Sonderbedingungen für die Teilnahme am Onlinebanking der Bank of Scotland

Stand: 13.01.2018

1. Leistungsangebot

(1) Der Kontoinhaber kann Bankgeschäfte mittels Onlinebanking in dem von der Bank of Scotland („Bank“) angebotenen Umfang abwickeln. Zudem kann er Informationen der Bank mittels Onlinebanking abrufen.

(2) Nutzungsberechtigter des Onlinebanking-Angebotes der Bank ist der Kontoinhaber. Eine Berechtigung weiterer Personen, das Onlinebanking-Angebot anstelle des Kontoinhabers zu nutzen, ist nicht möglich.

2. Voraussetzungen zur Nutzung des Onlinebanking

Der Kontoinhaber benötigt für die Nutzung des Onlinebanking die mit der Bank vereinbarten Personalisierten Sicherheitsmerkmale und das Authentifizierungsinstrument, um sich gegenüber der Bank als berechtigter Kontoinhaber auszuweisen (siehe Nummer 3) und Aufträge zu autorisieren (siehe Nummer 4).
Für die Nutzung des Onlinebanking ist ein Internetzugang erforderlich. Dieser Internetzugang wird nicht von der Bank bereitgestellt. Für das Onlinebanking bedarf es zurzeit eines Browsers, der mindestens eine 128-Bit-SSL-Verschlüsselung unterstützt. Das Onlinebanking ist zurzeit für die Nutzung mit den Browsern Internet Explorer und Firefox optimiert; die Nutzbarkeit mit anderen Browsern kann nicht gewährleistet werden.

2.1 Personalisierte Sicherheitsmerkmale

Personalisierte Sicherheitsmerkmale sind personalisierte Merkmale, die die Bank dem Kontoinhaber zum Zwecke der Authentifizierung bereitstellt. Personalisierte Sicherheitsmerkmale sind

- der Benutzername
- das persönliche Kennwort
- die vom Kontoinhaber festzulegende Sicherheitsfrage nebst Antwort sowie
- die einmal verwendbaren mobilen Transaktionsnummern („mTAN").

2.2 Authentifizierungsinstrument

Authentifizierungsinstrumente sind personalisierte Instrumente oder Verfahren, deren Verwendung zwischen der Bank und dem Kontoinhaber vereinbart wurden und die vom Kontoinhaber zur Erteilung eines Online-Banking-Auftrags verwendet werden. Mittels folgendem Authentifizierungsinstrumente kann das Personalisierte Sicherheitsmerkmal dem Kontoinhaber zur Verfügung gestellt werden:

- ein zum Empfang von mTAN per Textnachricht (SMS) geeignetes Empfangsgerät (z. B. Mobiltelefon).

Das für das mTAN-Verfahren erforderliche Empfangsgerät besteht aus dem entsprechenden Gerät sowie aus der SIM-Karte eines deutschen Mobilfunk-Netzbetreibers.

3. Zugang zum Onlinebanking

Der Kontoinhaber erhält Zugang zum Onlinebanking, wenn

- die Erstaktivierung erfolgreich durchgeführt wurde, und er seinen Benutzernamen, das persönliche Kennwort sowie die Antwort auf die Sicherheitsfrage übermittelt hat,
- die Prüfung dieser Daten bei der Bank eine Zugangsberechtigung ergeben hat und
- keine Sperre des Zugangs (siehe Nummern 9.1 und 10) vorliegt.

Nach Gewährung des Zugangs zum Onlinebanking kann der Kontoinhaber Informationen abrufen oder Aufträge erteilen.

4. Onlinebanking-Aufträge

4.1 Auftragserteilung und Autorisierung

Der Kontoinhaber muss Onlinebanking-Aufträge (z. B. Überweisungen) zu deren Wirksamkeit mit einer mTAN autorisieren und der Bank mittels Onlinebanking übermitteln. Die Bank bestätigt mittels Onlinebanking den Eingang des Auftrags. Erklärungen, die keiner Autorisierung durch eine mTAN bedürfen, sind gegenüber der Bank wirksam abgegeben, wenn der Nutzungsberechtigte die in der Benutzerführung vorgeschriebene Freigabe zur Übermittlung an die Bank vorgenommen hat.

4.2 Widerruf von Aufträgen

Die Widerrufbarkeit eines Onlinebanking-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 Onlinebanking erfolgen, es sei denn, die Bank sieht eine Widerrufsmöglichkeit im Onlinebanking ausdrücklich vor.

