zum Online- und Mobile-Banking

3.1 Beantragung des Zugangs zum Online-Banking

Bei Eröffnung eines neuen Kleeblatt-Sparkontos über die Website der GarantiBank wird das Konto des oder der Teilnehmer:in automatisch für das Online-Banking registriert, sofern der oder die Teilnehmer:in nicht widerspricht. Darüber hinaus können die Teilnehmer:innen von bestehenden Kleeblatt-Sparkonten einen Zugang zum Online-Banking beantragen.

3.2 Erhalt der Zugangsdaten für das Online-Banking

Nach der Kontoeröffnung oder der Antragstellung erhält der oder die Teilnehmer:in seinen bzw. ihren Benutzernamen über den Postweg an die bei der Bank hinterlegte Adresse oder per E-Mail an die hinterlegte E-Mail-Adresse. Gleichzeitig erhält er oder sie über die hinterlegte E-Mail-Adresse eine E-Mail zur Aktivierung des Online-Bankings und zur Festlegung eines individuellen Passwortes. Die oder der Teilnehmer:in benötigt des Weiteren ein mobiles Endgerät mit Mobilfunk, für den Erhalt einer SMS-TAN, durch die die jeweilige Anmeldung verifiziert wird.

3.3 Zugang zum Mobile-Banking

3.3.1 Für den Zugang zum Mobile-Banking müssen der oder die Teilnehmer:in die Zugangsdaten für das Online-Banking erhalten und das Online-Banking aktiviert haben (siehe Nummer 3.2). Mit diesen Zugangsdaten können sich der oder die Teilnehmer:in in der App der GarantiBank anmelden. Für die Erstanmeldung auf einem mobilen Endgerät wird die Verifizierung via SMS-Tan verlangt, so dass der oder die Teilnehmer:in über ein mobiles Endgerät mit Mobilfunk verfügen muss, um Zugang zum Mobile-Banking zu erhalten.

3.3.2 Der oder die Teilnehmer:in kann die GarantiBank App nur auf einem registrierten Gerät nutzen. Meldet sich der oder die Teilnehmer:in auf einem neuen Gerät an, so kann die App auf dem alten Gerät nicht mehr genutzt werden, bis eine erneute Anmeldung erfolgt.

3.4 Zugangsvoraussetzungen

Der oder die Teilnehmer:in erhält Zugang zum Online- und Mobile-Banking der GarantiBank, wenn

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

Diese Voraussetzungen gelten sowohl für das Online- als auch für das Mobile-Banking. Nach Gewährung des Zugangs zum Online- und Mobile-Banking kann auf Informationen zugegriffen oder können Aufträge (siehe Nummer 4) erteilt werden.

4. Autorisierung und Auftragserteilung

4.1 Voraussetzungen für die Autorisierung

Der oder die Teilnehmer:in muss einem über das Online- oder Mobile-Banking erteilten Auftrag (z. B. einer Auszahlung) für dessen Wirksamkeit zustimmen (Autorisierung). Auf Aufforderung hat der oder die Teilnehmer:in hierzu Authentifizierungselemente (z. B. die Eingabe einer MobilTAN) zu verwenden, um seine oder ihre Zustimmung zu erteilen.

4.2 Widerrufbarkeit von Aufträgen

Die Widerrufbarkeit eines Auftrags richtet sich nach den gesetzlichen Vorschriften und den für die jeweilige Auftragsart geltenden Sonderbedingungen (z. B. Besondere Bedingungen für Kleeblatt-Sparkonto). Der Widerruf von Aufträgen kann nur außerhalb des Online-Banking erfolgen, es sei denn, die GarantiBank sieht eine Widerrufsmöglichkeit im Online-Banking ausdrücklich vor.

5. Bearbeitung von Aufträgen durch die GarantiBank
5.1 Bearbeitung von Aufträgen

Die Bearbeitung der Aufträge erfolgt innerhalb der 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. Diese Informationen sind für das Mobile-Banking auch in der App einsehbar. 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 Ausführungsbedingungen

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

- Der oder die Teilnehmer:in hat den Auftrag autorisiert (vgl. Nummer 4 Absatz 1).
- Die Berechtigung des Teilnehmers oder der Teilnehmerin für die jeweilige Auftragsart liegt vor.
- Das Online-Banking-Datenformat ist eingehalten.
- Das gesondert vereinbarte Online-Banking-Verfügungslimit ist nicht überschritten.
- 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) müssen erfüllt sein.

