Version 2.2., gültig ab 31.10.2018

ANHANG B – SONDERBEDINGUNGEN ZUM ONLINE-BANKING

INHALTSVERZEICHNIS

1. Leistungsangebot

(1) Der Kontoinhaber kann Bankgeschäfte mittels Online-Banking in dem von der Ferratum Bank p.l.c. (nachfolgend „die Bank"), angebotenen Umfang abwickeln. Zudem kann er Informationen der Bank mittels Online-Banking abrufen.

(2) Der Kontoinhaber wird im Folgenden einheitlich und geschlechtsneutral als „Teilnehmer" bezeichnet. Das Sparkonto und das Festgeldkonto werden im Folgenden einheitlich als „das Konto" bezeichnet.

(3) Die Bank ist berechtigt, dem Kunden Änderungen ihrer Geschäftsbedingungen auf elektronischem Weg sowie zur Abholung bereitzustellen. Im Hinblick auf die Gültigkeit von Änderungen gelten die Bestimmungen unter Nummer 1, Absatz 2 der allgemeinen Geschäftsbedingungen.

2. Voraussetzungen für die Nutzung des Online-Banking

Der Teilnehmer benötigt für die Abwicklung von Bankgeschäften mittels Online-Banking 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).

2.1 Personalisierte Sicherheitsmerkmale

Die personalisierten Sicherheitsmerkmale sind:

• die Persönliche Identifikationsnummer (PIN)

• das Passwort

• Nutzerkennung

3. Zugang zum Online-Banking

Die Kunden haben Zugang zum Online-Banking, wenn

• die Kontonummer des Kunden oder dessen individuelle Kundenkennung und seine PIN oder elektronische

Unterschrift übertragen werden,

• die Überprüfung dieser Daten Zugangsberechtigung des Kunden zur Bank ergeben hat und

• keine Zugangssperre (siehe Nummer 16 und 17) besteht.

Nach Gewähren des Zugangs zum Online-Banking kann der Kunde Informationen einholen und Aufträge erteilen.

4. Online-Banking-Aufträge

4.1 Aufträge und Ermächtigung erteilen

Der Kunde muss Online-Banking-Aufträge (z. B. Überweisungen auf das Referenzkonto) anhand des vereinbarten personalisierten Sicherheitsmerkmals (PIN) genehmigen, damit diese wirksam werden, und diese per Online-Banking an die Bank senden. Die Bank bestätigt den Eingang des Auftrags per Online-Banking. Schriftliche Aufträge oder Verträge in anderer Form als per Online-Banking werden nicht von der Bank akzeptiert.

4.2 Widerruf von Aufträgen

Die Widerrufbarkeit eines Onlinebanking-Vertrags unterliegt Sonderbedingungen. Eine Zahlungsanweisung an die Bank ist unwiderruflich und kann nicht storniert oder widerrufen werden. (Siehe Bestimmung 8 „Kommunikation und Zahlungsanweisungen" der allgemeinen Geschäftsbedingungen).

5. Bearbeitung von Online-Banking-Aufträgen durch die Bank

(1) Die Bearbeitung der Online-Banking-Aufträge erfolgt an den für die Abwicklung der jeweiligen Auftragsart (zum Beispiel Überweisung) auf der Online-Banking-Seite der Bank bekannt gegebenen Geschäftstagen im Rahmen des ordnungsgemäßen Arbeitsablaufes. Geht der Auftrag nach dem auf der Online-Banking-Seite der Bank angegebenen bestimmten Zeitpunkt (Annahmefrist) ein oder fällt der Zeitpunkt des Eingangs nicht auf einen Geschäftstag der Bank, so gilt der Auftrag als am darauf folgenden Geschäftstag zugegangen. Die Bearbeitung beginnt erst an diesem Tag.

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

- Der Teilnehmer hat sich mit seinem personalisierten Sicherheitsmerkmal (z. B. PIN) legitimiert;
- Die Berechtigung des Teilnehmers für die jeweilige Auftragsart liegt vor;
- Das Online-Banking-Datenformat ist eingehalten.
- Die gesondert vereinbarte Online-Banking-Verfügungslimit ist nicht überschritten.
- Die Ausführungsvoraussetzungen nach den für die jeweilige Auftragsart maßgeblichen Sonderbedingungen (zum Beispiel ausreichende Kontodeckung gemäß den Geschäftsbedingungen für Zahlungs- und Überweisungsverkehr) liegen vor.

