

Bedingungen für die Nutzung von Online-Banking (Fassung 2007)

1. Vereinbarungsgegenstand

Zweck dieser Vereinbarung ist die Regelung von Online-Banking, das ist die Abfrage von Informationen über das Internet, zwischen einerseits dem Kontoinhaber und den von ihm bestimmten nutzungsberechtigten Personen, beide nachfolgend Kunden genannt, und andererseits der PRIVATINVEST BANK AG, nachfolgend Bank genannt. Mit dieser Vereinbarung werden die Kunden bis auf weiteres berechtigt, nach Freischaltung und Eingabe der vereinbarten Anmeldedaten im Rahmen des jeweils möglichen Umfangs nach Wahl des Kunden Leistungen von der Bank zu beanspruchen, wenn für die von der Bank angebotenen Geschäfte diese Möglichkeit vorgesehen ist. Dabei bleiben die für diese Bankgeschäfte und Dienstleistungen geltenden Vereinbarungen unberührt.

2. Voraussetzungen

- Bestand eines Kontos/Depots bei der Bank
- Freischaltung des Kontos/Depots (Antragsformular)
- Vereinbarung von Anmeldedaten, das sind
 - eine Benutzerkennung und
 - ein geheimes Passwort
- technische Voraussetzungen (z. B. Internet-Zugang, geeigneter Browser)

3. Leistungsumfang

Online-Banking ermöglicht derzeit die Abfrage von Informationen zu Konten/Depots, zu denen die Kunden Inhaber oder alleine zeichnungsberechtigt sind. Die Bank ist berechtigt, aufgrund des technischen Fortschrittes, von gesetzlichen Änderungen und notwendigen Sicherheitsmassnahmen Änderungen zum Leistungsumfang vorzunehmen. Änderungen werden an geeigneter Stelle bekanntgegeben.

4. Nutzungszeiten

Online-Banking steht grundsätzlich von Montag bis Sonntag zwischen 00:00 und 24:00 Uhr zur Verfügung. Die Bank ist berechtigt, diese Nutzungszeiten - vor allem aus technischen Erfordernissen - auch ohne vorherige Ankündigung zu ändern.

5. Nutzungsberechtigte Personen

Die Nutzungsberechtigung kann der Konto-/Depotinhaber nur dem Kontoinhaber und/oder einem/mehreren Einzelzeichnungsberechtigten erteilen und ist bei der Bank persönlich zu beantragen. Kunden im Sinne dieser Vereinbarung sind somit nutzungsberechtigte Personen. Änderungen der Verfügungsberechtigung zu einem von Online-Banking erfassten Konto/Depot können auch eine Änderung der Nutzungsberechtigung bewirken und sind der Bank schriftlich bzw. in anderer nachweislicher Form bekanntzugeben.

6. Zugriffsberechtigung

Zur Sicherung des Zugriffs auf Online-Banking erhalten alle Kunden von der Bank die Anmeldedaten, das sind

- eine Benutzerkennung und
- ein geheimes Passwort.

Die Bank kann das Verfahren zur Sicherung des Zugriffes gegen vorherige Mitteilung an die Kunden abändern.

7. Sorgfaltspflichten

Die Kunden haben die Anmeldedaten stets geheim zu halten und dafür zu sorgen, dass kein Dritter die Möglichkeit erhält, in deren Besitz zu kommen. Insbesondere sind die elektronische Speicherung, z.B. auf einem nicht ausreichend gesicherten Datenträger und eine Weitergabe an Dritte nicht zulässig. Die Kunden sind verpflichtet, bei Verlust der Anmeldedaten oder bei Verdacht, dass eine unbefugte Person von den Anmeldedaten Kenntnis erlangt hat, dies der Bank unverzüglich schriftlich bzw. in anderer nachweislicher Form mitzuteilen. Die Kunden können bei Verdacht auf missbräuchliche Verwendung ihrer Anmeldedaten bei der Bank jederzeit eine Zugriffssperre veranlassen. Die Veranlassung einer Sperre durch Kunden ohne Angabe von Gründen ist nur für die jeweils eigene Zugriffsberechtigung möglich.