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

5.3 Nichtvorliegen der Ausführungsbedingungen

Sind die Ausführungsbedingungen nach Absatz 2 nicht erfüllt, wird die GarantiBank den Auftrag nicht ausführen. Sie wird dem Teilnehmer oder der Teilnehmerin mittels Online-Banking bzw. dem ePostfach 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 Teilnehmers oder der Teilnehmerin über Online- und Mobile-Banking Aufträgen
6.1 Unterrichtung durch die GarantiBank über getätigte Aufträge durch den oder die Teilnehmer:in

Die GarantiBank unterrichtet den oder die Teilnehmer:in über die mittels Online- und Mobile-Banking getätigten Aufträge auf dem für Kontoinformationen vereinbarten Weg. Inhalt und Häufigkeit der Informationen richten sich nach den für die jeweilige Auftragsart geltenden Sonderbedingungen. Wählt der oder die Teilnehmer:in die ausschließliche Online-Kontoführung, so wird die Bank die Kontoauszüge online – d.h. über das Medium Internet (im .pdf-Format) – zur Verfügung stellen. Online-Kontoauszüge stehen jeweils 24 Monate ab Kontoauszugerstellung zur Ansicht, zum Speichern und zum Ausdrucken zur Verfügung. Danach können der oder die Teilnehmer:in die jeweiligen Kontoauszüge postalisch erhalten, wofür möglicherweise ein Entgelt nach dem Preis-/Leistungsverzeichnis anfällt. Greift der oder die Teilnehmer:in auf das Online-Postfach, in welchem die Kontoauszüge bereitgestellt sind, länger als 90 Tage nicht zu, ist die Bank berechtigt, die Kontoauszüge in Papierform zu erstellen und dem oder der Teilnehmer:in auf dem Postweg gegen Auslagenersatz zuzusenden.

6.2 Prüfung der Ausführungsdaten durch den oder die Teilnehmer:in

Die GarantiBank zeigt dem oder der Teilnehmer:in die von ihr empfangenen Auftragsdaten (z. B. Betrag, Kontonummer des Zahlungsempfängers, Wertpapierkennnummer) über das mobile Endgerät des Teilnehmers oder der Teilnehmerin an. Der oder die Teilnehmer:in ist verpflichtet, vor der Bestätigung die Übereinstimmung der angezeigten Daten mit den für den Auftrag vorgesehenen Daten zu prüfen.

6.3 Anzeigepflicht des Teilnehmers oder der Teilnehmerin in Fällen nicht autorisierter oder fehlerhaft ausgeführter Aufträge

Der oder die Teilnehmer:in 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 oder die Teilnehmer:in der GarantiBank unverzüglich anzuzeigen.

7. Sorgfaltspflichten des Teilnehmers oder der Teilnehmerin
7.1 Schutz der Authentifizierungselemente

(1) Der oder die Teilnehmer:in hat alle zumutbaren Vorkehrungen zu treffen, um seine oder ihre Authentifizierungselemente (siehe Nummer 2) vor unbefugtem Zugriff zu schützen. Ansonsten besteht die Gefahr, dass das Online- und Mobile-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 oder die Teilnehmer:in 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 Online- oder Mobile-Banking 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 Seinselements (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 oder der Teilnehmerin nicht zugreifen können,
- ist dafür Sorge zu tragen, dass andere Personen die auf dem mobilen Endgerät (z. B. Mobiltelefon) befindliche Anwendung für das Online Banking (z.B. Online-Banking-App) nicht nutzen können,
- ist die Anwendung für das Online-Banking (z.B. Online-Banking-App) auf dem mobilen Endgerät des Teilnehmers oder der Teilnehmerin zu deaktivieren, bevor der oder die Teilnehmer:in den Besitz an diesem mobilen Endgerät aufgibt (z.B. durch Verkauf des Mobiltelefons),
- 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 oder die Teilnehmer:in von der GarantiBank einen Code zur Aktivierung des Besitzelements erhalten, muss er diesen vor dem unbefugten Zugriff anderer Personen sicher verwahren.

(c) Seinselemente, wie z. B. der Fingerabdruck des Teilnehmers oder der Teilnehmerin, dürfen auf einem mobilen Endgerät des Teilnehmers oder der Teilnehmerin für das Online- und Mobile-Banking nur dann als Authentifizierungselement verwendet werden, wenn auf dem mobilen Endgerät keine Seinselemente anderer Personen gespeichert sind. Sind auf dem mobilen Endgerät, das für das Internetbanking genutzt wird, Seinselemente 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 Seinselement (z. B. Fingerabdruck).

