Bedingungen für die Nutzung des Online-Banking durch natürliche Personen (Fassung vom 01.02.2023)

1. Leistungsangebot
(1) Der Kontoinhaber kann Bankgeschäfte mittels Online-Banking in dem von der Bausparkasse Mainz AG, nachstehend BKM genannt, angebotenen Umfang abwickeln. Zudem kann er Informationen der BKM mittels Online-Banking abrufen.
(2) Kontoinhaber und Bevollmächtigte werden im Folgenden einheitlich und geschlechtsneutral als „Teilnehmer" bezeichnet.
(3) Das Online-Banking kann nur von im eigenen Namen handelnden, voll geschäftsfähigen natürlichen Personen genutzt werden. Bei Gemeinschaftskonten können die Teilnehmer Informationen abrufen, jedoch im Rahmen des Online-Banking keine Aufträge erteilen.
(4) Die jeweiligen Produktbedingungen (Bedingungen für Geldanlagen nebst Sonderbedingungen, Allgemeine Bedingungen für Bausparverträge sowie Allgemeine Darlehensbedingungen bzw. Darlehensbedingungen) gelten jeweils unabhängig von dem Inhalt dieser Bedingungen auch für das Online-Banking.

2. Voraussetzungen zur Nutzung des Online-Banking
(1) Der Teilnehmer kann das Online-Banking nutzen, wenn die BKM ihn authentifiziert hat.
(2) Authentifizierung ist das mit der BKM gesondert vereinbarte Verfahren, mit dessen Hilfe die BKM die Identität des Teilnehmers oder die berechtigte Verwendung eines vereinbarten Zahlungsinstrumentes, einschließlich der Verwendung des Personalisierten Sicherheitsmerkmals des Teilnehmers überprüfen kann. Mit den hierfür vereinbarten Authentifizierungselementen kann der Teilnehmer sich gegenüber der BKM als berechtigter Teilnehmer ausweisen, auf Informationen zugreifen (siehe Nummer 3 dieser Bedingungen) sowie Aufträge erteilen (siehe Nummer 4 dieser Bedingungen).
(3) Authentifizierungselemente sind
– Wissenselemente, also etwas, das nur der Teilnehmer weiß (z. B. persönliche Identifikationsnummer (PIN) oder der Nutzungscode für eine elektronische Signatur)
– Besitzelemente, also etwas, das nur der Teilnehmer besitzt (z. B. Gerät zur Erzeugung oder zum Empfang von einmal verwendbaren Transaktionsnummern (TAN), die den Besitz des Teilnehmers nachweisen, wie ein mobiles Endgerät, sowie
– 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 BKM das Wissenselement, den Nachweis des Besitzelements und/oder den Nachweis des Seinselements an die BKM übermittelt.

3. Zugang zum Online-Banking
Der Teilnehmer erhält Zugang zum Online-Banking, wenn
– dieser seine individuelle Kennung und seine PIN übermittelt hat,
– die Prüfung dieser Daten bei der BKM 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.

4. Online-Banking-Aufträge und Autorisierung
Der Teilnehmer muss Online-Banking-Aufträge (zum Beispiel Überweisungen) zu deren Wirksamkeit mit dem vereinbarten personalisierten Sicherheitsmerkmal (TAN) autorisieren und der BKM mittels Online-Banking übermitteln. Die BKM bestätigt mittels Online-Banking den Eingang des Auftrags.

5. Bearbeitung von Online-Banking-Aufträgen durch die BKM
(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 BKM bekannt gegebenen Geschäftstagen im Rahmen des ordnungsgemäßen Arbeitsablaufes. Geht der Auftrag nach dem auf der Online-Banking-Seite der BKM angegebenen bestimmten Zeitpunkt (Annahmefrist) ein oder fällt der Zeitpunkt des Eingangs nicht auf einen Geschäftstag der BKM, so gilt der Auftrag als am darauf folgenden Geschäftstag zugegangen. Die Bearbeitung beginnt erst an diesem Tag.
(2) Die BKM 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.
Liegen die Ausführungsbedingungen nach Satz 1 vor, führt die BKM die Online-Banking-Aufträge aus.
(3) Liegen die Ausführungsbedingungen nach Absatz 2 Satz 1 nicht vor, wird die BKM den Online-Banking-Auftrag nicht ausführen und dem 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, eine Information zur Verfügung stellen.

