AKBANK AG

English translation is merely for information purposes and not legally binding. It should only be interpreted as an attempt to help understand the German version of the Terms & Conditions. The German version is legally binding.

Sonderbedingungen für die Teilnahme am Onlinebanking und Mobilebanking der Akbank AG

1.Leistungsangebot

(1) Der Kontoinhaber kann Bankgeschäfte mittels Onlinebanking in dem von der Bank angebotenen Umfang abwickeln. Zusätzlich 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

(1) Der Kontoinhaber benötigt für die Abwicklung von Bankgeschäften mittels Onlinebanking die mit der Bank vereinbarten personalisierten Sicherheitsmerkmale und Authentifizierungsinstrumente (Passwort und PIN), um sich gegenüber der Bank als berechtigter Kontoinhaber ausweisen und auf Informationen zugreifen und Aufträge autorisieren zu können.

(2) Personalisierte Sicherheitsmerkmale, die auch alphanumerisch sein können, sind (i) die persönliche Identifikationsnummer (PIN), (ii) einmal verwendbare Transaktionsnummern (TAN), (iii) der Nutzungscode für die elektronische Signatur.

(3) Die TAN beziehungsweise die elektronische Signatur können dem Kontoinhaber auf folgenden Authentifizierungsinstrumenten zur Verfügung gestellt werden: (i) auf einer Liste mit einmal verwendbaren TAN, (ii) mittels eines TAN-Generators, der Bestandteil einer Chipkarte oder eines anderen elektronischen Gerätes zur Erzeugung von TAN ist, (iii) mittels eines mobilen Endgerätes zum Empfang von TAN per SMS (mobileTAN), (iv) auf einer Chipkarte mit Signaturfunktion oder (iv) auf einem sonstigen Authentifizierungsinstrument, auf dem sich Signaturschlüssel befinden. Für eine Chipkarte benötigt der Kundeninhaber zusätzlich ein geeignetes Lesegerät.

(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. Die Bank behält sich vor, diesen Verschlüsselungsstandard jederzeit zu ändern. Über eine Änderung des Verschlüsselungsstandards wird die Bank den Kontoinhaber durch eine vorherige Mitteilung im Internet unterrichten. Das Onlinebanking ist zurzeit für die Nutzung mit den Internet Browsern Explorer und Firefox optimiert. Die Nutzbarkeit mit anderen Browsern kann nicht gewährleistet werden.

3.Zugang zum Onlinebanking

(1) Im Rahmen der Erstaktivierung des Onlinebanking wird dem Kontoinhaber postalisch eine Benutzer-ID (=Kundennummer) und ein Passwort mittgeteilt. Nach erstmaliger Eingabe dieses Passwortes wird der Kontoinhaber aufgefordert ein persönliches Passwort festzulegen.

(2) Nach erfolgreicher Erstaktivierung erhält der Kontoinhaber Zugang zum Onlinebanking, nachdem er seine Benutzer-ID (=Kundennummer) und das persönliche Passwort auf der Onlinebanking-Seite der Bank (akbank.de) eingegeben hat. Der Kontoinhaber erhält Zugang zum Onlinebanking, wenn die Prüfung dieser Daten bei der Bank eine Zugangsberechtigung ergeben hat und keine Sperre des Zugangs vorliegt.

(3) Der Kontoinhaber ist berechtigt, seine PIN und/oder sein Passwort jederzeit zu ändern. Bei Änderung dieser Zugangsdaten verlieren seine bisherigen Zugangsdaten ihre Gültigkeit.

4.Auftragsabwicklung im Rahmen des Onlinebankings

(1) Der Kontoinhaber muss seine Onlinebanking-Aufträge, damit sie Wirksamkeit erlangen, mit dem vereinbarten personalisierten Sicherheitsmerkmal (PIN) autorisieren und der Bank mittels Onlinebanking übermitteln. Die Bank bestätigt mittels Onlinebanking den Eingang des Auftrags. Andere Erklärungen, die keiner Autorisierung durch ein personalisiertes Sicherheitsmerkmal bedürfen, gelten gegenüber der Bank als wirksam abgegeben, wenn der Nutzungsberechtigte, die in der Benutzerführung vorgeschriebene Freigabe zur Übermittlung an die Bank vorgenommen hat.

