

Bedingungen für das Online-Banking

Stand: 21.04.2018

1. Vertragsgegenstand

(1) Der Kontoinhaber (künftig auch: Kunde) und dessen Bevollmächtigte können Bankgeschäfte mittels Online-Banking in dem von der Mercedes-Benz Bank AG (künftig: Bank) angebotenen Umfang abwickeln. Zudem können Sie Informationen der Bank mittels Online-Banking abrufen. Sofern die Bank entscheidet solche Dienste zuzulassen, sind Sie zusätzlich berechtigt, für die Auslösung eines Zahlungsauftrages einen Zahlungsauslösedienst gemäß §1 Absatz 33 Zahlungsdienstaufsichtsgesetz und für die Mitteilung von Informationen über ein Zahlungskonto einen Kontoinformationsdienst gemäß §1 Absatz 34 Zahlungsdienstaufsichtsgesetz zu nutzen.

(2) Nutzungsberechtigte des Online-Banking Angebots der Bank sind der Kontoinhaber, bei minderjährigen Kontoinhabern grundsätzlich der/die gesetzlichen Vertreter und etwaige bevollmächtigte Personen. Diese werden künftig einheitlich als „Teilnehmer“ bezeichnet, es sei denn, dies ist ausdrücklich anders bestimmt.

2. Voraussetzungen zur Nutzung des Online-Banking

Der Teilnehmer benötigt für die Nutzung des Online-Bankings die mit der Bank vereinbarten personalisierten Sicherheitsmerkmale und Authentifizierungsinstrumente, um sich gegenüber der Bank als berechtigter Teilnehmer auszuweisen (siehe Nummer 3) und Aufträge zu autorisieren (siehe Nummer 4). Statt eines personalisierten Sicherheitsmerkmals kann auch ein biometrisches Merkmal des Teilnehmers zum Zwecke der Authentifizierung beziehungsweise Autorisierung vereinbart werden, sofern die Bank dies anbietet.

2.1 Personalisiertes Sicherheitsmerkmal: Personalisierte Sicherheitsmerkmale sind personalisierte Merkmale, die die Bank dem Teilnehmer zum Zwecke der Authentifizierung bereitstellt. Diese werden vor jeder Nutzung abgefragt. Hierbei handelt es sich um die persönliche Identifikationsnummer (PIN) und die Kundennummer,

2.2 Authentifizierungsinstrumente: Authentifizierungsinstrumente sind personalisierte Instrumente oder Verfahren, deren Verwendung zwischen der Bank und dem Kontoinhaber vereinbart wurden und die vom Teilnehmer zur Erteilung eines Online-Banking-Auftrags verwendet werden. Hierbei handelt es sich um das persönliche Auftragskennwort.

2.3 Voraussetzung für die Nutzung des Online-Bankings und des elektronischen Postfachs ist darüber hinaus die Hinterlegung einer gültigen E-Mailadresse.

3. Zugang zum Online-Banking

Der Teilnehmer erhält Zugang zum Online-Banking, wenn
- dieser seine individuelle Kundennummer und seine PIN übermittelt hat
- die Prüfung dieser Daten bei der Bank eine Zugangsberechtigung des Teilnehmers ergeben hat und

- keine Sperre des Zugangs (siehe Nummern 8.1 und 9) vorliegt.

Nach Gewährung des Zugangs zum Online-Banking kann der Teilnehmer Informationen abrufen oder Aufträge erteilen.

Sofern die Bank entscheidet solche Dienste zuzulassen, gelten die Sätze 1 und 2 auch dann, wenn der Teilnehmer Zahlungsaufträge über einen Zahlungsauslösedienst auslöst und Zahlungskontoinformationen über einen Kontoinformationsdienst anfordert (siehe Nummer 1 Absatz 1 Satz 3).