Nach dreimaligem Zugriff mit, auch nur zum Teil falschen Anmeldedaten, sperrt die Bank automatisch den Zugriff für den betreffenden Kunden. Die Bank wird die Sperre im Rahmen des üblichen Arbeitsablaufes (Montag bis Freitag von 9:00 bis 16:30 Uhr) unverzüglich veranlassen. Die Kosten einer Sperre sowie allfällige Schäden bis zur Durchführung der Sperre tragen die Kunden eines Depots/Kontos gemeinsam.

Die Aufhebung von Zugriffssperren, die entweder wegen der Eingabe von falschen Anmeldedaten oder durch Kunden bzw. die Bank veranlasst wurden, muss bei der Bank wie eine neue Nutzungsberechtigung beantragt werden.

Bei Kunden, die sich durch die Anmeldedaten legitimieren, ist die Bank nicht verpflichtet, eine darüber hinausgehende Prüfung der Zugriffsberechtigung vorzunehmen.

8. Haftung

Die Kunden tragen alle Schäden, die durch missbräuchliche Verwendung der Anmeldedaten oder von Teilen derselben entstehen, sofern diese nicht durch die Bank grob fahrlässig oder vorsätzlich verursacht wurden. Die Kunden haben bei einer Verletzung dieser Vereinbarung den erzielten Nutzen in vollem Umfang abzugelten sowie die Bank gegenüber Dritten schad- und klaglos zu halten. Der Bank bleibt die Geltendmachung weiterer Schadenersatzansprüche ausdrücklich vorbehalten.

Die Bank haftet für allfällige Schäden, die aus Störungen bei der Hard- oder Software der Kunden oder durch das Nichtzustandekommen des Verbindungsaufbaues mit der Bank entstehen können nur, sofern sie diese Schäden vorsätzlich oder grob fahrlässig verursacht hat. Der Datenaustausch erfolgt über Einrichtungen der Post und privater Netzwerkanbieter. Für die den Kunden aufgrund von Übermittlungsfehlern, technischen Mängeln, Leistungsunterbrechungen, Verspätungen, Störungen oder rechtswidrigen Eingriffen der Post oder privater Netzwerkanbieter entstehenden Schäden und/oder entgangene Gewinne kann die Bank keine Haftung übernehmen.

Die Bank haftet nicht für den aus fehlgeleiteten oder verloren gegangenen Postsendungen, aus Übermittlungsfehlern, Irrtümern, Unterbrechungen, Verspätungen, Auslassungen oder Störungen irgendwelcher Art sowie aus Eingriffen in technische Einrichtungen der Bank oder im übrigen System entstehende Schäden, es sei denn, sie hat den Schaden vorsätzlich oder gar grob fahrlässig verursacht, und dann nur in dem Maß, in dem sie im Verhältnis zu anderen Ursachen an der Entstehung des Schadens mitgewirkt hat. Für entgangenen Gewinn haftet die Bank in keinem Fall. Im Verhältnis zu Unternehmern ist in allen hier genannten Fällen die Haftung für grobe Fahrlässigkeit ausgeschlossen.

9. Hotline

Für Anfragen von Kunden zu Online-Banking und zur technischen Abwicklung ist während der Banköffnungszeiten die Online-Banking-Hotline zuständig. Bei Problemen mit der Datenleitung haben die Kunden selbst die erforderlichen Schritte zu setzen.

10. Nutzungskosten

Die Kunden haben gemeinsam die Nutzungskosten der Bank in der jeweils festgelegten Höhe zu tragen (Pkt. 9 der Allgemeinen Geschäftsbedingungen der Bank). Die Nutzungskosten sind jeweils im voraus am 1. des Monats bei der Bank fällig. Die Kunden beauftragen die Bank, fällige Nutzungskosten vom Konto bei der Bank oder einem anderen Konto der Kunden abzubuchen. Die Nutzungskosten sind derzeit (Stand 02/2007) durch die sonstigen Gebühren, die die Bank für Konto-/Depotführung verrechnet, abgedeckt.