(2) Die Bank wird den Auftrag ausführen, wenn (i) der Kundeninhaber sich mit seinem personalisierten Sicherheitsmerkmal legitimiert hat, (ii) die Berechtigung des Kontoinhabers für den jeweiligen Auftrag vorliegt, (iii) das Onlinebanking-Datenformat eingehalten ist, (iv) das gesondert vereinbarte Onlinebanking-Verfügungslimit nicht überschritten ist, (v) die Ausführungsvoraussetzungen nach den für die jeweilige Auftragsart maßgeblichen Sonderbedingungen (z. B. Sonderbedingungen für das Tages- und Festgeldkonto) vorliegt.

Special conditions for participation in Akbank AG Online Banking and Mobile Banking channels

1.Service offer

(1) The account holder can carry out banking transactions using online banking to the extent offered by the bank. In addition, he can call up information from the bank via online banking.

(2) The account holder is the authorized user of the bank's online banking offer. Authorization of other persons to use the online banking offer instead of the account holder, is not possible.

2. Prerequisites for using online banking

(1) In order to process banking transactions via online banking, the account holder needs the personalized security features and authentication tools (password and PIN) agreed with the bank in order to identify himself to the bank as an authorized account holder and to be able to access information and authorize orders.

(2) Personalized security features, which can also be alphanumeric, are (i) the personal identification number (PIN), (ii) one-time use transaction numbers (TAN), (iii) the usage code for the electronic signature.

(3) The TAN or the electronic signature can be made available to the account holder on the following authentication instruments: (i) on a list of single-use TANs, (ii) using a TAN generator, which is part of a chip card or another electronic device for generating TANs (iii) using a mobile device to receive TANs via SMS (mobileTAN), (iv) on a chip card with a signature function or (iv) on another authentication instrument on which signature keys are located. The customer owner also needs a suitable reader for a chip card.

(4) Internet access is required to use online banking. This internet access is not provided by the bank. Online banking currently requires a browser that supports at least 128-bit SSL encryption. The bank reserves the right to change this encryption standard at any time. The bank will inform the account holder of a change in the encryption standard by prior notification on the Internet. Online banking is currently optimized for use with the Internet browsers Explorer and Firefox. Usability with other browsers cannot be guaranteed.

3. Access to online banking

(1) As part of the initial activation of online banking, the account holder will be sent a user ID (= customer number) and a password by post. After entering this password for the first time, the account holder will be asked to set a personal password.

(2) After successful initial activation, the account holder gains access to online banking after entering their user ID (= customer number) and personal password on the bank's online banking site (akbank.de). The account holder is granted access to online banking if the bank's examination of this data has resulted in access authorization and the access has not been blocked.

(3) The account holder is entitled to change his PIN and/or his password at any time. If these access data are changed, the previous access data will lose their validity.

4. Order processing within the framework of online banking

(1) In order for them to become effective, the account holder must authorize his online banking orders with the agreed personalized security feature (PIN) and transmit them to the bank via online banking. The bank confirms receipt of the order via online banking. Other declarations that do not require authorization by means of a personalized security feature are deemed to have been given to the Bank as effective if the authorized user has given the approval for transmission to the Bank as stipulated in the user guide.

(2) The bank will execute the order if (i) the customer owner has identified himself with his personalized security feature, (ii) the account holder is authorized for the respective order, (iii) the online banking data format has been complied with, (iv) the separately agreed online banking disposal limit has not been exceeded, (v) the execution requirements according to the special conditions applicable to the respective order type (e.g. special conditions for the current and time deposit account) are met.