4. Online-Banking-Aufträge

4.1 Auftragserteilung und Autorisierung

Der Teilnehmer muss Online-Banking-Aufträge (zum Beispiel Überweisungen) zu deren Wirksamkeit mit seinem persönlichen Auftragskennwort autorisieren und der Bank mittels Online-Banking übermitteln. Die Bank bestätigt mittels Online-Banking den Eingang des Auftrags. Sofern die Bank entscheidet solche Dienste zuzulassen, gelten die Sätze 1 und 2 auch dann, wenn der Teilnehmer einen Zahlungsauftrag über einen Zahlungsauslösedienstleister (siehe Nummer 1 Absatz 1 Satz 3) auslöst und übermittelt.

4.2 Widerruf von Aufträgen

Die Widerrufbarkeit eines Online-Banking-Auftrags richtet sich nach den für die jeweilige Auftragsart geltenden Sonderbedingungen (zum Beispiel Überweisungsbedingungen). Nach Zugang des Auftrags des Teilnehmers bei der Bank kann dieser grundsätzlich nicht mehr widerrufen werden. Der Widerruf von Aufträgen kann nur außerhalb des Online-Banking erfolgen, es sei denn, die Bank sieht eine Widerrufsmöglichkeit im Online-Banking ausdrücklich vor.

5. Bearbeitung von Online-Banking Aufträgen durch die Bank

(1) Die Bank und die in die Abwicklung der Aufträge eingeschalteten Institute sind berechtigt, die Bearbeitung ausschließlich anhand der vom Nutzungsberechtigten angegebenen numerischen Angaben (International Bank Account Number – „IBAN“) vorzunehmen. Fehlerhafte Angaben können Fehlleistungen und damit ggf. Schaden für den Kontoinhaber zur Folge haben.

(2) Die Bearbeitung der Aufträge erfolgt an den auf der Online-Banking-Seite der Bank oder im Preis- und Leistungsverzeichnis bekannt gegebenen Geschäftstagen im Rahmen des ordnungsgemäßen Arbeitsablaufes. Geht der Auftrag nach dem auf der Online-Banking-Seite der Bank angegebenen oder im Preis- und Leistungsverzeichnis bestimmten Zeitpunkt (Annahmefrist) ein oder fällt der Zeitpunkt des Eingangs nicht auf einen Geschäftstag gemäß Preis- und Leistungsverzeichnis der Bank, so gilt der Auftrag als am darauffolgenden Geschäftstag zugegangen. Die Bearbeitung beginnt erst an diesem Tag.

(3) Die Bank wird den Auftrag ausführen, wenn folgende Ausführungsbedingungen vorliegen:

- Der Teilnehmer hat den Auftrag autorisiert.

- Das Online-Banking-Datenformat ist eingehalten.

- Die weiteren Ausführungsvoraussetzungen nach den für die jeweilige Auftragsart maßgeblichen Sonderbedingungen (zum Beispiel ausreichende Kontodeckung gemäß den Überweisungsbedingungen) liegen vor.

Liegen die Ausführungsbedingungen nach Satz 1 vor, führt die Bank die Online-Banking-Aufträge nach Maßgabe der Bestimmungen der für die jeweilige Auftragsart geltenden Sonderbedingungen (zum Beispiel Überweisungsbedingungen) aus.

(4) Erklärungen jeder Art gelten als abgegeben, wenn sie abschließend zur Übermittlung an die Bank freigegeben sind. Ist zur Durchführung einer Transaktion die Eingabe der PIN, der Super-PIN oder des Auftragskennworts notwendig, so erfolgt die Freigabe mit Eingabe und Bestätigung derselben/desselben.

(5) Liegen die Ausführungsbedingungen nach Absatz 3 Satz 1 nicht vor, wird die Bank den Online-Banking-Auftrag nicht ausführen. Sie wird den Teilnehmer hierüber mittels Online-Banking 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

Die Bank unterrichtet den Kontoinhaber mindestens einmal monatlich über die mittels Online-Banking getätigten Verfügungen auf dem für Kontoinformationen vereinbarten Weg.