5. Bearbeitung von Onlinebanking-Aufträgen durch die Bank

(1) Die Bearbeitung der Onlinebanking-Aufträge erfolgt an den für die Abwicklung der jeweiligen Auftragsart (z. B. Überweisung) auf der Onlinebanking-Seite der Bank oder im „Preis- und Leistungsverzeichnis“ bekannt gegebenen Geschäftstagen im Rahmen des ordnungsgemäßen Arbeitsablaufes. Geht der Auftrag nach dem auf der Onlinebanking-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 darauf folgenden Geschäftstag zugegangen. Die Bearbeitung beginnt dann erst an diesem Tag.

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

- Der Kontoinhaber hat den Auftrag autorisiert.
- Die Berechtigung des Kontoinhabers für die jeweilige Auftragsart liegt vor.
- Das Onlinebanking-Datenformat ist eingehalten.
- Die weiteren Ausführungsvoraussetzungen nach den für die jeweilige Auftragsart maßgeblichen Sonderbedingungen (z. B. Bedingungen für den Überweisungsverkehr) liegen vor.

Liegen die Ausführungsbedingungen nach Satz 1 vor, führt die Bank die Onlinebanking-Aufträge nach Maßgabe der Bestimmungen der für die jeweilige Auftragsart geltenden Sonderbedingungen (z. B. Beispiel Bedingungen für den Überweisungsverkehr) aus.

(3) Liegen die Ausführungsbedingungen nach Absatz 2 Satz 1 nicht vor, wird die Bank den Onlinebanking-Auftrag nicht ausführen. Sie wird den hierüber mittels Onlinebanking 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 Onlinebanking - Verfügungen

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

7. Postbox

(1) Im Rahmen der Geschäftsbeziehung zwischen der Bank und dem Kontoinhaber gilt die Nutzung der Postbox als vereinbarter Kommunikationsweg. In der Postbox werden dem Kontoinhaber Nachrichten der Bank online zur Verfügung gestellt. Der Kontoinhaber hat ferner die Möglichkeit, der Bank Anfragen und bestimmte Aufträge über die Postbox zu senden.

(2) Der Kontoinhaber verzichtet durch die Nutzung der Postbox ausdrücklich auf den postalischen Versand aller Dokumente und Nachrichten durch die Bank in papiergebundener Form. Dokumente, die aufgrund rechtlicher Anforderungen von der Bank erteilt werden müssen, insbesondere Kontoauszüge und Kontoabschlüsse, sowie Nachrichten betreffend den Geschäftsverkehr mit der Bank, werden dem Kontoinhaber daher grundsätzlich nur in elektronischer Form auf verschlüsselten Seiten in die Postbox im Rahmen des Onlinebanking übermittelt. Hierbei werden Nachrichten der Bank an den Kontoinhaber direkt in der Postbox zur Verfügung gestellt und Dokumente (z. B. Kontoauszüge) unter dem Menüpunkt „Kontoinformationen“. Auf Wunsch des Kontoinhabers kann nachträglich ein ggf. kostenpflichtiger postalischer Versand von Dokumenten oder Nachrichten entsprechend den Regelungen im „Preis- und Leistungsverzeichnis“ der Bank erfolgen. Die Bank ist berechtigt, dem Kontoinhaber die hinterlegten Dokumente und Nachrichten auf dem Postweg oder auf andere Weise zu übermitteln, wenn dies gesetzliche Vorgaben erforderlich machen oder die Bank dies aufgrund anderer Umstände (z. B. technischer Probleme) unter Berücksichtigung des Kundeninteresses als zweckmäßig erachtet.

(3) Im Rahmen des Onlinebanking an den Kontoinhaber übermittelte Dokumente und Nachrichten gelten mit der Einstellung und der Möglichkeit des Abrufs als zugegangen. Der Zugang gilt als am darauf folgenden Werktag bewirkt, wenn die Einstellung nach 18.00 Uhr oder an einem Sonn- oder Feiertag erfolgt.

(4) Der Kontoinhaber verpflichtet sich, regelmäßig zu prüfen, ob neue Dokumente in der Postbox und unter dem Menüpunkt „Kontoinformationen“ hinterlegt sind. Er kontrolliert die hinterlegten Dokumente auf Richtigkeit und Vollständigkeit. Beanstandungen sind der Bank unverzüglich, spätestens jedoch 6 Wochen nach Zugang der Dokumente gemäß Absatz 3 und aus Beweisgründen in Textform mitzuteilen.

(5) Die Bank garantiert die Unveränderbarkeit der Daten in der Postbox und der unter dem Menüpunkt „Kontoinformationen“ gespeicherten Dokumente, sofern diese innerhalb des Menüpunkts „Kontoinformationen“ gespeichert oder aufbewahrt werden. Werden Dokumente außerhalb der Postbox bzw. des Menüpunkt „Kontoinformationen“ gespeichert, aufbewahrt oder in veränderter Form in Umlauf gebracht, übernimmt die Bank hierfür keine Haftung.