Die Bank kann die Nutzungskosten anpassen: Als Index für solche Anpassungen gilt der Verbraucherpreisindex 1996 mit Stand 1. Juli 2000 oder ein an dessen Stelle tretender, vergleichbarer Index. Änderungen unter 5% werden nicht vorgenommen. Änderungen der Nutzungskosten werden vor Inkrafttreten durch Aushang in den Schalterräumen der Bank bekanntgegeben. Die anfallenden Telefongebühren und die Entgelte der Netzwerkbetreiber sind von den Kunden zu bezahlen.

11. Vertragsdauer/Beendigung

Durch diese Vereinbarung wird den Kunden bis auf weiteres das Recht eingeräumt, Bankdienstleistungen der Bank mittels Online-Banking in Anspruch zu nehmen. Die Bank ist berechtigt, den Kunden ohne Angabe von Gründen die Zugriffsberechtigung zur Teilnahme an Online-Banking mit sofortiger Wirkung zu entziehen.

Bei Auflösung der Konto- und/oder Geschäftsverbindung mit der Bank erlischt die Möglichkeit zur Teilnahme an Online-Banking. Die Kunden sind berechtigt, die weitere Inanspruchnahme von Online-Banking oder einzelne Nutzungsberechtigungen mit sofortiger Wirkung jederzeit schriftlich oder in anderer nachweislicher Form der Bank gegenüber zu kündigen. Diese Kündigung wird mit dem auf den Tag des Einlangens der Kündigung bei der Bank folgenden Bankarbeitstag wirksam. Allfällige Kosten der Kündigung sowie allfällige Schäden bis zur Durchführung des Widerrufs gehen zu Lasten der Kunden.

12. Geltung der Geschäftsbedingungen

Ergänzend gelten die „Allgemeinen Geschäftsbedingungen der Bank“ in der jeweils geltenden Fassung.

13. Rechtliches

Erfüllungsort für alle aus dieser Vereinbarung hervorgehenden Ansprüche ist für beide Teile der Sitz der Bank. Für alle Rechtsbeziehungen aus dieser Vereinbarung gilt österreichisches Recht. Klagen gegen die Bank können nur am Erfüllungsort erhoben werden. Der Gerichtsstand des Erfüllungsortes ist auch für Klagen gegen einen Unternehmer maßgeblich.

Die Bank kann ihre Ansprüche auch bei jedem anderen örtlich und sachlich zuständigen Gericht geltend machen. Der für die Ansprüche eines Verbrauchers oder gegen einen Verbraucher bei Vertragsabschluss gegebene allgemeine Gerichtsstand in Österreich bleibt auch dann erhalten, wenn der Verbraucher nach Vertragsabschluss seinen Wohnsitz ins Ausland verlegt und österreichische gerichtliche Entscheidungen in diesem Lande vollstreckbar sind.

Technische/ organisatorische Voraussetzungen und Sicherheitshinweise

Technische Voraussetzungen

- Sie benötigen einen Internetzugang und einen Webbrowser, der moderne Sicherheitsstandards mit hoher Verschlüsselung unterstützt.
- Der Browser muss Secure-Socket-Layer (SSL) in der Version 3.0 oder höher sowie eine 128-Bit-Verschlüsselung oder höher unterstützen.
- In der Regel erfüllen alle gängigen Browser diese Anforderungen.
- Ältere Versionen, die diese Technologie nicht unterstützen, können für Online-Banking nicht eingesetzt werden. Sie können sich jedoch kostenlos eine aktuelle Version eines Browsers Ihrer Wahl, entweder über Internet oder auf einem anderen Weg besorgen.
- Online-Banking verwendet keine ActiveX-Controls oder JAVA-Applets. Sie können diese Funktionen in Ihrem Browser deaktivieren.
- Online-Banking verwendet JavaScripts. Sie müssen diese Funktionen in Ihrem Browser erlauben.
- Online-Banking verwendet aus Sicherheitsgründen Cookies. Sie müssen Cookies zumindest während der Dauer einer Verbindung mit Online-Banking zulassen.

Organisatorische Voraussetzungen

Vertragsverhältnis

- Voraussetzung ist das Bestehen von zumindest einem Konto oder Wertpapierdepot bei der Privatinvest Bank AG, über das Sie einzeln verfügungsberechtigt sind.
- Für die Freischaltung Ihrer Konten/Depots benötigen wir von Ihnen einen schriftlichen Antrag.
- Sie akzeptieren die Bedingungen für Online-Banking.