7. Sorgfaltspflichten des Teilnehmers

7.1 Technische Verbindung zum Online-Banking

Der Teilnehmer ist verpflichtet, die technische Verbindung zum Online-Banking über die von der Bank gesondert mitgeteilten Online-Banking-Zugangskanäle (zum Beispiel Internetadresse) herzustellen. Sofern die Bank entscheidet solche Dienste zuzulassen, kann zur Auslösung eines Zahlungsauftrags und zum Abruf von Informationen über ein Konto der Teilnehmer die technische Verbindung zum Online-Banking auch über einen Zahlungsauslösedienst beziehungsweise einen Kontoinformationsdienst (siehe Nummer 1 Absatz 1 Satz 3) herstellen.

7.2 Geheimhaltung der Personalisierten Sicherheitsmerkmale

Zur Abwicklung der Bankgeschäfte erhält jeder Nutzungsberechtigte nach Antragstellung eine persönliche Identifikationsnummer (PIN) und eine persönliche Super-Identifikationsnummer (Super-PIN) zugesandt. Die von der Bank übermittelte PIN muss durch jeden Nutzungsberechtigten nach Zugang geändert werden. Zur Durchführung der Änderung benötigt der Nutzungsberechtigte die Super-PIN. Die Super-PIN ist nicht abänderbar. Beim erstmaligen Anmelden wird durch den Nutzungsberechtigten zusätzlich ein individuelles Auftragskennwort vergeben. Die Bestätigung dieses Auftragskennworts erfolgt durch die Eingabe der Super-PIN. PIN, Super-PIN und Auftragskennwort (künftig: geheime Daten) sind geheim zu halten und getrennt voneinander – vor dem Zugriff Dritter – sicher aufzubewahren. Denn jede Person, die die geheimen Daten kennt, hat die Möglichkeit, das Online-Banking-Angebot ungehindert zu Lasten des Kontoinhabers missbräuchlich zu nutzen.

Die Geheimhaltungspflicht bezüglich der Personalisierten Sicherheitsmerkmale nach Satz 1 gilt nicht, wenn der Teilnehmer diese zur Erteilung eines Zahlungsauftrags oder zum Abruf von Informationen über ein Zahlungskonto an den von ihm ausgewählten Zahlungsauslösedienst beziehungsweise Kontoinformationsdienst übermittelt (siehe Nummer 1 Absatz 1 Satz 3), sofern die Bank entscheidet solche Dienste zuzulassen.

(2) Insbesondere ist vom Teilnehmer zum Schutz der geheimen Daten Folgendes zu beachten:

- Die geheimen Daten dürfen nicht ungesichert gespeichert werden.
- Bei der Eingabe der geheimen Daten ist sicherzustellen, dass andere Personen diese nicht ausspähen können.
- Die geheimen Daten dürfen nicht per E-Mail weitergegeben werden.

7.3 Sicherheitshinweise der Bank

Der Teilnehmer muss die Sicherheitshinweise auf der Internetseite der Bank zum Online-Banking, insbesondere die Maßnahmen zum Schutz der eingesetzten Hard- und Software (Kundensystem), beachten.

7.4 Kontrolle der Auftragsdaten mit von der Bank angezeigten Daten
Zur Autorisierung der Leistungen im Rahmen des Online-Banking-Angebots der Bank muss der Nutzungsberechtigte bei bestimmten Funktionen sein Auftragskennwort oder seine Super-PIN eingeben. Die Bank bestätigt mittels Online-Banking jeweils den Eingang des Auftrags. Soweit die Bank dem Teilnehmer Daten aus seinem Online-Banking-Auftrag zur Bestätigung anzeigt (zum Beispiel den Betrag), ist er verpflichtet, vor der Bestätigung die Übereinstimmung der angezeigten Daten mit den für die Transaktion vorgesehenen Daten zu prüfen.