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

(3) Liegen die Ausführungsbedingungen nach Absatz 2 Satz 1 nicht vor, wird die Bank den Online-Banking-Auftrag nicht ausführen und den Teilnehmer über die Nichtausführung und soweit möglich über deren Gründe und die Möglichkeiten, mit denen die Fehler, die zur Ablehnung geführt haben, berichtigt werden können, informieren, damit der Online-Banking-Dienst wieder genutzt werden kann. Laut „Anhang D – Geschäftsbedingungen für Zahlungs – und Überweisungsverkehr“ der allgemeinen Geschäftsbedingungen kann die Bank die Ausführung der Zahlungsanweisung verweigern.

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 Kunden

7.1 Technische Verbindung zum Online-Banking

Der Kunde ist verpflichtet, die technische Verbindung zum Online-Banking nur über die von der Bank gesondert mitgeteilte Online-Banking-Zugangskanälen Online-Banking-Zugangskanäle (z. B. Internetadresse) herzustellen.

7.2 Geheimhaltung der personalisierten Sicherheitsmerkmale und sichere Aufbewahrung der Authentifizierungsinstrumente

(1) Der Teilnehmer hat

- seine personalisierten Sicherheitsmerkmale (vgl. Nummer 2.1) geheim zu halten und nur im Rahmen einer Auftragserteilung über die von der Bank gesondert mitgeteilten Online-Banking-Zugangskanäle an diese zu übermitteln

Denn jede andere Person, die im Besitz der personalisierten Sicherheitsmerkmale ist, kann das Online-Banking-Verfahren missbräuchlich nutzen.

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

- Das personalisierte Sicherheitsmerkmal darf nicht elektronisch gespeichert werden (z. B. im Kundensystem).
- Bei Eingabe des personalisierten Sicherheitsmerkmals ist sicherzustellen, dass andere Personen dieses nicht ausspähen können.
- Das Personalisierte Sicherheitsmerkmal darf nicht außerhalb des Online-Banking-Verfahrens weitergegeben werden, also beispielsweise nicht per E-Mail.

- Die PIN und der Nutzungscode für die elektronische Signatur dürfen nicht zusammen mit dem Authentifizierungsinstrument verwahrt werden

7.3 Sicherheit des Kundensystems

Der Teilnehmer muss die Sicherheitshinweise der Bank zum Online-Banking, insbesondere die Maßnahmen zum Schutz der eingesetzten Hard- und Software (Kundensystem), beachten. Die Hard- und Software muss den aktuellen Sicherheitsstandards gerecht werden und er muss die im Handel erhältlichen Sicherheitsvorkehrungen zum Schutz vor Viren und Missbrauch nutzen.

7.4 Sicherheit und Zugang

7.4.1 Außer den in den häufig gestellten Fragen (FAQ) erwähnten Sicherheitsmerkmalen verlangt die Bank keine diesbezüglichen Angaben. Sollte Sie Ihre Sicherheitsmerkmale vergessen oder bemerken oder vermuten, dass eine andere Person Kenntnis von einem oder mehreren Sicherheitsmerkmale erlangt hat, sollten Sie unverzüglich den Kundenservice der Bank informieren und den Anweisungen in den häufig gestellten Fragen Folge leisten.

7.4.2 Es obliegt Ihrer Verantwortung, sicherzustellen, dass die Sicherheitsmerkmale für Ihr Online-Konto sicher aufbewahrt werden. Sie haben die folgenden Pflichten:

- Wenn Sie eines Ihrer Sicherheitsmerkmale verloren haben oder vermuten, dass eine andere Person Ihre Sicherheitsmerkmale kennt, Ihre Konten benutzt oder die Sicherheitsmerkmale gestohlen hat, müssen Sie die Bank unverzüglich durch telefonische Mitteilung an den Kundenservice informieren.
- Sie müssen die vorliegenden Transaktionsübersichten prüfen und die Bank unverzüglich über etwaige nicht autorisierte
- Transaktionen informieren.
- Sie dürfen keiner anderen Person erlauben, Ihre Konten zu verwenden.
- Sie müssen die Sicherheitswarnungen oder die Ratschläge der Bank einschließlich etwaiger Sicherheitswarnungen auf der Website und/oder im Online-Konto befolgen.