(3) Liegen die oben genannten Ausführungsbedingungen nicht vor, wird die Bank den Onlinebanking-Auftrag nicht ausführen und dem Kontoinhaber über die Nichtausführung und soweit möglich über deren Gründe und die Möglichkeiten, mit denen Fehler, die zur Ablehnung geführt haben, berichtigt werden können, mittels Onlinebanking eine Information zur Verfügung stellen.

(4) Die Widerrufbarkeit eines Onlinebanking-Auftrages richtet sich nach den für die jeweilige Auftragsart geltenden Sonderbedingungen (z. B. Sonderbedingungen für das Tages- und Festgeldkonto). Der Widerruf von Aufträgen kann nur außerhalb des Onlinebanking erfolgen, es sei denn, die Bank sieht eine Widerrufsmöglichkeit im Onlinebanking ausdrücklich vor.

(5) Die Bearbeitung der Onlinebanking-Aufträge erfolgt an den für die Abwicklung der jeweiligen Auftragsart (z. B. Überweisung auf das Referenzkonto) 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.

5.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.

6.Sorgfaltspflichten des Kontoinhabers

6.1 Technische Verbindung zum Onlinebanking

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

6.2 Sicherheit des Kundensystems

Der Kontoinhaber hat die Sicherheitshinweise auf der Internetseite der Bank zum Onlinebanking, insbesondere die Maßnahmen zum Schutz der eingesetzten Hard- und Software (Kundensystem), zu beachten. Hierzu gehören insbesondere die Installation und regelmäßige Aktualisierung einer handelsüblichen Antivirensoftware, die Installation einer Firewall sowie regelmäßige Sicherheits-Updates für den vom Kontoinhaber verwendeten Browser.

6.3 Geheimhaltung und sichere Aufbewahrung der Zugangsdaten

(1) Der Kontoinhaber ist verpflichtet:

- seine personalisierten Sicherheitsmerkmale geheim zu halten und nur über die von der Bank zur Verfügung gestellten Onlinebanking-Zugangskanäle an diese zu übermitteln.
- sein Authentifizierungsinstrument 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 Onlinebanking-Verfahren missbräuchlich nutzen.

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

- Das personalisierte Sicherheitsmerkmal darf nicht ungesichert elektronisch gespeichert werden.
- Bei Eingabe des personalisierten Sicherheitsmerkmals ist sicherzustellen, dass andere Personen diese nicht ausspähen können.
- Das personalisierte Sicherheitsmerkmal darf nicht außerhalb des Onlinebanking-Verfahrens weitergegeben werden (z.B. nicht per E-Mail, telefonisch oder persönlich).
- Das personalisierten Sicherheitsmerkmal darf nicht zusammen mit dem Authentifizierungsinstrument verwahrt werden, also beispielsweise nicht per E-Mail.

6.4 Kontrolle der Auftragsdaten mit von der Bank angezeigten Daten

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

(3) If the above conditions for execution are not met, the Bank will not execute the online banking order and will inform the account holder via online banking about the non-execution and, as far as possible, about the reasons for this and the possibilities for correcting errors that led to the refusal provide information.

(4) The revocability of an online banking order depends on the special conditions applicable to the respective order type (e.g. special conditions for the current and time deposit account). Orders can only be revoked outside of online banking, unless the Bank expressly provides a revocation option in online banking.

(5) Online banking orders are processed on the business days specified for the processing of the respective order type (e.g. transfer to the reference account) on the Bank’s online banking page or in the “List of Prices and Services” as part of the regular workflow. If the order is received after the time specified on the Bank’s online banking site or specified in the “List of Prices and Services” (acceptance period) or if the time of receipt does not fall on a business day according to the Bank’s “List of Prices and Services”, the order as received on the following business day. Processing then only begins on this day.

5.Information of the account holder about online banking transactions

The bank will inform the account holder at least once a month about the transactions made via online banking via the agreed account information channel.

6.Account Holder Due Diligence

6.5 Technical connection to online banking

The account holder is obliged to establish the technical connection to online banking only via the online banking access channels (internet address) provided by the bank.