7.5 Zusätzliche Authentifizierungsstufe

Die Bank bietet jedem Zugangsberechtigten zudem die Möglichkeit, bestimmte Informationen auf Wunsch durch eine zweite Authentifizierungsstufe zu schützen. Sofern diese Funktion aktiviert wird, sind folgende Informationen bei allen verknüpften Konten für den Zugang des jeweiligen Nutzers nur nach Eingabe des Auftragskennworts ersichtlich: elektronisches Postfach, Profil, Freistellungsauftrag, Kirchensteuer.

8. Anzeige- und Unterrichtungspflichten

8.1 Sperranzeige

(1) Stellt der Teilnehmer den Verlust oder den Diebstahl der geheimen Daten, die missbräuchliche Verwendung oder die sonstige nicht autorisierte Nutzung der geheimen Daten fest, muss der Teilnehmer die Bank hierüber unverzüglich unterrichten (Sperranzeige). Der Teilnehmer kann der Bank eine Sperranzeige jederzeit auch über die gesondert mitgeteilten Kontaktdaten abgeben.

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

(3) Hat der Teilnehmer den Verdacht, dass eine andere Person unberechtigt Kenntnis von den geheimen Daten erlangt hat oder die geheimen Daten verwendet, muss er ebenfalls eine Sperranzeige abgeben.

8.2 Unterrichtung über nicht autorisierte oder fehlerhaft ausgeführt Aufträge

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

9. Nutzungssperre

9.1 Sperre auf Veranlassung des Teilnehmers

Die Bank sperrt auf Veranlassung des Teilnehmers den Online-Banking-Zugang für ihn oder alle Nutzungsberechtigten.

9.2 Sperre auf Veranlassung des Teilnehmers

(1) Die Bank 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 geheimen Daten dies rechtfertigen oder
- der Verdacht einer nicht autorisierten oder einer betrügerischen Verwendung der geheimen Daten besteht.

(2) Die Bank wird den Kontoinhaber unter Angabe der hierfür maßgeblichen Gründe möglichst vor, spätestens jedoch unverzüglich nach der Sperre auf dem vereinbarten Weg unterrichten.

9.3. Aufhebung der Sperre

Die Bank wird eine Sperre aufheben oder die geheimen Daten austauschen, wenn die Gründe für die Sperre nicht mehr gegeben sind. Hierüber unterrichtet sie den Kontoinhaber unverzüglich.

10. Mercedes-Benz Bank Postfach/ Kostenpflichtiger postalischer Versand

10.1. Das Mercedes-Benz Bank Postfach (künftig: Postfach) gilt im Rahmen der Geschäftsbeziehung als elektronisches Kommunikationsmedium, soweit die einzelnen Dokumentenarten postfachfähig sind. Dokumente (Informationen mit direktem Bezug zu einem bestehenden Vertrag, z. B. Kontoauszüge, Kontoabschlüsse und AGB-Änderungen) und Nachrichten (Information ohne direkten Bezug zu einem bestehenden Vertrag) werden grundsätzlich in elektronischer Form (pdf- bzw. HTML-Format) auf verschlüsselten Seiten in das Postfach übermittelt. Über die Einstellung von Dokumenten und Nachrichten in das Postfach wird der Kunde grundsätzlich per E-Mail unter der hinterlegten E-Mail-Adresse informiert.

Der Kunde verzichtet ausdrücklich auf den postalischen Versand dieser Dokumente und Nachrichten. Die Sätze 1 und 2 dieses Absatzes finden keine Anwendung auf Dokumente und Nachrichten, für die eine über die

Textform hinausgehende Form vorgeschrieben ist. Die Bank ist berechtigt, einzelne oder bei technischen Problemen alle Dokumente und Nachrichten auf dem Postweg oder in sonstiger Weise an den Kunden zu übermitteln, wenn dies von der Bank unter Berücksichtigung des Kundeninteresses als zweckmäßig erachtet wird. Der Kunde muss der Bank in diesen Fällen für den postalischen Versand die anfallenden Auslagen (Porto) nicht erstatten. Die Bank verpflichtet sich, bei Übermittlung von Dokumenten und Nachrichten in das Postfach die gesetzlichen Fristen einzuhalten, sofern solche bestehen.