7.4.3 Die Bank wird ihr Möglichstes tun, um unberechtigte Zugriffe auf Ihr Online-Konto zu verhindern und sicherzustellen, dass dieses sicher ist, einschließlich angemessener Maßnahmen zum Schutz der Geheimhaltung Ihrer Sicherheitsmerkmale. Die Bank behält sich das Recht vor, die Nutzung Ihrer Sicherheitsmerkmale für den Zugriff auf Ihr Online-Konto, für Abbuchungen von Ihrem Konto oder sonstigen Transaktionen unverzüglich zu sperren, falls:

- die Bank Grund zur Annahme hat, dass das Online-Konto nicht sicher ist oder sein könnte,
- die Bank Grund zur Annahme hat, dass eine unberechtigte oder betrügerische Nutzung des Online-Kontos erfolgt ist, oder
- Sie die Bank über eine unberechtigte oder betrügerische Nutzung des Online-Kontos informiert haben.

7.4.4. Wenn einer der über Ihr Online-Konto verfügbaren Dienste gesperrt ist, können Sie den Kundenservice der Bank anrufen oder die Freischaltung des gesperrten Dienstes über das Nachrichtencenter anfordern.

7.4.5. Falls eines der folgenden Probleme auftritt, sollten Sie sich umgehend telefonisch oder über das Nachrichtencenter mit dem Kundenservice der Bank in Verbindung setzen:

- wenn bei der Nutzung der Website der Bank oder der mobilen Ferratum-App Probleme auftreten,
- wenn Sie beim Zugriff auf Ihr Online-Konto eine technische oder sonstige Störung bemerken, welche die Sicherheit der Bankdienstleistungen gefährdet, oder
- wenn Sie Unregelmäßigkeiten bei Zahlungsvorgängen auf Websites von Drittanbietern oder an anderer Stelle entdecken, die dazu führen können, dass Ihr Online-Konto ohne Ihre Genehmigung von anderen Personen benutzt wird oder darauf zugegriffen wird.

7.5 Kontrolle der Auftragsdaten mit von der Bank angezeigten Daten

Soweit die Bank dem Teilnehmer Daten aus seinem Online-Banking- Auftrag (zum Beispiel Betrag, Kontonummer des Zahlungsempfängers) im Kundensystem oder über ein anderes Gerät des Teilnehmers zur Bestätigung anzeigt, ist der Teilnehmer verpflichtet, vor der Bestätigung die Übereinstimmung der angezeigten Daten mit den für die Transaktion vorgesehenen Daten zu prüfen.

8. Anzeige- und Unterrichtungspflichten

8.1 Sperranzeige

(1) Stellt der Teilnehmer den Verlust oder den Diebstahl des Authentifizierungsinstruments, die missbräuchliche Verwendung oder die sonstige nicht autorisierte Nutzung seines Authentifizierungsinstruments oder seines personalisierten Sicherheitsmerkmals fest, muss der Teilnehmer die Bank hierüber unverzüglich unterrichten (Sperranzeige). Der Teilnehmer kann der Bank eine Sperranzeige jederzeit auch über gesondert mitgeteilte Kontaktdaten aufgeben.

(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

- den Besitz an seinem Authentifizierungsinstrument oder die Kenntnis seines personalisierten Sicherheitsmerkmals erlangt hat oder
- das Authentifizierungsinstrument oder das personalisierte Sicherheitsmerkmal verwendet, muss er ebenfalls eine Sperranzeige abgeben.

8.2 Unterrichtung über nicht genehmigte oder falsch ausgeführte 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, insbesondere im Fall der Sperranzeige nach Nummer 8.1,

- den Online-Banking-Zugang für ihn oder alle Teilnehmer oder
- sein Authentifizierungsinstrument.

