Hinweise zur Nutzung mit einer Finanzsoftware

Bitte führen Sie die Erstellung Ihrer elektronischen Unterschrift mit der von Ihnen genutzten Software durch. Sämtliche von der OLB vertriebenen Programme werden mit einer Kurzanleitung, in der die Erstellung Schritt für Schritt beschrieben ist, ausgeliefert. Falls Sie eine andere Finanzsoftware verwenden, beachten Sie bitte die jeweilige Programmdokumentation des Herstellers.

Adresse des Bankrechners	**hbci.olb.de**
Port	**3000**
HBCI-/FinTS-Version	**3.0**
Bankleitzahl zur Erstellung der elektronischen Unterschrift	**28020050 (für sämtliche Nutzer identisch)**
Hash-Wert/Fingerabdruck zur Kontrolle des Bankrechners-Schlüssels (Nicht für alle Softwareprodukte erforderlich) **Stand 11/2017**. Falls Sie Ihre elektronische Signatur zu einem späteren Zeitpunkt erneut initialisieren, ist der angegebene Hash-Wert ggf. nicht mehr aktuell. Die jeweils aktuellen Hash-Werte können Sie unter www.olb.de/key abfragen.	**Sicherheitsverfahren RDH-1** 1E F1 56 D5 08 B2 87 C1 49 70 56 C8 EA 4E DA 93 06 87 20 C6 **Sicherheitsverfahren RDH-9 (Chipkarte)** 19 37 85 E0 84 61 C2 82 1D B5 8C 76 A3 AD 07 BB 19 A2 11 DD BB 2A A2 3C 35 A3 82 C6 AA 8F B6 D9 **Sicherheitsverfahren RDH-10 (Wechseldatenträger)** B2 CA 77 29 E7 27 13 B7 C2 53 7C 88 E0 51 65 D6 70 A6 20 45 37 51 AF BB 2D 53 86 CC A0 C7 C7 95

Support-Telefon-Nummer: 0800 5 70 90 40 (Anrufe aus deutschen Fest- und Mobilfunknetzen sind für Sie kostenfrei)
Aus dem Ausland: 0049 441 36141470
Montag – Freitag von 8.00 bis 18.00 Uhr

Sicherheitshinweise zum OLB Onlinebanking mit elektronischer Unterschrift (HBCI)

I. Legitimationsverfahren/Geheimhaltung

Der Nutzer ist verpflichtet, die mit der Bank vereinbarten Sicherungsmaßnahmen durchzuführen. Mit Hilfe der mit der Bank vereinbarten Medien identifiziert und legitimiert sich der Nutzer gegenüber der Bank. Der Nutzer hat dafür Sorge zu tragen, dass kein Dritter in den Besitz der Identifikations- und Legitimationsmedien kommt (oder eines entsprechenden Duplikates) sowie Kenntnis von dem zu deren Schutz dienenden Passwort erlangt. Denn jede Person, die im Besitz der Medien ist und das Passwort kennt, kann die vereinbarten Dienstleistungen nutzen. Insbesondere Folgendes ist zur Geheimhaltung der Identifikations- und Legitimationsmedien zu beachten:

- Die den Nutzer identifizierenden Daten dürfen nicht außerhalb der Sicherheitsmedien, z.B. auf der Festplatte des Rechners, gespeichert werden;
- die Identifikations- und Legitimationsmedien sind nach Beendigung der Online-Banking-Nutzung aus dem Lesegerät zu entnehmen und sicher zu verwahren;
- das zum Schutz der Identifikations- und Legitimationsmedien dienende Passwort darf nicht notiert oder elektronisch abgespeichert werden;
- bei Eingabe des Passwortes ist sicherzustellen, dass Dritte dieses nicht ausspähen können.

II. Zugangssperre

(1) Gehen die zur Identifikation und Legitimation dienenden Medien verloren, werden sie anderen Personen bekannt oder besteht der Verdacht ihrer missbräuchlichen Nutzung, so hat der Nutzer den Online-Banking-Zugang zum Konto/Depot durch die Bank unverzüglich sperren zu lassen.

(2) Hat der Nutzer seiner Bank eine Sperre übermittelt, so haftet die Bank ab dem Zugang der Sperrnachricht für alle Schäden, die aus ihrer Nichtbeachtung entstehen.

(3) Werden dreimal hintereinander Aufträge mit falscher elektronischer Signatur an die Bank übermittelt, so sperrt die Bank den Online-Banking-Zugang zum Konto/Depot. In diesem Fall sollte sich der Nutzer mit der Bank in Verbindung setzen.

(4) Die Bank wird den Online-Banking-Zugang zum Konto/Depot sperren, wenn der Verdacht einer missbräuchlichen Nutzung des Kontos/ Depots über das Online-Banking besteht. Sie wird den Kontoinhaber hierüber außerhalb des Online-Banking informieren. Diese Sperre kann mittels Online-Banking nicht aufgehoben werden.

(5) Bitte beachten Sie, dass die Chipkarte nach dreimaliger Falscheingabe des Kennwortes unwiderruflich gesperrt ist und ausgetauscht werden muss. Dieser Vorgang ist kostenpflichtig.

III. Behandlung der vom Nutzer übermittelten Daten durch die Bank

(1) Die der Bank mittels Online-Banking erteilten Aufträge, deren Eingang von der Bank elektronisch bestätigt wird, werden im Rahmen des ordnungsgemäßen Arbeitsablaufes bearbeitet. Ist die Durchführung am Tag der Auftragserteilung nicht möglich, wird die Bank den Auftrag am darauf folgenden Bankarbeitstag bearbeiten.

(2) Die Bank prüft die Legitimation des Absendenden sowie die Einhaltung der Datenformate.

(3) Ergibt die Legitimationsprüfung Unstimmigkeiten, wird die Bank den betreffenden Auftrag nicht bearbeiten und dem Nutzer hierüber unverzüglich eine Information zur Verfügung stellen.

(4) Ergeben sich bei den von der Bank durchgeführten Prüfungen Fehler, so wird die Bank die fehlerhaften Daten nachweisen und sie dem Nutzer unverzüglich bereitstellen. Die Bank ist berechtigt, die fehlerhaften Daten von der weiteren Bearbeitung auszuschließen, wenn die ordnungsgemäße Ausführung des Auftrages nicht sichergestellt werden kann.

IV. Rückruf oder Änderung von Aufträgen

Der Rückruf oder die Änderung von Aufträgen kann nur außerhalb des Online-Banking-Verfahrens erfolgen, es sei denn, die Bank sieht eine solche Möglichkeit innerhalb des Verfahrens ausdrücklich vor. Die Bank kann einen Rückruf oder eine Änderung allerdings nur beachten, wenn ihr diese Nachricht so rechtzeitig zugeht, dass ihre Berücksichtigung im Rahmen des ordnungsgemäßen Arbeitsablaufes möglich ist.

Wichtiger Hinweis zur Zugangssperre:

Gehen die zur Identifikation und Legitimation dienenden Medien verloren, werden sie anderen Personen bekannt oder besteht der Verdacht ihrer missbräuchlichen Nutzung, sperren Sie Ihren OLB InternetBanking-Zugang mit HBCI/FinTS bitte unverzüglich. Dies können Sie i.d.R. **selbst online** über die von Ihnen verwendete Software **oder durch die Bank** durchführen lassen.

Hierfür steht Ihnen unser **Sperr-Service für HBCI/FinTS** unter der **Telefon-Nr. 0441 2212021 jederzeit zur Verfügung**.

Unter dieser Rufnummer werden keine Hotline-Auskünfte erteilt.