(6) Die Bank speichert die in der Postbox enthaltenen Dokumente nur für einen begrenzten Zeitraum. Die für ein Dokument geltende Aufbewahrungsfrist wird in der Postbox im Postbox-Posteingang jeweils für jede Nachricht angezeigt. Für unter dem Menüpunkt „Kontoinformationen“ abrufbare Dokumente gelten die jeweiligen gesetzlichen Aufbewahrungsfristen. Nach Ablauf der jeweiligen Aufbewahrungsfrist kann die Bank die

entsprechenden Dokumente und Nachrichten aus der Postbox entfernen, ohne dass der Kontoinhaber hierüber eine gesonderte Nachricht erhält. Falls ein Nachdruck erforderlich sein sollte, kann dies durch die Bank auf Anfrage erfolgen. Hierfür gilt das „Preis- und Leistungsverzeichnis" der Bank.

8. Sorgfaltspflichten des Kontoinhabers

8.1 Technische Verbindung zum Onlinebanking

Der Kontoinhaber ist verpflichtet, die technische Verbindung zum Onlinebanking nur über die von der Bank gesondert mitgeteilten Onlinebanking-Zugangskanäle (z. B. Internetadresse) herzustellen.

8.2 Geheimhaltung der personalisierten Sicherheitsmerkmale und sichere Aufbewahrung des Authentifizierungsinstrumentes

(1) Der Kontoinhaber hat
- seine personalisierten Sicherheitsmerkmale (siehe Nummer 2.1) geheim zu halten sowie
- sein Authentifizierungsinstrument (siehe Nummer 2.2) vor dem Zugriff anderer Personen sicher zu verwahren.

Denn jede andere Person, die im Besitz des Authentifizierungsinstruments ist, kann in Verbindung mit der Kenntnis des dazu gehörigen Personalisierten Sicherheitsmerkmals das Onlinebanking-Verfahren missbräuchlich nutzen.

(2) Insbesondere ist Folgendes zum Schutz des Personalisierten Sicherheitsmerkmals sowie des Authentifizierungsinstruments zu beachten:

- Die personalisierten Sicherheitsmerkmale dürfen nicht ungesichert elektronisch gespeichert werden.
- Bei Eingabe des Personalisierten Sicherheitsmerkmals ist sicherzustellen, dass andere Personen dieses nicht ausspähen können.
- Das personalisierte Sicherheitsmerkmal darf nicht per E-Mail weitergegeben werden.
- Das personalisierte Sicherheitsmerkmal darf nicht zusammen mit dem Authentifizierungsinstrument verwahrt werden.
- Der Kontoinhaber darf zur Autorisierung zum Beispiel. eines Auftrages nicht mehr als eine mTAN verwenden.
- Das Empfangsgerät, mit dem die mTAN empfangen werden (z. B. Mobiltelefon), darf nicht gleichzeitig für das Onlinebanking benutzt werden.

8.3 Sicherheitshinweise der Bank

Der Kontoinhaber muss die Sicherheitshinweise auf der Internetseite der Bank zum Onlinebanking, insbesondere die Maßnahmen zum Schutz der eingesetzten Hard- und Software („Kundensystem"), beachten.

8.4 Kontrolle der Auftragsdaten mit von der Bank angezeigten Daten

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

9. Anzeige- und Unterrichtungspflichten

9.1 Sperranzeige

(1) Stellt der Kontoinhaber
- den Verlust oder den Diebstahl des Authentifizierungsinstruments, die missbräuchliche Verwendung oder
- die sonstige nicht autorisierte Nutzung seines Authentifizierungsinstruments oder eines seiner Personalisierten Sicherheitsmerkmale

fest, muss der Kontoinhaber die Bank hierüber unverzüglich unterrichten (Sperranzeige). Der Kontoinhaber kann der Bank eine Sperranzeige jederzeit auch über die gesondert mitgeteilten Kontaktdaten abgeben.

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

(3) 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 die personalisierten Sicherheitsmerkmale verwendet,

muss er ebenfalls eine Sperranzeige abgeben.

9.2 Unterrichtung über nicht autorisierte oder fehlerhaft ausgeführte Aufträge

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

10. Nutzungssperre

10.1 Sperre auf Veranlassung des Kontoinhabers

Die Bank sperrt auf Veranlassung des Kontoinhabers, insbesondere im Fall der Sperranzeige nach Nummer 9.1 den Onlinebanking-Zugang für ihn.

10.2 Sperre auf Veranlassung der Bank

(1) Die Bank darf den Onlinebanking-Zugang für einen Kontoinhaber sperren, wenn
- sie berechtigt ist, den Onlinebanking-Vertrag 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.

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

10.3 Aufhebung der Sperre

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

11. Haftung

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

Die Haftung der Bank bei einer nicht autorisierten Onlinebanking-Verfügung und einer nicht, fehlerhaft oder verspätet ausgeführten Onlinebanking-Verfügung richtet sich nach den für die jeweilige Auftragsart vereinbarten Sonderbedingungen (z. B. Bedingungen für den Überweisungsverkehr).