6.6 Customer System Security

The account holder must observe the security instructions on the Bank's website for online banking, in particular the measures to protect the hardware and software used (customer system). This includes in particular the installation and regular updating of commercial antivirus software, the installation of a firewall and regular security updates for the browser used by the account holder.

6.7 Secrecy and secure storage of access data

(3) The account holder is obliged to:

- to keep his personalized security credentials secret and to only transmit them to the bank via the online banking access channels provided by the bank.
- to keep his authentication instrument safe from access by other people.
- Because any other person who is in possession of the authentication tool can misuse the online banking process in connection with the associated personalized security feature.

(4) In particular, the following must be observed to protect the personalized security feature and the authentication tool:

- The personalized security feature must not be stored electronically in an unsecured manner.
- When entering the personalized security feature, it must be ensured that other people cannot spy on it.
- The personalized security feature must not be passed on outside of the online banking process (e.g. not by e-mail, by telephone or in person).
- The personalized security feature must not be kept together with the authentication tool, e.g. not by e-mail.

6.8 Control of the order data with data displayed by the bank

If the bank shows the account holder data from his online banking order (e.g. amount and/or account number of the payee) in the customer system or via another device of the account holder (e.g. mobile phone) for confirmation, the account holder is obliged to confirm the to check that the data displayed matches the data intended for the transaction.

7.Anzeige- und Unterrichtungspflichten

7.1 Sperranzeige

(7) Stellt der Kontoinhaber (i) den Verlust oder den Diebstahl des Authentifizierungsinstruments, (ii) die missbräuchliche Verwendung oder die sonstige nicht autorisierte Nutzung seines Authentifizierungsinstruments oder seines persönlichen Sicherheitsmerkmals fest, ist der Kontoinhaber verpflichtet, dies der Bank unverzüglich mitzuteilen (Sperranzeige).

(8) Der Kontoinhaber hat jeden Diebstahl oder Missbrauch unverzüglich bei der Polizei anzuzeigen.

(9) Hat der Kontoinhaber den Verdacht, dass eine andere Person unberechtigt den Besitz an seinem Authentifizierungsinstrument oder die Kenntnis seines personalisierten Sicherheitsmerkmals erlangt hat, muss er ebenfalls eine Sperranzeige abgeben.

7.2 Unterrichtung über nicht autorisierte oder fehlerhaft ausgeführte Aufträge

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

8. Nutzungssperre

8.9 Sperre auf Veranlassung des Kontoinhabers

Die Bank sperrt auf Veranlassung des Kontoinhabers, insbesondere im Fall der Sperranzeige nach Nr. 7.1 unverzüglich den Onlinebanking-Zugang oder sein Authentifizierungsinstrument.

8.10 Sperre auf Veranlassung der Bank

(5) Der Onlinebanking-Zugang wird von der Bank gesperrt werden, wenn

- sie berechtigt ist, die Onlinebanking-Vereinbarung aus wichtigem Grund zu kündigen,
- sachliche Gründe im Zusammenhang mit der Sicherheit des Authentifizierungsinstruments oder des Personalisierten Sicherheitsmerkmals dies rechtfertigen,
- der Verdacht einer nicht autorisierten oder einer betrügerischen Verwendung hinsichtlich des Authentifizierunginstruments besteht,
- der Kontoinhaber sich 6 Monate lang nicht in das Onlinebanking mit den mit der Bank vereinbarten Zugangsdaten einloggt.

(6) Die Bank wird den Kontoinhaber unter Angabe der hierfür maßgeblichen Gründe möglichst vor, jedoch spätestens unverzüglich nach der Sperre unterrichten.

8.11 Automatische Sperre des Zugangs

Der Onlinebanking-Zugang wird von Seiten der Bank gesperrt, wenn dreimal hintereinander das personalisierte Sicherheitsmerkmal falsch eingegeben wird.

8.12 Aufhebung der Sperre

Die Bank 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.

