Bedingungen für das Online-Banking

1 Leistungsangebot

(1) Der (Mit-) Kontoinhaber kann Bankgeschäfte mittels Online-Banking in dem von der LBS angebotenen Umfang abwickeln. Zudem kann er Informationen der LBS mittels Online-Banking abrufen.

(2) Bausparer, (Mit-) Kontoinhaber werden einheitlich als „Teilnehmer“, Bausparkonto einheitlich als „Konto“ bezeichnet, es sei denn, dies ist ausdrücklich anders bestimmt.

2 Voraussetzungen zur Nutzung des Online-Banking

(1) Der Teilnehmer kann das Online-Banking nutzen, wenn die LBS ihn authentifiziert hat.

(2) Authentifizierung ist das mit der LBS gesondert vereinbarte Verfahren, mit dessen Hilfe die LBS die Identität des Teilnehmers überprüfen kann. Mit den hierfür vereinbarten Authentifizierungselementen kann der Teilnehmer sich gegenüber der LBS als berechtigter Teilnehmer ausweisen, auf Informationen zugreifen (siehe Nummer 3) sowie Aufträge erteilen (siehe Nummer 4).

(3) Authentifizierungselemente sind

– Wissenselemente, also etwas, das nur der Teilnehmer weiß (z. B. persönliche Identifikationsnummer [PIN]),

– Besitzelemente, also etwas, das nur der Teilnehmer besitzt (z. B. das mobile Endgerät mit der pushTAN-App), oder

– Seinselemente, also etwas, das der Teilnehmer ist (Inhärenz, z. B. Fingerabdruck als biometrisches Merkmal des Teilnehmers).

(4) Die Authentifizierung des Teilnehmers erfolgt, indem der Teilnehmer gemäß der Anforderung der LBS das Wissenselement, den Nachweis des Besitzelements und/oder den Nachweis des Seinselements an die LBS übermittelt.

3 Zugang zum Online-Banking

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

– er seine individuelle Teilnehmerkennung (z. B. Anmeldename) angibt und

– er sich unter Verwendung des oder der von der LBS angeforderten Authentifizierungselemente(s) ausweist und

– keine Sperre des Zugangs (siehe Nummern 7.1 und 8) vorliegt.

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

4 Aufträge

4.1 Auftragsarten

Es können Aufträge verschiedener Art erteilt werden, z. B. Vertragsänderungen beantragt sowie Zustimmungen und Lastschriftmandate erteilt werden.

4.2 Auftragserteilung

Aufträge bedürfen zu ihrer Wirksamkeit einer Autorisierung durch den Teilnehmer. Auf Anforderung hat er hierzu Authentifizierungselemente zu verwenden.

Die LBS bestätigt mittels Online-Banking die Ausführung des Auftrags.

5 Information des Teilnehmers über Online-Banking-Verfügungen

Die LBS unterrichtet den Teilnehmer über die mittels Online-Banking getätigten Verfügungen auf dem für Kontoinformationen vereinbarten Weg.

6 Sorgfaltspflichten des Teilnehmers

6.1 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 (vgl. Nummer 3 und 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 Online-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 im 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 Anwendung für das Online-Banking und Fingerabdrucksensor) dient.

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

- ist sicherzustellen, dass unberechtigte Personen auf das mobile Endgerät des Teilnehmers (z. B. Mobiltelefon) 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, Authentifizierungs-App) nicht nutzen können,
- ist die Anwendung für das Online-Banking (z. B. Online-Banking-App, Authentifizierungs-App) auf dem mobilen Endgerät des Teilnehmers zu deaktivieren, bevor der Teilnehmer den Besitz an diesem mobilen Endgerät aufgibt (z. B. durch Verkauf oder Entsorgung des Mobiltelefons),
- dürfen die Nachweise des Besitzelements (z. B. TAN) nicht außerhalb des Online-Banking mündlich (z. B. per Telefon) oder in Textform (z. B. per E-Mail, Messenger-Dienst) weiter gegeben werden und
- muss der Teilnehmer, der von der LBS einen Code zur Aktivierung des Besitzelements (z. B. Mobiltelefon mit Anwendung für das Online-Banking) erhalten hat, diesen vor dem unbefugten Zugriff anderer Personen sicher verwahren; ansonsten besteht die Gefahr, dass andere Personen ihr Gerät als Besitzelement für das Online-Banking des Teilnehmers aktivieren.