11.2 Haftung des Kontoinhabers bei missbräuchlicher Nutzung eines Personalisierten Sicherheitsmerkmals oder eines Authentifizierungsinstruments

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 verloren gegangenen, gestohlenen oder sonst abhanden gekommenen Authentifizierungsinstruments oder auf der sonstigen missbräuchlichen Verwendung eines Authentifizierungsinstruments, haftet der Kontoinhaber für den der Bank hierdurch entstehenden Schaden bis zu einem Betrag von 50 Euro, ohne dass es darauf ankommt, ob den Kontoinhaber 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 des Authentifizierungsinstruments vor dem nicht autorisierten Zahlungsvorgang zu bemerken.

(3) Kommt es vor der Sperranzeige zu nicht autorisierten Zahlungsvorgängen und hat der Kontoinhaber in betrügerischer Absicht gehandelt oder seine Anzeige- und Sorgfaltspflichten nach diesen Bedingungen vorsätzlich oder grob fahrlässig verletzt, trägt der Kontoinhaber abweichend von den Absätzen 1 und 2 den hierdurch entstandenen Schaden im vollen Umfang. Grobe Fahrlässigkeit des Kontoinhabers kann insbesondere vorliegen, wenn er
- den Verlust oder Diebstahl des Authentifizierungsinstruments oder die missbräuchliche Nutzung des Authentifizierungsinstruments oder der personalisierten Sicherheitsmerkmale der Bank nicht unverzüglich anzeigt, nachdem er hiervon Kenntnis erlangt hat (siehe Nummer 9.1 Absatz 1),
- das Personalisierte Sicherheitsmerkmal ungesichert elektronisch gespeichert hat (siehe Nummer 8.2 Absatz 2, 1. Spiegelstrich),
- das Personalisierte Sicherheitsmerkmal nicht geheim gehalten hat und der Missbrauch dadurch verursacht wurde (siehe Nummer 8.2 Absatz 1, 1. Spiegelstrich),
- das Personalisierte Sicherheitsmerkmal per E-Mail weitergegeben hat (siehe Nummer 8.2 Absatz 2, 3. Spiegelstrich),
- das Personalisierte Sicherheitsmerkmal auf dem Authentifizierungsinstrument vermerkt oder zusammen mit diesem verwahrt hat (siehe Nummer 8.2, Absatz 2, 4. Spiegelstrich),
- mehr als eine mTAN zur Autorisierung eines Auftrags verwendet hat (siehe Nummer 8.2 Absatz 2, 5. Spiegelstrich),
- das Empfangsgerät, mit dem die mTAN empfangen werden (z. B. Mobiltelefon), auch für das Onlinebanking nutzt (siehe Nummer 8.2 Absatz 2, 6. Spiegelstrich).

(4) Abweichend von den Absätzen 1 und 3 ist der Kontoinhaber nicht zum Schadensersatz verpflichtet, wenn die Bank eine starke Kundenauthentifizierung nach § 1 Absatz 24 Zahlungsdiensteaufsichtsgesetz nicht verlangt hat, obwohl die Bank zur starken Kundenauthentifizierung nach

§ 68 Absatz 4 Zahlungsdiensteaufsichtsgesetz verpflichtet war. Eine starke Kundenauthentifizierung erfordert insbesondere die Verwendung von zwei voneinander unabhängigen Elementen aus den Kategorien Wissen (etwas, das der Kontoinhaber weiß, zum Beispiel PIN), Besitz (etwas, das der Kontoinhaber besitzt, zum Beispiel TAN-Generator) oder Inhärenz (etwas, das der Kontoinhaber ist, zum Beispiel Fingerabdruck).

11.2.2 Haftung der Bank ab Sperranzeige

Sobald die Bank eine Sperranzeige des Kontoinhabers erhalten hat, übernimmt sie alle danach durch nicht autorisierte Onlinebanking-Verfügungen entstehenden Schäden. Dies gilt nicht, wenn der Kontoinhaber in betrügerischer Absicht gehandelt hat.

11.2.3 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.

12. Verarbeitung von personenbezogenen Daten nach § 13 Absatz 1 TMG (Telemediengesetz)

Alle im Rahmen des Onlinebanking anfallenden personenbezogenen Daten werden zum Zwecke der Vertragsdurchführung von der Bank und gegebenenfalls von dem von ihr beauftragten Rechenzentrum innerhalb Deutschlands bzw. der Europäischen Union verarbeitet.

13. Geschäftsbedingungen

Die Allgemeinen Geschäftsbedingungen und die jeweiligen Produktbedingungen gelten ergänzend zu diesen Sonderbedingungen.