Zugangs- und Nutzungsbedingungen der E-Banking-Dienste (Online-Banking)

Das vorliegende Dokument ergänzt die Allgemeinen Geschäftsbedingungen der Banque de Luxembourg (nachfolgend die „Bank"), die für alle Geschäftsbeziehungen des Kunden mit der Bank, insbesondere für die Festlegung des anwendbaren Rechts und die Wahl des Gerichtsstands, gelten.

1. Gegenstand

Die vorliegenden Bedingungen regeln den Zugang zu und die Nutzung der Online-Banking-Dienste durch den Kunden über die E-Banking-Website und/oder die BL-Mobile-Banking-App (nachfolgend die „E-Banking-Dienste") der Bank sowie die Modalitäten für den Nachweis des erfolgten Informationsaustausches und der ausgeführten Transaktionen auf einem oder mehreren Konten der Bank, für die er eine Zeichnungsberechtigung hat, sei es als Inhaber oder als Vertreter oder als Bevollmächtigter (nachfolgend die „abfragbaren Konten").

Diese Zugangs- und Nutzungsbedingungen der E-Banking-Dienste schaffen weder eine neue Verpflichtung zu Information oder Beratung noch ein neues Mandat zu Lasten der Bank.

Die E-Banking-Dienste der Bank bieten insbesondere die folgenden Funktionen:

- Vorstellung der Bank, ihrer Produkte und Dienstleistungen,
- Marktinformationen,
- Informationen über Kapitalmaßnahmen / wertpapierbezogene Vorkommnisse und die Möglichkeit, diesbezügliche Anweisungen zu erteilen,
- Recherchen und Finanzanalysen,
- Abfrage der abfragbaren Konten,
- Ausführung bestimmter Transaktionen,
- Elektronische Mitteilungen,
- Abfrage und Erstellung von Dokumenten,
- Elektronische Unterschrift von Dokumenten und Anweisungen,
- Festlegung/Änderung bestimmter personenbezogener Daten, sowie für bestimmte zugelassene Kunden die Möglichkeit, im Rahmen der Aktualisierung der Kundenakte Dokumente herunterzuladen bzw. hochzuladen,
- Zusammenführung von bei anderen Zahlungsdienstleistern geführten Konten,
- die Bereitstellung, über einen ein Subunternehmen, einer Plattform zur Zentralisierung und Verwaltung von Identifizierungsdaten und -dokumenten mit der Möglichkeit, falls vom Kunden erwünscht, diese Informationen und Dokumente mit Banken zu teilen, mit denen der Kunde ebenfalls Geschäftsbeziehungen unterhält und die dieselbe Plattform nutzen.

Mit dem Zugang zu den E-Banking-Diensten nimmt der Kunde zur Kenntnis und akzeptiert, dass der Bevollmächtigte gemäß den Allgemeinen Geschäftsbedingungen für Zahlungskarten über diesen Zugang gegebenenfalls alle mit den abfragbaren Konten verknüpften Kreditkarten einsehen, deren Sperrung beantragen, die Höhe ihrer Nutzungslimits ändern und das 3D Secure-Verfahren aktivieren kann.

Einige der vorstehend genannten Funktionen stehen unter Umständen nur bestimmten zugelassenen Kunden zur Verfügung oder sind unter Umständen nur im E-Banking-Bereich auf der Website der Bank oder in der BL-Mobile-Banking-App verfügbar oder unterscheiden sich im E-Banking-Bereich auf der Website der Bank und in der BL-Mobile-Banking-App voneinander.

Die Bank behält sich das Recht vor, diese Funktionen jederzeit zu ändern.

2. Kosten

Der Zugang zu den E-Banking-Diensten erfolgt gemäß den gültigen Tarifen der Bank, und der Kunde erklärt, diese zur Kenntnis genommen zu haben und zu akzeptieren. Weitere Gebühren wie die für das Internet-Abonnement (Internet Service-Provider), für Roaming, Datendienste oder Sonstiges gehen zu Lasten des Kunden.