6. Sorgfaltspflichten des Teilnehmers
6.1. Technische Verbindung zum Online-Banking
Der Teilnehmer ist verpflichtet, die technische Verbindung zum Online-Banking nur über die von der BKM gesondert mitgeteilten Online-Banking-Zugangskanäle (zum Beispiel Internetadresse) herzustellen.
6.2. Geheimhaltung der personalisierten Sicherheitsmerkmale und sichere Aufbewahrung der Authentifizierungsinstrumente
(1) Der Teilnehmer hat
– seine personalisierten Sicherheitsmerkmale (siehe Nummer 2.1) geheim zu halten und nur über die von der BKM gesondert mitgeteilten Online-Banking-Zugangskanäle an diese zu übermitteln 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 dem dazugehörigen personalisierten Sicherheitsmerkmal 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 (zum Beispiel im Kundensystem).
– Bei Eingabe des personalisierten Sicherheitsmerkmals ist sicherzustellen, dass andere Personen dieses nicht ausspähen können.
– Das personalisierte Sicherheitsmerkmal darf nicht außerhalb der gesondert mitgeteilten BKM-Onlinebanking-Seite eingegeben werden (zum Beispiel nicht auf Online-Händlerseiten).
– Das personalisierte Sicherheitsmerkmal darf nicht außerhalb des Online-Banking-Verfahrens weitergegeben werden, also beispielsweise nicht per E-Mail.
– Die PIN darf nicht zusammen mit dem Authentifizierungsinstrument verwahrt werden.
– Der Teilnehmer darf zur Autorisierung zum Beispiel eines Auftrags, der Aufhebung einer Sperre oder zur Freischaltung eines neuen TAN-Generators nicht mehr als eine TAN verwenden.
6.3. Sicherheit des Kundensystems
Der Teilnehmer muss die Sicherheitshinweise auf der Internetseite der BKM zum Online-Banking, insbesondere die Maßnahmen zum Schutz der eingesetzten Hard- und Software (Kundensystem), beachten.
6.4. Kontrolle der Auftragsdaten mit von der BKM angezeigten Daten
Soweit die BKM 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.

7. Anzeige- und Unterrichtungspflichten
7.1. 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 persönlichen Sicherheitsmerkmals fest, muss der Teilnehmer die BKM hierüber unverzüglich unterrichten (Sperranzeige).
(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.
7.2. Unterrichtung über nicht autorisierte oder fehlerhaft ausgeführte Aufträge
Der Kontoinhaber hat die BKM unverzüglich nach Feststellung eines nicht autorisierten oder fehlerhaft ausgeführten Auftrags hierüber zu unterrichten.

8. Nutzungssperre
8.1. Sperre auf Veranlassung des Teilnehmers
Die BKM sperrt auf Veranlassung des Teilnehmers, insbesondere im Fall der Sperranzeige nach Nummer 7.1.
– den Online-Banking-Zugang für ihn oder alle Teilnehmer oder
– sein Authentifizierungsinstrument.
8.2. Sperre auf Veranlassung der BKM
(1) Die BKM 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 BKM wird den Kontoinhaber unter Angabe der hierfür maßgeblichen Gründe möglichst vor, spätestens jedoch unverzüglich nach der Sperre unterrichten.
8.3. Aufhebung der Sperre
Die BKM wird eine Sperre aufheben oder das personalisierte Sicherheitsmerkmal beziehungsweise das Authentifizierungsinstrument austauschen, wenn die Gründe für die Sperre nicht mehr gegeben sind. Hierüber unterrichtet sie den Kontoinhaber unverzüglich.