Anmeldung zum Online-Banking

- Sie erhalten Ihre Anmeldedaten (Benutzerkennung und Passwort) per Post zugesandt oder können diese in unserer Bank persönlich abholen.
- Das initiale Passwort bzw. ein nach einer Sperre neu generiertes Passwort wird durch einen Zufallsgenerator erzeugt und auf dem Postweg übermittelt oder persönlich übergeben.
- Bei der ersten Anmeldung bzw. nach Aufhebung einer Passwortsperre werden Sie aufgefordert, das initiale Passwort sofort auf ein neues Passwort Ihrer Wahl zu ändern.
- Wenn zwischen der automatischen Generierung eines Passwortes und Ihrer darauf folgenden Anmeldung eine bestimmte Zeit verstreicht (üblicherweise 60 Tage), so verfällt dieses Passwort automatisch und Sie müssen ein neues beantragen.
- Ihr Passwort muss mindestens 6 Zeichen lang sein und ist mit 20 Zeichen in der Länge begrenzt.
- Sie können numerische, alphanumerische und Sonderzeichen im Passwort verwenden. Das Passwort darf nicht durch Leerzeichen (blank) unterbrochen sein.
- Bei alphanumerischen Zeichen wird zwischen Groß- und Kleinschreibung unterschieden.
- Sollten Sie Ihr geheimes Passwort vergessen oder wird Ihr Passwort aus irgendeinem Grund gesperrt, so muss von der Bank ein neues Passwort generiert werden.
- Wenn Sie Ihr Passwort länger als sechs Monate nicht geändert haben, werden Sie von uns daran erinnert es aus Sicherheitsgründen zu ändern.
- Sie werden zwar nicht gezwungen, Ihr Passwort zu ändern, wir empfehlen Ihnen die regelmäßige Änderung jedoch unbedingt.
- Gewisse triviale Passwörter unterbindet das System. So ist es nicht möglich, ein Passwort gleich der Benutzerkennung zu wählen. Ausserdem sind nicht 6 oder mehrere gleiche Zeichen als Passwort möglich. Weiters erlauben wir uns aus Sicherheitsgründen, häufig verwendete und leicht zu erratende Wörter nicht zuzulassen.
- Verwenden Sie möglichst lange (max. 20 Zeichen) Passwörter.
- Nach 10 Minuten Inaktivität trennt Online-Banking automatisch die Verbindung. Sie können sich jederzeit wieder neu anmelden.

Übermittlung der Anmeldedaten

- Benutzerkennung und Passwort werden Ihnen mit der Post übermittelt oder persönlich übergeben.
- Sie quittieren mittels Rückbestätigung den Empfang der Anmeldedaten.

Freischaltung Ihrer Konten/Depots

- Aus Sicherheitsgründen erfolgt die Freischaltung Ihrer Konten/Depots erst nach Eintreffen der unterschriebenen Rückbestätigung.
- Dadurch wird sichergestellt, dass kein Unbefugter Ihre Anmeldedaten abfangen und Ihre Konto-/Depotdaten einsehen kann.

Geheimhaltung Ihrer Anmeldedaten

- Beachten Sie die Regeln zur Geheimhaltung Ihrer Benutzerkennung (siehe Sicherheitshinweise für Online-Banking).

Sicherheitshinweise für Online-Banking

Online-Banking ist nach den modernsten Sicherheitsstandards konzipiert und bietet nach dem aktuellen Stand der Technik höchstmögliche Sicherheit. Voraussetzung dafür ist die Verwendung eines Browsers, der moderne Sicherheitsstandards mit hoher Verschlüsselung unterstützt (siehe technische und organisatorische Voraussetzungen).

Was tragen wir zur Sicherheit bei?

Absicherung unserer Server gegen unbefugten Zugriff

Alle Systeme der PRIVATINVEST BANK AG werden durch ein modernes, mehrstufiges Firewall-System gegen jeden unbefugten Zugriff geschützt. Die Firewall sorgt dafür, dass ausschließlich Daten aus dem Internet an uns und umgekehrt übertragen werden können, die für unsere Anwendungen bestimmt sind und von uns zugelassen werden. Es besteht für einen Unbefugten keine Möglichkeit, direkt auf unsere Server zuzugreifen.