(c) Seinselemente, wie z. B. Fingerabdruck des Teilnehmers, dürfen auf einem mobilen Endgerät des Teilnehmers für das Online-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 Online-Banking genutzt wird, Seinselemente anderer Personen gespeichert, ist für das Online-Banking das von der LBS ausgegebene Wissenselement (z. B. PIN) zu nutzen und nicht das auf dem mobilen Endgerät gespeicherte Seinselement.

710 900.003 D0 LBS (Fassung Nov. 2026) - v1.2
© S-Management Services • DSV Gruppe

6.2 Sicherheitshinweise der LBS
Der Teilnehmer muss die Sicherheitshinweise auf der Online-Banking-Seite der LBS, insbesondere die Maßnahmen zum Schutz der von ihm eingesetzten Hard- und Software, beachten.

6.3 Prüfung der Auftragsdaten mit von der LBS angezeigten Daten
Die LBS zeigt dem Teilnehmer die von ihr empfangenen Auftragsdaten über das gesondert vereinbarte Gerät des Teilnehmers an (z. B. mittels mobilem Endgerät). Der Teilnehmer ist verpflichtet, vor der Bestätigung die Übereinstimmung der angezeigten Daten mit den für den Auftrag vorgesehenen Daten zu prüfen.

7 Anzeige- und Unterrichtungspflichten

7.1 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, muss der Teilnehmer die LBS hierüber unverzüglich unterrichten (Sperranzeige). Der Teilnehmer kann eine solche Sperranzeige jederzeit auch über die gesondert mitgeteilten Kommunikationskanäle abgeben.
(2) Der Teilnehmer hat jeden Diebstahl oder Missbrauch eines Authentifizierungselements unverzüglich bei der Polizei zur Anzeige zu bringen.
(3) Hat der Teilnehmer den Verdacht einer nicht autorisierten oder betrügerischen Verwendung eines seiner Authentifizierungselemente, muss er ebenfalls eine Sperranzeige abgeben.

7.2 Unterrichtung über nicht autorisierte oder fehlerhaft ausgeführte Aufträge
Der Kontoinhaber hat die LBS unverzüglich nach Feststellung eines nicht autorisierten oder fehlerhaft ausgeführten Auftrags hierüber zu unterrichten.

8 Nutzungssperre

8.1 Sperre auf Veranlassung des Teilnehmers
Die LBS sperrt auf Veranlassung des Teilnehmers, insbesondere im Fall der Sperranzeige nach Nummer 7.1,
- den Online-Banking-Zugang für ihn oder alle Teilnehmer oder
- seine Authentifizierungselemente zur Nutzung des Online-Banking.

8.2 Sperre auf Veranlassung der LBS
(1) Die LBS 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 eines Authentifizierungselements besteht.

(2) Die LBS wird den Kontoinhaber 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 LBS hierdurch gegen gesetzliche Verpflichtungen verstoßen würde.

8.3 Aufhebung der Sperre
Die LBS wird eine Sperre aufheben oder die betroffenen Authentifizierungselemente austauschen, wenn die Gründe für die Sperre nicht mehr gegeben sind. Hierüber unterrichtet sie den Teilnehmer unverzüglich.

9 Haftung

9.1 Haftung der LBS bei Ausführung eines nicht autorisierten Auftrags und eines nicht, fehlerhaft oder verspätet ausgeführten Auftrags
Die Haftung der LBS bei einem nicht autorisierten Auftrag und einem nicht, fehlerhaft oder verspätet ausgeführten Auftrag richtet sich nach den gesetzlichen Regelungen.