Auf Wunsch des Kunden erfolgt im Einzelfall abweichend von Absatz 2 Satz 1 dieser Ziffer 10.1. ein postalischer Versand. Nach Übermittlung der Dokumente und Nachrichten in das Postfach ist der Kunde in der Lage, diese online anzusehen, herunterzuladen und auszudrucken.

10.2. Dokumente und Nachrichten, welche dem Kunden in das Postfach übermittelt werden, gelten grundsätzlich als mit dem Tag der Einstellung und der Möglichkeit des Abrufs im Postfach als zugegangen. Soweit die Einstellung eines Dokuments oder einer Information nach 18.00 Uhr erfolgt, gilt das jeweilige Dokument bzw. die jeweilige Information erst an dem Werktag (Montag bis Freitag) als zugegangen, der dem Einstellungstag nachfolgt.

10.3. In das Postfach übermittelte Dokumente werden grundsätzlich 24 (vierundzwanzig) Monate und übermittelte Nachrichten grundsätzlich 1 (einen) Monat – jeweils gerechnet ab Zugang des jeweiligen Dokuments oder der jeweiligen Nachricht nach Ziffer 10.2 – vorgehalten. Vom Kunden innerhalb der in dem vorstehenden Absatz genannten Zeiträume abgerufene Dokumente und abgerufene/nicht abgerufene Nachrichten werden nach Ablauf der genannten Zeiträume gelöscht. Ein Hinweis der Bank an den Kunden dahin gehend, wann welches Dokument und/oder welche Nachrichten nach den vorstehenden Vorschriften gelöscht werden, erfolgt nicht.

10.4. Auf die in das Postfach übermittelten Dokumente und Nachrichten haben nur Zugangsberechtigte Zugriff. Zugangsberechtigt sind die unter Ziffer 1 genannten Nutzungsberechtigten.

10.5. Der Kunde verpflichtet sich, die in das Postfach eingestellten Dokumente regelmäßig – entsprechend den üblichen Gepflogenheiten bei einem normalen Briefkasten – abzurufen und deren Inhalte auf Richtigkeit zu prüfen. Einwendungen wegen Unrichtigkeiten oder Unvollständigkeit eines Dokuments hat der Kunde entsprechend Ziffer 7 Absatz 2 der Allgemeinen Geschäftsbedingungen der Bank zu erheben.

10.6. Die Bank garantiert die Unveränderbarkeit der im Postfach gespeicherten Daten. Diese Garantie gilt nicht, soweit die Daten außerhalb des Postfachs gespeichert oder aufbewahrt werden. Im Zusammenhang damit wird darauf hingewiesen, dass aufgrund von individuellen Hard- oder Softwareeinstellungen Ausdrücke von Dokumenten und Nachrichten nicht immer mit der Bildschirmdarstellung übereinstimmen. Werden Dokumente oder Nachrichten verändert oder in veränderter Form in Umlauf gebracht, übernimmt die Bank hierfür keine Haftung. Die Bank kann die Anerkennung der im Postfach in elektronischer Form gespeicherten Dokumente und Nachrichten durch Steuer- oder Finanzbehörden nicht garantieren. Es obliegt dem Kunden, dies durch vorherige Erkundigung bei den zuständigen Steuer- oder Finanzbehörden sicherzustellen.

10.7. Im Falle einer Deaktivierung des Postfaches durch den Kunden gilt ab dem Zeitpunkt der Deaktivierung Ziffer 10.1 Absatz 3. Die Dokumente und Nachrichten, die bis zur Deaktivierung in das Postfach eingestellt worden sind, sind auch über jenen Zeitpunkt hinaus durch den Kunden über das Postfach abrufbar, bis sie nach den Regelungen in Ziffer 10.3 gelöscht werden. Die Regelungen dieser Ziffer 10 gelten bzgl. der Dokumente und Nachrichten, die bis zur Deaktivierung in das Postfach eingestellt worden sind, über den Zeitpunkt der Deaktivierung hinaus fort. Eine Verpflichtung der Bank zum nachträglichen postalischen Versand dieser Dokumente und Nachrichten besteht nicht.