9.2 Sperre auf Veranlassung der Bank

(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 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 unterrichten.

9.3 Aufhebung der Sperre

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

9.4 Automatische Anmeldesperre im Internet-Banking und automatische Sperrung der Ferratum-Karte

(1) Die mobile App und die Weboberfläche werden automatisch eine Stunde lang gesperrt, wenn die Nutzerkennung oder das Passwort dreimal (3) in Folge falsch eingegeben wurden.

Nach 60 Minuten kann ein erneuter Anmeldeversuch erfolgen. Werden die Anmeldeinformationen erneut dreimal in Folge falsch eingegeben, wird der Teilnehmer dauerhaft gesperrt.

Die Ferratum-Karte wird automatisch gesperrt, wenn die PIN dreimal (3) in Folge falsch eingegeben wird. In diesem Fall können die in Absatz 1 und 2 genannten Authentifizierungsinstrumente nicht mehr für das Online-Banking verwendet werden. Wurde der Teilenehmer dauerhaft gesperrt, kann er sich unter der rund um die Uhr besetzten Telefonnummer +46 2020 2121 mit dem Kundenservice der Bank in Verbindung setzen, der nach erfolgreicher Identitätsprüfung die Sperre wiederaufheben kann.

10. Haftung

10.1 Haftung der Bank bei einer nicht autorisierten Online-Banking-Verfügung und einer nicht oder fehlerhaft ausgeführten Online-Banking-Verfügung

Die Haftung der Bank 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. Geschäftsbedingungen für den Überweisungsverkehr).

10.2 Haftung des Kontoinhabers bei missbräuchlicher Nutzung seines Authentifizierungsinstruments

10.2.1 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 abhandengekommenen Authentifizierungsinstruments, haftet der Kontoinhaber für den der Bank hierdurch entstehenden Schaden bis zu einem Betrag von 150 Euro, ohne dass es darauf ankommt, ob dem Teilnehmer an dem Verlust, Diebstahl oder sonstigem Abhandenkommen des Authentifizierungsinstruments ein Verschulden trifft.

(2) Kommt es vor der Sperranzeige zu nicht autorisierten Zahlungsvorgängen aufgrund einer missbräuchlichen Verwendung eines Authentifizierungsinstruments, ohne dass dieses verlorengegangen, gestohlen oder sonst abhandengekommen ist, haftet der Kontoinhaber für den der Bank hierdurch entstehenden Schaden bis zu einem Betrag von 150 Euro, wenn der Teilnehmer seine Pflicht zur sicheren Aufbewahrung der Personalisierten Sicherheitsmerkmale schuldhaft verletzt hat

(3) Der Kontoinhaber ist nicht zum Ersatz des Schadens nach den Absätzen 1, 2 und 3 verpflichtet, wenn der Teilnehmer die Sperranzeige nach Nummer 8.1 nicht abgeben konnte, weil die Bank nicht die Möglichkeit zur Entgegennahme der Sperranzeige sichergestellt hatte und der Schaden dadurch eingetreten ist.

(4) Kommt es vor der Sperranzeige zu nicht autorisierten Zahlungsvorgängen und hat der Teilnehmer seine Sorgfaltspflichten nach diesen Bedingungen vorsätzlich oder grob fahrlässig verletzt oder in betrügerischer Absicht gehandelt, trägt der Kontoinhaber den hierdurch entstandenen Schaden in vollem Umfang. Grobe Fahrlässigkeit des Teilnehmers kann insbesondere dann vorliegen, wenn er