Es gelten die Gebühren und Konditionen der Bank für Überweisungsvorgänge, Börsenaufträge, Zinssätze und Wechselkurse.

3. Sicherheit der E-Banking-Dienste

3.1. Zugangsarten

Um auf die E-Banking-Dienste zugreifen zu können, muss der Kunde über einen Internetzugang bei einem Anbieter seiner Wahl verfügen. Die Bank übernimmt keinerlei Verantwortung in Bezug auf den Internetzugang des Kunden. Dieser erfolgt auf das ausschließliche und alleinige Risiko des Kunden.

Der Zugang zu den E-Banking-Diensten der Bank erfolgt über die BL-Mobile-Banking-App oder über die dem Kunden mitgeteilte Adresse der E-Banking-Website mit seinen Benutzerkenndaten oder über eine andere Adresse, die die Bank dem Kunden auf einem von ihr für geeignet erachteten Wege, insbesondere auf elektronischem Wege, mitteilt.

Wird für den Zugang zu den E-Banking-Diensten ein Signing-Server-Zertifikat von LuxTrust (LuxTrust Scan oder LuxTrust Mobile-App) verwendet, erhält der Kunde von LuxTrust in einem verschlossenen Umschlag oder per SMS die Benutzerkenndaten für das von ihm gewählte Zugangsverfahren, damit er sich bei den E-Banking-Diensten einloggen, authentifizieren und seine Anweisungen unterzeichnen kann. Wenn der Kunde sich die Benutzerkenndaten gemerkt hat, müssen die SMS oder das gedruckte Schreiben vernichtet werden. Wird für den Zugang zu den E-Banking-Diensten eine andere von LuxTrust anerkannte Authentifizierungslösung verwendet, erfährt der Kunde die Modalitäten und Nutzungsbedingungen vom Anbieter seiner Authentifizierungslösung.

Alle Hilfsmittel für die Authentifizierung werden ihm gegebenenfalls in einem gesonderten Umschlag überreicht bzw. übersendet.

Der Kunde bevollmächtigt die Bank und LuxTrust ausdrücklich, seinen derzeitigen oder künftigen Bevollmächtigten, die über eine Zeichnungsberechtigung oder ein Recht auf Einsichtnahme für die über das Online-Banking abfragbaren Konten verfügen, auf deren Anfrage die Benutzerkenndaten und Mittel zur Authentifizierung zukommen zu lassen, die für den Zugang zu den E-Banking-Diensten erforderlich sind.

3.2. Sorgfaltspflicht des Kunden

Um jeglicher betrügerischen Nutzung vorzubeugen, verpflichtet sich der Kunde, alle Benutzerkenndaten zu schützen und alle Sicherheitsmaßnahmen zu ergreifen, um seine Mittel zur Zugangsauthentifizierung (Authentifizierungsmedium und Benutzerkenndaten von LuxTrust bzw. vom Anbieter einer alternativen Authentifizierungslösung, Passwort, One Time Password), die nur er kennt und besitzt, unter seiner alleinigen Kontrolle zu behalten. Es liegt in seiner ausschließlichen Verantwortung, diese persönlichen Codes strikt vertraulich zu behandeln. Sie dürfen weder notiert oder einem Dritten mitgeteilt werden noch auf einem oder mehreren Geräten gespeichert werden.

Der Kunde nimmt zur Kenntnis, dass die Bank ihn niemals per Telefon, E-Mail, SMS oder über sonstige Kommunikationsmittel auffordern wird, vertrauliche Daten (Benutzerkenndaten, Passwort, One Time Password) mitzuteilen oder einem Link in einer E-Mail oder SMS zu folgen, um sich bei den E-Banking-Diensten der Bank anzumelden.

Der Kunde hat daher jede unaufgefordert eingehende E-Mail oder SMS als verdächtig einzustufen, die vorgibt, von der Bank zu stammen, und in der er aufgefordert wird, seine persönlichen Daten und/oder Passwörter preiszugeben. Darüber

hinaus rät die Bank ihrem Kunden, die URL https://www.banquedeluxembourg.com stets selbst in die Adresszeile des Browsers einzugeben, die richtige Schreibweise der Adresse zu überprüfen und keinen in einer E-Mail oder SMS angegebenen Links zu folgen.