J 384 – 02/2023

9. Haftung

9.1. Haftung bei einer nicht autorisierten Online-Banking-Verfügung und einer nicht oder fehlerhaft ausgeführten Online-Banking-Verfügung

Der Kunde haftet für alle Schäden, die er durch unsachgemäße und missbräuchliche Verwendung der von ihm festgelegten und der BKM als verbindlich mitgeteilten personalisierten Sicherheitsmerkmale oder des Authentifizierungsinstruments bzw. die Nichtbeachtung dieser Bedingungen verschuldet hat oder die daraus entstehen, dass ein unberechtigter Dritter durch ihn von dem Sicherheitsmerkmal oder den Authentifizierungsinstrumenten Kenntnis erlangt hat. Die Haftung des Kunden entfällt für alle Schäden, die entstehen, nachdem der Kunde die BKM davon benachrichtigt hat, dass ein Dritter Kenntnis von dem Sicherheitsmerkmal oder den Authentifizierungsinstrumenten erhalten hat oder ein entsprechender Verdacht besteht. Ab diesem Zeitpunkt übernimmt die BKM die durch unsachgemäße oder missbräuchliche Verwendung des Sicherheitsmerkmals oder der Authentifizierungsinstrumente entstehenden Schäden. Bei Schäden aus Übermittlungsfehlern, Missverständnissen und Irrtümern bei der Abwicklung des Online-Banking haftet die BKM nur für grobe Fahrlässigkeit und Vorsatz und nur in dem Maße, wie sie im Verhältnis zu anderen Ursachen an der Entstehung des Schadens mitgewirkt hat. In jedem Falle einer Haftung der BKM ist diese auf die für die BKM vorhersehbaren typischen Schäden sowie auf den Ersatz des unmittelbaren Schadens unter Ausschluss einer Haftung für Folgeschäden, insbesondere entgangenen Gewinn, begrenzt.

9.2. Haftung des Kontoinhabers bei missbräuchlicher Nutzung seines Authentifizierungsinstruments

9.2.1. 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 abhanden gekommenen Authentifizierungsinstruments, haftet der Kontoinhaber für den der Bank hierdurch entstehenden Schaden bis zu einem Betrag von 150,- Euro, ohne dass es darauf ankommt, ob den Teilnehmer an dem Verlust, Diebstahl oder sonstigen 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 abhanden gekommen ist, haftet der Kontoinhaber für den der BKM 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) Ist der Kontoinhaber kein Verbraucher, haftet er für Schäden aufgrund von nicht autorisierten Zahlungsvorgängen über die Haftungsgrenze von 150,– Euro nach Absatz 1 und 2 hinaus, wenn der Teilnehmer fahrlässig oder vorsätzlich gegen seine Anzeige- und Sorgfaltspflichten nach diesen Bedingungen verstoßen hat.

(4) 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 angeben konnte, weil die BKM nicht die Möglichkeit zur Entgegennahme der Sperranzeige sichergestellt hatte und der Schaden dadurch eingetreten ist.

(5) 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 vorliegen, wenn er

- den Verlust oder Diebstahl des Authentifizierungsinstruments oder die missbräuchliche Nutzung des Authentifizierungsinstruments oder des personalisierten Sicherheitsmerkmals der BKM nicht unverzüglich anzeigt, nachdem er hiervon Kenntnis erlangt hat (siehe Nummer 7.1 Absatz 1),
- das personalisierte Sicherheitsmerkmal im Kundensystem gespeichert hat (siehe Nummer 6.2 Absatz 2 1. Spiegelstrich),
- das personalisierte Sicherheitsmerkmal einer anderen Person mitgeteilt hat und der Missbrauch dadurch verursacht wurde (siehe Nummer 6.2 Absatz 2 2. Spiegelstrich),
- das personalisierte Sicherheitsmerkmal erkennbar außerhalb der gesondert vereinbarten Internetseiten eingegeben hat (siehe Nummer 6.2 Absatz 2 3. Spiegelstrich),
- das personalisierte Sicherheitsmerkmal außerhalb des Online-Banking-Verfahrens, beispielsweise per E-Mail, weitergegeben hat (siehe Nummer 6.2. Absatz 2 4. Spiegelstrich),
- das personalisierte Sicherheitsmerkmal auf dem Authentifizierungsinstrument vermerkt oder zusammen mit diesem verwahrt hat (siehe Nummer 6.2 Absatz 2 5. Spiegelstrich),
- mehr als eine TAN zur Autorisierung eines Auftrags verwendet hat (siehe Nummer 6.2 Absatz 2 6. Spiegelstrich).

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

9.2.2. Haftung der BKM ab der Sperranzeige

Sobald die BKM 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.

9.2.3. 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.