9.2 Haftung des Teilnehmers bei missbräuchlicher Nutzung der Authentifizierungselemente

9.2.1 Haftung des Teilnehmers für nicht autorisierte Verfügungen vor der Sperranzeige
(1) Beruhen nicht autorisierte Verfügungen vor der Sperranzeige auf der Nutzung eines verlorengegangenen, gestohlenen oder sonst abhanden gekommenen Authentifizierungselements oder auf der sonstigen missbräuchlichen Verwendung eines Authentifizierungselements, haftet der Teilnehmer für den der LBS hierdurch entstehenden Schaden.
(2) Der Teilnehmer ist nicht zum Ersatz des Schadens nach Absatz 1 verpflichtet, wenn
- es dem Teilnehmer nicht möglich gewesen ist, den Verlust, den Diebstahl, das Abhandenkommen oder eine sonstige missbräuchliche Verwendung des Authentifizierungselements vor der nicht autorisierten Verfügung zu bemerken, oder
- der Verlust des Authentifizierungselements durch einen Angestellten oder eine sonstige Stelle, an die Tätigkeiten des Zahlungsdienstleisters ausgelagert wurden, verursacht worden ist.

(3) Kommt es vor der Sperranzeige zu nicht autorisierten Verfügungen und hat der Teilnehmer in betrügerischer Absicht gehandelt oder seine Sorgfalts- und Anzeigepflichten nach diesen Bedingungen vorsätzlich oder grob fahrlässig verletzt, trägt der Teilnehmer abweichend von den Absätzen 1 und 2 den hierdurch entstandenen Schaden in vollem Umfang. Grobe Fahrlässigkeit des Teilnehmers kann insbesondere vorliegen, wenn er eine seiner Sorgfaltspflichten nach
- Nummer 6.1 Absatz 2,
- Nummer 6.3 oder
- Nummer 7.1 Absatz 1

verletzt hat.
(4) Abweichend von den Absätzen 1 und 3 ist der Teilnehmer nicht zum Schadensersatz verpflichtet, wenn die LBS vom Teilnehmer eine starke Kundenauthentifizierung nach § 1 Absatz 24 ZAG nicht verlangt hat. Eine starke Kundenauthentifizierung erfordert insbesondere die Verwendung von zwei voneinander unabhängigen Authentifizierungselementen aus den Kategorien Wissen, Besitz oder Sein (siehe Nummer 2 Absatz 3).
(5) Der Teilnehmer ist nicht zum Ersatz des Schadens nach Absatz 1 und 3 verpflichtet, wenn der Teilnehmer die Sperranzeige nach Nummer 7.1 nicht abgeben konnte, weil die LBS nicht die Möglichkeit zur Entgegennahme der Sperranzeige sichergestellt hatte.
(6) Die Absätze 2 und 4 finden keine Anwendung, wenn der Teilnehmer in betrügerischer Absicht gehandelt hat.
(7) Ist der Teilnehmer kein Verbraucher, gilt ergänzend Folgendes:
- Die Haftungsbeschränkung in Absatz 2 erster Spiegelstrich findet keine Anwendung.

9.2.2 Haftung des Teilnehmers bei nicht autorisierten Verfügungen außerhalb von Zahlungsdiensten vor der Sperranzeige

Beruhen nicht autorisierte Verfügungen außerhalb von Zahlungsdiensten vor der Sperranzeige auf der Nutzung eines verlorengegangenen oder gestohlenen Authentifizierungselements oder auf der sonstigen missbräuchlichen Nutzung des Authentifizierungselements und ist der LBS hierdurch ein Schaden entstanden, haften der Teilnehmer und die LBS nach den gesetzlichen Grundsätzen des Mitverschuldens.

9.2.3 Haftung ab der Sperranzeige

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

9.2.4 Haftungsausschluss

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.

10 Außergerichtliche Streitschlichtung und sonstige Beschwerdemöglichkeit

Für die Beilegung von Streitigkeiten mit der LBS kann sich der Teilnehmer an die in der Verbraucherinformation Rahmenvereinbarung, Online-Banking und Elektronisches Postfach näher bezeichneten Streitschlichtungs- und Beschwerdestellen wenden.