(3) Ungeachtet der Schutzpflichten nach den Absätzen 1 und 2 darf der oder die Teilnehmer:in seine oder ihre Authentifizierungselemente gegenüber einem von ihm ausgewählten sonstigen Drittdienst (z.B. Zahlungsauslösedienst oder Kontoinformationsdienst) verwenden (siehe Nummer 1.2). Sonstige Drittdienste hat der oder die Teilnehmer:in mit der im Verkehr erforderlichen Sorgfalt auszuwählen.

(4) Der Aufforderung per elektronischer Nachricht (z. B. E-Mail), eine damit übersandte Verknüpfung zum (vermeintlichen) Online-Banking der Bank anzuwählen und darüber persönliche Zugangsdaten einzugeben, darf nicht gefolgt werden.

(5) Anfragen außerhalb der bankseitig zur Verfügung gestellten originären Zugangswege, in denen nach vertraulichen Daten wie PIN, Geheimzahl oder Passwort/TAN gefragt wird, dürfen nicht beantwortet werden.

(8) Der oder die Teilnehmer:in hat vor seinem oder ihrem jeweiligen Zugang zum Online-Banking sicherzustellen, dass auf dem verwendeten System handelsübliche Sicherheitsvorkehrungen (wie Anti-Viren-Programm und Firewall) installiert sind und diese ebenso wie die verwendete System- und Anwendungssoftware regelmäßig aktualisiert werden. Beispiele handelsüblicher Sicherheitsvorkehrungen kann der oder die Teilnehmer:in den Internetseiten der Bank entnehmen.

(9) Die Softwareanwendungen der Bank sind ausschließlich direkt von der Bank oder von einem von der Bank benannten Anbieter zu beziehen.

7.2 Sicherheitshinweise der GarantiBank

Der oder die Teilnehmer:in muss die Sicherheitshinweise zum Online- und Mobile-Banking auf der Internetseite der GarantiBank, insbesondere auch die Maßnahmen zum Schutz der von ihm oder ihr eingesetzten Hard- und Software (Kundensystem) beachten. Der oder die Teilnehmer:in ist verpflichtet, die technische Verbindung zum Online- und Mobile Banking nur über die von der Bank gesondert mitgeteilten Online- und Mobile-Banking- Zugangskanäle (z. B. Internetadresse, offizielle App) herzustellen. Der oder die Teilnehmer:in hat in eigener Verantwortung etwaige Sicherheitshinweise der Anbieter der eingesetzten Kundensysteme zu beachten (z. B. Sicherheitsupdates von Systemsoftware mobiler Endgeräte).

7.3 Prüfung der Auftragsdaten mit von der GarantiBank angezeigten Daten

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

7.4 Richtigkeit der Auftragsinformationen

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 oder die Teilnehmer:in

- 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 oder die Teilnehmer:in die GarantiBank hierüber unverzüglich unterrichten (Sperranzeige).

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

8.2 Änderung der E-Mail-Adresse des Teilnehmers oder der Teilnehmerin

Der oder die Teilnehmer:in hat in der mobilen App unverzüglich eine neue E-Mail-Adresse zu hinterlegen, wenn er oder sie zur hinterlegten E-Mail-Adresse regelmäßig keinen Zugriff mehr haben sollte. Sollte der oder die Teilnehmer:in Dritten Zugang zu seinem oder ihrem E-Mail-Postfach gewähren, hat der oder die Teilnehmer:in diese Dritten anzuweisen, keine E-Mails von der GarantiBank zu löschen oder anderweitig aus dem Posteingang zu entfernen, ohne dass eine Kenntnisnahme durch den Teilnehmer oder die Teilnehmer:in gewährleistet ist.

8.3 Anzeige von technischen Störungen

Der oder die Teilnehmer:in ist verpflichtet, Störungen bei der Übertragung von Daten oder der sonstigen Nutzung des Online- oder Mobile Banking gegenüber der GarantiBank unverzüglich anzuzeigen.

9. Nutzungssperre

9.1 Sperre auf Veranlassung des Teilnehmers oder der Teilnehmerin

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

- den Online- und Mobile-Banking-Zugang für den oder die Teilnehmer:in oder
- die Authentifizierungselemente zur Nutzung des Online- und Mobile-Banking.

Gesetzliche Vertreter:innen einer Kontoinhaberin oder eines Kontoinhabers können darüber hinaus auch den Zugang der Kontoinhaberin oder des Kontoinhabers oder deren Authentifizierungselemente sperren.