9.Haftung

9.1. Haftung der Bank bei einer nicht autorisierten Onlinebanking-Verfügung und einer nicht oder fehlerhaft ausgeführten Onlinebanking-Verfügung

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

9.2 Haftung des Kontoinhabers bei missbräuchlicher Nutzung seines Authentifizierungsinstruments

9.2.1 Haftung des Kontoinhabers für nicht autorisierte Onlinebanking-Verfügungen vor der Sperranzeige

(9) Beruhen nicht autorisierte Onlinebanking-Verfügungen 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 150 Euro. Der Kontoinhaber haftet nicht, wenn es ihm nicht möglich gewesen ist, den Verlust, den Diebstahl, das Abhandenkommen oder eine sonstige missbräuchliche Verwendung des Authentizifierungsinstruments vor der nicht autorisierten Onlinebanking-Verfügung zu bemerken oder wenn die der Verlust durch einen Mitarbeiter oder sonstigen Vertreter oder Erfüllungsgehilfen der Bank versucht worden ist.

7. Reporting and Informing Obligations

7.1 Blocking notification

(1) If the account holder discovers (i) the loss or theft of the authentication tool, (ii) misuse or other unauthorized use of his authentication tool or personal security feature, the account holder is obliged to notify the Bank of this immediately (blocking notification).

(2) The account holder must report any theft or misuse to the police immediately.

(3) If the account holder suspects that another person has unauthorized possession of his authentication tool or knowledge of his personalized security feature, he must also submit a blocking notification.

7.2 Notification of Unauthorized or Incorrectly Executed Orders

The account holder must inform the bank immediately after discovering an unauthorized or incorrectly executed order.

8. Blocking of use

8.1 Blocking by account holder

At the instigation of the account holder, the Bank will immediately block the online banking access or its authentication instrument, particularly in the case of a blocking notification in accordance with Nr. 7.1.

8.2 Blocking at the instigation of the bank

(1) Online banking access will be blocked by the bank if

- it is entitled to terminate the online banking agreement for good cause,
- objective reasons in connection with the security of the authentication tool or the personalized security feature justify this,
- there is a suspicion of unauthorized or fraudulent use of the authentication tool,
- the account holder does not log into online banking with the access data agreed with the bank for 6 months.

(2) The bank will inform the account holder, stating the relevant reasons, if possible before, but at the latest immediately after, the blocking.

8.3 Automatic blocking of access

Online banking access will be blocked by the bank if the personalized security feature is entered incorrectly three times in a row.

8.4 Unblocking

The bank will remove a block or replace the personalized security feature or the authentication tool if the reasons for the block no longer apply. It shall inform the account holder of this immediately.

9. Liability

9.1 Liability of the bank in the event of unauthorized online banking transactions and online banking transactions that are not executed or are executed incorrectly

The liability of the bank in the event of an unauthorized online banking transaction and an online banking transaction that is not carried out or is carried out incorrectly is based on the special conditions agreed for the respective type of order (e.g. special conditions for the current and time deposit account).

9.2 Liability of the account holder in the event of misuse of his authentication instrument

9.2.1 Liability of the account holder for unauthorized online banking transactions prior to the blocking notification

(1) If unauthorized online banking transactions prior to the blocking notification are based on the use of a lost, stolen or otherwise misplaced authentication instrument or on the other misuse of an authentication instrument, the account holder is liable for the damage incurred by the bank up to an amount of 150 Euro. The account holder is not liable if it was not possible for him to notice the loss, theft, misplacement or other misuse of the authentication instrument prior to the unauthorized online banking transaction or if the loss was caused by an employee or other representative or vicarious agent the bank has been attempted.

(2) Ist der Kontoinhaber kein Verbraucher, haftet er für Schäden aufgrund von nicht autorisierten Onlinebanking-Verfügungen über die Haftungsgrenze von 150 Euro nach Absatz 1 und 2 hinaus, wenn der Kontoinhaber fahrlässig oder vorsätzlich gegen seine Anzeige- oder Sorgfaltspflichten verstoßen hat.