Hinweis

Beim Aufruf von Online-Banking kann abhängig von den Sicherheitseinstellungen Ihres Browsers, folgender Sicherheitshinweis erscheinen: "Diese Seite enthält sowohl sichere als auch nicht sichere Objekte. Möchten Sie die nicht sicheren Objekte anzeigen?" Fahren Sie bitte mit "Ja" fort.

Dies ist kein Problem von Online-Banking, sondern ein Problem der neuesten Browser-Versionen. Eine gesicherte Online-Banking-Verbindung ist auch weiterhin gewährleistet, sodass kein Sicherheitsrisiko besteht!

Authentifizierung der Bank gegenüber dem Kunden

Bei Anwahl unserer Anmeldeseite zum Online-Banking wird von unserem Web-Server automatisch das Zertifikat einer unabhängigen, vertrauenswürdigen Zertifizierungsstelle vorgelegt. Das Zertifikat stammt von der renommierten Firma VeriSign und bestätigt Ihnen, dass Sie tatsächlich mit unserem Web-Server verbunden sind. Noch vor der Eingabe Ihrer Benutzerkennung wird eine HTTPS-Verbindung zwischen Ihnen und der Bank aufgebaut.

Ab diesem Zeitpunkt erfolgt die Datenübertragung über eine hochsichere 128-Bit-Verschlüsselung.

Integrität der Applikation am Kunden-PC

Online-Banking verwendet außer Ihrem Webbrowser keine aktiven Programmkomponenten. Sie haben dadurch die Sicherheit, dass nicht ungewollt fremde Programme, die nicht Ihrer Kontrolle unterliegen, auf Ihrem Rechner laufen.

Authentifizierung der Applikation beim Start

Über ein von der weltweit anerkannten Zertifizierungsstelle VeriSign ausgegebenes Zertifikat, wird beim Start von Online-Banking eine sichere Verbindung zu unserem Applikations-Server aufgebaut.

Vertraulichkeit der übertragenen Kundendaten

Alle übertragenen Daten, vom Beginn bis zum Ende der bestehenden Verbindung, werden mit Hilfe einer Secure-Socket-Layer Implementierung (SSL Version 3.0) zwischen Kunden-PC und Applikations-Server verschlüsselt. Bei SSL werden zwei Verschlüsselungstechniken eingesetzt:

Symmetrische Verschlüsselung zur Übertragung von großen Datenmengen:

Bei dieser Technik benutzen sowohl der Sender als auch der Empfänger den gleichen Schlüssel. Dieser darf daher nur den beiden Parteien bekannt sein. Er wird daher immer am Anfang der Verbindung mit Hilfe eines Zufallszahlengenerators neu generiert, vor Beginn der Datenübertragung mit einem asymmetrischen Schlüssel codiert und über eine sichere Verbindung zwischen Sender und Empfänger ausgetauscht.

Asymmetrische Verschlüsselung für den sicheren Austausch des symmetrischen Schlüssels:

Dabei kommen ein öffentlicher und ein privater Schlüssel zum Einsatz. Wird eine Nachricht mit einem der beiden Schlüssel chiffriert, kann sie nur mit dem jeweils anderen Schlüssel dechiffriert werden. Wichtig ist, dass der private Schlüssel geheim ist und niemals über eine öffentliche Leitung übertragen wird.

Der Nachteil einer reinen asymmetrischen Verschlüsselung ist, dass diese für große Datenmengen nur bedingt geeignet ist. SSL vereint daher die Vorteile beider Verfahren.

Identifikation des Kunden für den Zugang zum Server

Der Zugang zu unserer Online-Banking Applikation und den entsprechenden Kundendaten wird nur nach Freischaltung des Kontos/Depots durch die Bank und erfolgreicher Eingabe der Benutzerkennung und eines mindestens 6-stelligen Passwortes (max. 20 Stellen) gewährt. Bei mehrfachen Fehlversuchen der Passworteingabe wird der Zugang automatisch gesperrt. Es ist somit nicht möglich, durch einfaches Probieren aller denkbaren Kombinationen einen Zugang zu den Kontodaten zu erhalten.