9.2 Sperre auf Veranlassung der GarantiBank

Die GarantiBank darf den Online- und Mobile-Banking-Zugang für einen Teilnehmer oder eine Teilnehmerin sperren, wenn

- sie berechtigt ist, den Online-Banking-Vertrag aus wichtigem Grund (siehe hierzu Klausel 19.3 der Allgemeinen Geschäftsbedingungen) zu kündigen,
- sachliche Gründe im Zusammenhang mit der Sicherheit der Authentifizierungselemente des Teilnehmers oder der Teilnehmerin dies rechtfertigen oder
- der Verdacht einer nicht autorisierten oder einer betrügerischen Verwendung des Authentifizierungselements besteht.

Die GarantiBank wird dem Teilnehmer oder der Teilnehmerin 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 die GarantiBank den oder die Teilnehmer:in unverzüglich.

9.4 Zugangssperre für sonstige Drittdienste

Die GarantiBank kann sonstigen Drittdiensten den Zugang zu einem Konto des Teilnehmers oder der Teilnehmerin 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 oder die Teilnehmer:in 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 die GarantiBank den oder die Teilnehmer:in unverzüglich.

10. ePostfach

10.1 Einrichtung ePostfach

Mit Vereinbarung der Nutzung von GarantiBank Online- oder Mobile-Banking richtet die GarantiBank dem oder der Teilnehmer:in ein elektronisches Postfach (ePostfach) ein. Mit der Einrichtung des ePostfachs verzichtet der oder die Teilnehmer:in 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 oder der Teilnehmer:in zuzusenden, wenn dies gesetzliche Vorgaben erforderlich machen oder es aufgrund anderer Umstände (z. B. des vorübergehenden Ausfalls des ePostfach) zweckmäßig ist. Gleiches gilt im Fall einer Sperrung des Zugangs zum Online- und Mobile-Bankings (siehe Nummer 9). Mögliche Kosten für den Versand ergeben sich aus den Angaben im Preis-/Leistungsverzeichnis.

10.2 Frist zum Herunterladen von Kontoinformationen aus dem ePostfach

In das ePostfach werden für den oder die Teilnehmer:in bestimmte Kontoinformationen der GarantiBank online eingestellt. Soweit die GarantiBank die betreffenden Informationen nicht nur zum Abruf durch den oder die Teilnehmer:in bereitstellt (z. B. Kontoauszüge), sondern zur Mitteilung verpflichtet ist, wird sie den oder die Teilnehmer:in zusätzlich per Nachricht an die hinterlegte E-Mail-Adresse oder auf sonstige Weise auf die Einstellung der Informationen in das ePostfach hinweisen. Der oder die Teilnehmer:in ist zu diesem Zweck verpflichtet, der GarantiBank eine E-Mail-Adresse mitzuteilen und auf dem aktuellen Stand zu halten, die er oder sie üblicherweise für die Kommunikation mit Dritten verwendet. Der oder die Teilnehmer:in kann sich die Informationen innerhalb der unter 10.6 genannten Frist online ansehen, diese herunterladen, ausdrucken und archivieren. Nach Ablauf der Frist sind die Informationen nicht mehr einsehbar. Diese Funktionen sind ausschließlich dem oder der Teilnehmer:in vorbehalten.

10.3 Bereitstellung von Kontoauszügen

Wenn Kontoumsätze vorliegen, werden dem oder der Teilnehmer:in einmal im Quartal Kontoauszüge bereitgestellt. Etwas anderes gilt nur, wenn vertraglich mit dem oder der Teilnehmer:in abweichende Vereinbarungen getroffen wurden. Im Zeitraum zwischen zwei Kontoauszügen kann der oder die Teilnehmer:in die Kontobewegungen durch eine Umsatzabfrage im Online- und Mobile-Banking einsehen.

10.4 Pflicht zum zeitnahen Abrufen der eingestellten Kontoinformationen und Überprüfung auf Richtigkeit durch den oder die Teilnehmer:in

Der oder die Teilnehmer:in ist verpflichtet, die eingestellten Informationen zeitnah abzurufen und sie unverzüglich auf ihre Richtigkeit zu überprüfen. Etwaige Einwendungen sind unverzüglich über das ePosfach Infoservice (Kommunikationszentrum) des GarantiBank-Online oder Mobile-Bankings oder über die E-Mail Kontaktdaten (info@garantibank.de) oder über die Website (www.garantibank,de) der Bank zu erheben.