- den Verlust oder Diebstahl des Authentifizierungsinstruments oder die missbräuchliche Nutzung des Authentifizierungsinstruments oder des personalisierten Sicherheitsmerkmals der Bank nicht unverzüglich anzeigt, nachdem er hiervon Kenntnis erlangt hat (vgl. Nummer 8.1 Absatz 1),
- das personalisierte Sicherheitsmerkmal im Kundensystem gespeichert hat (vgl. Nummer 7.2 Absatz 2, 1. Spiegelstrich),
- das personalisierte Sicherheitsmerkmal einer anderen Person mitgeteilt und der Missbrauch dadurch verursacht wurde (vgl. Nummer 7.2 Absatz 1, 2. Spiegelstrich),
- das personalisierte Sicherheitsmerkmal außerhalb des Online-Banking-Verfahrens, beispielsweise per E-Mail, weitergegeben hat (vgl. Nummer 7.2 Absatz 2, 4. Spiegelstrich),
- das Personalisierte Sicherheitsmerkmal auf dem Authentifizierungsinstrument vermerkt oder zusammen mit diesem verwahrt hat (vgl. Nummer 7.2 Absatz 2, 5. Spiegelstrich),

(5) Die Haftung für Schäden, die innerhalb des Zeitraums, für den der Verfügungsrahmen gilt, verursacht werden, beschränkt sich jeweils auf den vereinbarten Verfügungsrahmen.

10.2.2 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.

11. Speicherung der Kundendaten

Aufgrund der gesetzlichen Anforderungen werden die Kundendaten von der Bank zum Zweck der Vertragserfüllung gespeichert.

12. Außergerichtliche Streitschlichtung und sonstige Beschwerdemöglichkeit

Für die Beilegung von Streitigkeiten mit der Bank kann sich der Teilnehmer an die in den allgemeinen Geschäftsbedingungen näher bezeichneten Streitschlichtungs- oder Beschwerdestellen wenden.

13. Kommunikation mit der Bank

13.1 Der elektronische Posteingang

Im Rahmen der Geschäftsbeziehung zwischen der Bank und dem Kunden gilt der elektronische Posteingang (Online-Banking-Konto) als Kanal, über den der Kunde Dokumente in elektronischer Form an die Bank übermitteln kann (z. B. Kontoauszüge, Finanzberichte und andere Informationen), außer wenn die fraglichen Dokumente die schriftliche Form erfordern. Bei Registrierung zum Online-Banking werden Dokumente und Mitteilungen über aktuelle und zukünftige Konten im elektronischen Posteingang des Kunden abgelegt. Wenn der Kunde den elektronischen Posteingang für bestimmte Konten nicht benutzen will, kann die Bank für diese Konten einen anderen Versandkanal genehmigen. Die Nutzung anderer Kanäle ist jedoch gebührenpflichtig.

13.2. Verzicht auf papierbasierte Zustellung

Mit Aktivierung des elektronischen Posteingangs verzichtet der Kunde gemäß diesen Bedingungen ausdrücklich auf

die Zustellung der Nachrichten auf dem Postweg. Die Bank ist jedoch berechtigt, dem Kunden Papierdokumente auf dem Postweg zu senden, zum Beispiel um gesetzliche Verpflichtungen zu erfüllen, oder wenn die Bank dies unter Berücksichtigung des Kundeninteresses als angebracht erachtet.

13.3 Übermittlung der Konto- und Kundendokumente und Mitwirkungspflicht des Kunden

Die Bank stellt dem Kunden Mitteilungen, die sich auf die Geschäftsaktivitäten mit der Bank beziehen, in elektronischer Form als Dateien zur Verfügung. Dies gilt auch für Anlagen. Der Kunde ist verpflichtet, seine Dokumente regelmäßig aus dem elektronischen Posteingang abzurufen, sie umgehend auf Korrektheit und Vollständigkeit zu prüfen und etwaige Einsprüche unverzüglich zu erheben.

13.4 Zugang

Die Nachrichten von der Bank an den elektronischen Posteingang gelten als zugegangen, sobald diese eingegeben

wurden und der Kunde die Möglichkeit hatte, sie abzurufen.

13.5. Speicherung von Dokumenten

Die Bank speichert die Informationen im elektronischen Posteingang für die Dauer der gesetzlichen Aufbewahrungsfristen. Nach dieser Frist kann die Bank diese Information aus dem elektronischen Posteingang löschen, ohne dem Kunden eine separate Benachrichtigung hierüber zu senden.

14. Geschäftsbedingungen

Die allgemeinen Geschäftsbedingungen und die jeweiligen Sonderbedingungen des Produkts sind als Ergänzung dieser Sonderbedingungen zu verstehen.