Überwachung der Verbindung (Session)

Alle bestehenden Verbindungen zu unserem System werden ständig überwacht. Beim Einstieg in die Anwendung wird zwischen unserem Webserver und Ihrem Browser eine hochsichere Session-Identifikation vereinbart. Jede folgende Serveranfrage muss sich damit identifizieren, um sicherzustellen, dass kein ungewollter Zugriff auf diese, von Ihnen initiierte Verbindung möglich ist. Erfolgt während einer Sitzung für längere Zeit (üblicherweise zehn Minuten) keine Eingabe, so wird die Verbindung automatisch geschlossen.

Was können Sie zur Sicherheit beitragen?

Vergewissern Sie sich über die sichere Verbindung

- Achten Sie darauf, dass Sie mit unserem Server nur über eine gesicherte Verbindung kommunizieren. Ein Sicherheitsymbol in Ihrem Browser (z.B. ein ungebrochener Schlüssel oder ein geschlossenes Vorhängeschloss) zeigt die aufrechte Verbindung zu unserem Server an. Sie erkennen diesen speziell geschützten Bereich auch an der Adresse <https://www.privatinvestbank.com>.
- Sie können das Server-Zertifikat überprüfen, indem Sie auf das Symbol für den Schlüssel doppelklicken.

Geheimhaltung Ihrer Benutzerkennung

- Halten Sie Ihre Benutzerkennung und Ihr Passwort geheim.
- Machen Sie sich keine Notizen. Sie verhindern damit, dass diese Daten in falsche Hände gelangen.
- Achten Sie darauf, dass Sie bei der Eingabe Ihres Passwortes niemand beobachtet.
- Geben Sie Ihr Passwort auch nicht an Bankmitarbeiter oder vermeintliche Bankmitarbeiter weiter. Kein Bankmitarbeiter benötigt für irgendwelche Transaktionen Ihr Passwort!
- Sollten Sie den Verdacht haben, dass Ihr Passwort bekannt ist, können Sie es selbst über Online-Banking ändern.

Regelmäßiges Ändern des Passwortes

- Ändern Sie Ihr Passwort regelmäßig.
- Verwenden Sie keine trivialen, leicht zu erratenden Passwörter.
- Vergeben Sie möglichst lange (max. 20 Zeichen) Passwörter.

Allgemein gültige Schutzmassnahmen auf Ihrem Rechner

- Achten Sie darauf, dass sich keine Computer-Viren auf Ihrem Rechner befinden.
- Verwenden Sie nur Browser, die Sie aus vertrauenswürdiger Quelle erhalten haben.
- Vermeiden Sie möglichst die Verwendung von ActiveX-Komponenten. Manche "böswilligen" ActiveX-Controls könnten wie Viren wirken. Deaktivieren Sie diese Funktion in Ihrem Internet-Browser.
- Sind Sie darauf angewiesen mit ActiveX zu arbeiten, dann laden Sie die ActiveX-Controls ausschließlich von vertrauenswürdigen Herstellern.
- Konfigurieren Sie Ihren Browser in den Einstellungen so, dass "SSL-Seiten" nicht im CACHE abgelegt werden.
- Erlauben Sie nach Möglichkeit nur Session-Cookies.

Zugriff auf Online-Banking sperren

- Falls Sie den Dienst gänzlich sperren wollen, können Sie das jederzeit selbst über Online-Banking veranlassen (Punkt - "Kundendaten ändern").
- Die Aufhebung dieser Sperre kann nur nach schriftlichem Antrag bei der Bank und nach Ausstellung eines neuen Initial-Passwortes erfolgen.
- Sollten Sie technische Probleme daran hindern, setzen Sie sich bitte mit Ihrem(r) persönlichen Betreuer(in) innerhalb der vereinbarten Geschäftszeiten in Verbindung.

Noch Fragen?

Falls Sie noch Fragen haben, wenden Sie sich bitte an Ihren persönlichen Betreuer oder kontaktieren Sie uns unter der Telefonnummer +43 662 8048 0.