10.5 Unveränderbarkeit der ins ePostfach gestellten Dokumente

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

10.6 Automatische Löschung von Informationen aus dem ePostfach

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 oder der Teilnehmer:in auf dessen oder deren Anforderung eine papierhafte Ausfertigung dieser Informationen zur Verfügung zu stellen. Die Kosten für die Ausfertigung in Papier auf Wunsch des Teilnehmers oder der Teilnehmerin gemäß dem Preis-/Leistungsverzeichnis müssen durch den oder die Teilnehmer:in getragen werden. Nach Beendigung der Kontobeziehung kann der oder die Teilnehmer:in die im ePostfach gespeicherten Dokumente nicht mehr online einsehen.

11. Haftung
11.1 Haftung der GarantiBank bei einem nicht autorisierten Online-Banking-Auftrag 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) und den gesetzlichen Vorschriften.

11.2. Haftung des Kontoinhabers bei missbräuchlicher Nutzung seines Authentifizierungselements
11.2.1 Haftung des Kontoinhabers für nicht autorisierte Zahlungsvorgänge vor der Sperranzeige

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

(2) Der oder die Kontoinhaber:in ist nicht zum Ersatz des Schadens nach Absatz 1 verpflichtet, wenn

- es ihm oder ihr nicht möglich gewesen ist, den Verlust, den Diebstahl, das Abhandenkommen oder eine sonstige missbräuchliche Verwendung des Authentifizierungselements vor dem nicht autorisierten Zahlungsvorgang zu bemerken, oder
- der Verlust des Authentifizierungselements durch einen Angestellten, einen Agenten, eine Zweigniederlassung eines Zahlungsdienstleisters oder eine sonstige Stelle, an die Tätigkeiten des Zahlungsdienstleisters ausgelagert wurden, verursacht worden ist.

(3) Kommt es vor der Sperranzeige zu nicht autorisierten Zahlungsvorgängen und hat der oder die Teilnehmer:in in betrügerischer Absicht gehandelt oder die Sorgfalts- und Anzeigepflichten nach diesen Vereinbarungen vorsätzlich oder grob fahrlässig verletzt, trägt der oder die Kontoinhaber:in abweichend von 11.2.1. (1) den hierdurch entstandenen Schaden in vollem Umfang. Grobe Fahrlässigkeit des Teilnehmers oder der Teilnehmerin kann insbesondere vorliegen, wenn der oder die Teilnehmer:in die 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 oder einer Teilnehmerin erhalten hat, übernimmt sie alle danach durch nicht autorisierte Online-Banking-Aufträge entstandenen Schäden. Dies gilt nicht, wenn der oder die Teilnehmer:in in betrügerischer Absicht gehandelt hat.

11.2.3 Haftungsausschluss

(1) Kann das Online- und Mobile-Banking aufgrund technischer oder sonstiger Störungen, oder im Rahmen von Wartungsarbeiten oder sonstigen Überarbeitungen der Anwendungen vorübergehend nicht genutzt 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. Die GarantiBank ist verpflichtet, den oder die Teilnehmer:in im Voraus zu informieren, wenn die Anwendungen vorhersehbar für mehr als 12 Std. nicht verfügbar sein werden.

(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.

11.2.4 Haftung für minderjährige Kontoinhaber:in
Würde nach den zuvor beschriebenen Bestimmungen eine minderjährige Person haften, so treten die gesetzlichen Vertreter:innen gesamtschuldnerisch für die Haftung der minderjährigen Person ein.

12. Datenschutzhinweis
Für das Online- und Mobile-Banking gelten die allgemeinen Datenschutzhinweise der GarantiBank.

13. Beendigung der Nutzung des Online- und Mobile-Banking
Die Nutzung des Online- und Mobile-Banking kann von dem oder der Kontoinhaber:in beendet werden. Dies führt nicht zur Beendigung der Verträge zwischen dem oder der Kontoinhaber:in und der GarantiBank. Das Löschen der GarantiBank App führt nicht zur Beendigung der Nutzung des Online- und Mobile-Bankings.

Stand: Juni 2023. Alle Angaben gelten bis auf Weiteres.

GarantiBank International N.V.Niederlassung Düsseldorf, Sitz: Düsseldorf, AG Düsseldorf HRB 35190 BLZ: 30130200 Hauptverwaltung: GarantiBank International N.V., Sitz: Amsterdam/NL,Keizersgracht 569-575, 1017 DR Amsterdam Kamer von Koophandel Amsterdam Dossier-Nr.: 33225009; AR Vorsitzender: Recep Bastug;
Vorstand: Suat Erhan Zeyneloglu (Vorstandsvorsitzender), Mustafa Övünc Sisman, Marcus Jacques Witteveen, Cem Bahadir Mutlu
Unsere Information zum Datenschutz finden Sie unter https://www.garantibank.de/datenschutz