11. Haftung

11.1 Haftung der Bank bei einer nicht autorisierten Online-Banking-Verfügung und einer nicht, fehlerhaft oder verspätet ausgeführten Online-Banking Verfügung

Die Haftung der Bank bei einer nicht autorisierten Online-Banking-Verfügung und einer nicht, fehlerhaft oder verspätet ausgeführten Online-Banking-Verfügung richtet sich nach den für die jeweilige Auftragsart vereinbarten Sonderbedingungen (zum Beispiel Überweisungsbedingungen).

11.2 Haftung des Kontoinhabers bei missbräuchlicher Nutzung der geheimen Daten

11.2.1 Haftung des Kontoinhabers für nicht autorisierte Zahlungsvorgänge vor der Sperranzeige

(1) Beruhen nicht autorisierte Zahlungsvorgänge vor der Sperranzeige auf der Nutzung der verlorengegangenen, gestohlen oder sonst abhandengekommen geheimen Daten oder auf der sonstigen missbräuchlichen Verwendung der geheimen Daten, haftet der Kontoinhaber für den der Bank hierdurch entstehenden Schaden bis zu einem Betrag von 50 Euro, ohne dass es darauf ankommt, ob den Teilnehmer ein Verschulden trifft.

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

- es ihm nicht möglich gewesen ist, den Verlust, den Diebstahl, das Abhandenkommen oder eine sonstige missbräuchliche Verwendung der geheimen Daten vor dem nicht autorisierten Zahlungsvorgang zu bemerken, oder
- der Verlust der geheimen Daten 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 einer nicht autorisierten Verfügung und hat der Teilnehmer in betrügerischer Absicht gehandelt oder seine Anzeige- und Sorgfaltspflicht nach diesen Bedingungen vorsätzlich oder grob fahrlässig verletzt, trägt der Kontoinhaber abweichend von den Absätzen 1 und 2 den hierdurch entstandenen Schaden in vollem Umfang. Grobe Fahrlässigkeit des Teilnehmers kann insbesondere dann vorliegen, wenn er

- den Verlust oder den Diebstahl der geheimen Daten oder deren missbräuchliche Verwendung der Bank schuldhaft nicht unverzüglich mitgeteilt hat, nachdem er hiervon Kenntnis erlangt hat,
- die geheimen Daten ungesichert elektronisch gespeichert hat
- die geheimen Daten zusammen verwahrt hat oder
- die geheimen Daten nicht geheim gehalten hat und der Missbrauch dadurch verursacht wurde.
- die geheimen Daten per E-Mail weitergegeben hat.

(4) Der Kontoinhaber ist nicht zum Ersatz des Schadens nach Absatz 1 und 3 verpflichtet, wenn der Teilnehmer die Sperranzeige nicht abgeben konnte, weil die Bank nicht die Möglichkeit zur Entgegennahme der Sperranzeige sichergestellt hatte .

(5) Die Absätze 2 und 4 finden keine Anwendung, wenn der Teilnehmer in betrügerischer Absicht gehandelt hat.

(6) Ist der Kontoinhaber kein Verbraucher, gilt ergänzend Folgendes:

- Der Kontoinhaber haftet für Schäden aufgrund von nicht autorisierten Zahlungsvorgängen über die Haftungsgrenze von 50 Euro nach Absatz 1 und 3 hinaus, wenn der Teilnehmer fahrlässig oder vorsätzlich gegen seine Anzeige- und Sorgfaltspflichten nach diesen Bedingungen verstoßen hat.
- Die Haftungsbeschränkung in Absatz 2 erster Spiegelstrich findet keine Anwendung.

11.2.2 Haftung der Bank ab Sperranzeige

Sobald die Bank 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.

12. Haftungsausschluss

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