(3) Der Kontoinhaber ist nicht zum Ersatz des Schadens nach den Absätzen 1, 2 und 3 verpflichtet, wenn der Kontoinhaber die Sperranzeige nach Nr. 9.1 nicht abgeben konnte, weil die Bank nicht die Möglichkeit zur Entgegennahme der Sperranzeige sichergestellt hatte und der Schaden hierdurch eingetreten ist.

(4) Kommt es vor der Sperranzeige zu nicht autorisierten Onlinebanking-Verfügungen und hat der Kontoinhaber seine Sorgfaltspflichten nach diesen Bedingungen vorsätzlich oder grob fahrlässig verletzt, oder in betrügerischer Absicht gehandelt, trägt der Kontoinhaber 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 des personalisierten Sicherheitsmerkmals der Bank nicht unverzüglich anzeigt, nachdem er hiervon Kenntnis erlangt hat,
- das personalisierte Sicherheitsmerkmal einer dritten Person mitgeteilt hat und der Missbrauch dadurch verursacht wurde,
- das personalisierte Sicherheitsmerkmal ungesichert elektronisch gespeichert hat,
- das personalisierte Sicherheitsmerkmal nicht geheim gehalten hat und der Missbrauch dadurch verursacht wurde,
- das personalisierte Sicherheitsmerkmal außerhalb des Onlinebanking-Verfahrens, beispielsweise per E-Mail, weitergegeben hat,
- das personalisierte Sicherheitsmerkmal auf dem Authentifizierungsinstrument vermerkt oder beide gemeinsam aufbewahrt hat.

9.2.2 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.

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.

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

Datenschutz 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.

11. Mobile Banking

Die vorstehenden Bedingungen zur Teilnahme am Online-Baniking gelten entsprechend für das Mobile-Banking. Unter Mobile-Banking ist die Nutzung des Konto unter Nutzung mobiler Endgeräte (z.B. über WAP – Wireless Application Protocol) zu verstehen.

12.Geschäftsbedingungen

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

(2) If the account holder is not a consumer, he is liable for damages due to unauthorized online banking transactions beyond the liability limit of 150 Euro according to paragraphs 1 and 2 if the account holder has negligently or intentionally violated his duty of disclosure or due diligence.

(3) The account holder is not obliged to compensate for the damage according to paragraphs 1, 2 and 3 if the account holder was unable to submit the blocking notification according to No. 9.1 because the bank had not ensured the possibility of receiving the blocking notification and the damage occurred as a result.

(4) If unauthorized online banking transactions occur before the blocking notification and the account holder has intentionally or grossly negligently violated his duty of care according to these conditions, or acted with fraudulent intent, the account holder shall bear the full extent of the damage incurred as a result. Gross negligence on the part of the account holder may exist in particular if he:

- fails to report the loss or theft of the authentication tool or misuse of the authentication tool or personalized security feature to the Bank immediately after becoming aware of it,
- has communicated the personalized security feature to a third party and the misuse was caused by this,
- stored the personalized security feature electronically in an unsecured manner,
- did not keep the personalized security feature secret and the misuse was caused by this,
- has passed on the personalized security feature outside of the online banking process, for example by e-mail,
- noted the personalized security feature on the authentication instrument or kept both together.

9.2.2 Liability of the bank from the blocking notification

As soon as the bank has received a blocking notification from the account holder, it assumes all subsequent damage caused by unauthorized online banking transactions. This does not apply if the account holder acted with fraudulent intent.

9.2.3 Disclaimer

Liability claims are excluded if the circumstances justifying a claim are based on an unusual and unforeseeable event over which the party who refers to this event has no influence and the consequences of which could not have been avoided despite exercising due care.

10. Processing of personal data according to § 13 paragraph 1 TMG (Tele media Act)

Data protection All personal data arising in the context of online banking are processed by the bank and, if necessary, by the data center commissioned by it within Germany or the European Union for the purpose of executing the contract.

11. Mobile Banking

The above conditions for participating in online banking apply accordingly to mobile banking. Mobile banking means using the account using mobile devices (e.g. via WAP – Wireless Application Protocol).

12.Terms and Conditions

The general terms and conditions and the respective product conditions apply in addition to these special conditions.