Der Kunde verpflichtet sich zudem, die im Anhang „Hinweise zu den Risiken von Überweisungen über die E-Banking-Dienste (Online-Banking)" beschriebenen Risiken zur Kenntnis zu nehmen und sich an die Sicherheitsempfehlungen und -hinweise in den „Sicherheitsinformationen" der E-Banking-Website und/oder der BL-Mobile-Banking-App und im Anhang „Was Sie tun können: Sicherheitshinweise zur Vermeidung von Risiken im Internet" zu halten.

Die Verletzung dieser Sicherheitshinweise gilt als grobe Fahrlässigkeit und verpflichtet den Kunden, den gesamten gegebenenfalls aus einem betrügerischen Zugang zu den E-Banking-Diensten entstehenden Verlust zu tragen.

3.3. Sperrung des Zugangs zu den E-Banking-Diensten

3.3.1. Auf Antrag des Kunden

Sobald der Kunde weiß oder vermutet, dass ein Dritter nach Verlust, Diebstahl, missbräuchlicher Verwendung oder unzulässiger Nutzung seiner Mittel zur Identifizierung Zugang zu den E-Banking-Diensten erlangen kann, hat er die Bank und LuxTrust bzw. den Anbieter der von ihm gewählten alternativen Authentifizierungslösung unverzüglich hiervon in Kenntnis zu setzen, damit sie diesen Zugang sperren können. Dies muss Montag bis Freitag von 8:00 Uhr bis 18:00 Uhr unter folgenden Rufnummern geschehen:

Hilfe LuxTrust: (+352) 24 550 550

Hilfe BL-Support: (+352) 26 20 26 30

Im Falle des Zugangs zu den E-Banking-Diensten mittels einer anderen Authentifizierungsmethode konsultiert der Kunde den Support des Anbieters dieser alternativen Authentifizierungslösung.

An anderen Tagen als an Werktagen nimmt der Kunde die Sperrung seines LuxTrust-Geräts auf der Website von LuxTrust (https://www.luxtrust.lu/de/management) vor, was an sieben Tagen der Woche rund um die Uhr möglich ist.

Im Falle des Zugangs zu den E-Banking-Diensten mittels einer anderen Authentifizierungsmethode konsultiert der Kunde die Website des Anbieters dieser alternativen Authentifizierungslösung.

3.3.2. Auf Initiative der Bank

Wenn die Erkennungsregeln der Bank auf einen Betrugsverdacht, einen erwiesenen Betrug oder Bedrohungen für die Sicherheit des Zugangs zu den E-Banking-Diensten des Kunden hindeuten, insbesondere im Falle des Verdachts einer betrügerischen Überweisung, wird die Bank auf jeglichem ihr geeignet erscheinenden Wege den Kunden kontaktieren und ihn gegebenenfalls darüber informieren, dass sein Zugang eingeschränkt oder gesperrt wurde, um das Risiko einer unzulässigen oder betrügerischen Nutzung zu begrenzen, ohne dass der Bank durch dieses Sicherheitsverfahren irgendeine Verpflichtung oder Haftung entsteht.

Die Bank behält sich das Recht vor, den Zugang des Kunden zu den E-Banking-Diensten einzuschränken oder zeitweise oder endgültig zu sperren, wenn dieser seine Verpflichtungen oder die Empfehlungen der Bank nicht einhält oder wenn die Bank es aus einem anderen objektiven Grund für sinnvoll erachtet, dem Kunden den Zugang zu untersagen. Ein solcher Grund kann insbesondere gegeben sein:

- **im Zusammenhang mit der Zugangssicherheit zu den E-Banking-Diensten;**
- **im Falle eines festgestellten, angenommenen oder befürchteten ungesetzlichen, nicht genehmigten, missbräuchlichen oder betrügerischen Zugangs;**
- **zur Wahrung der Interessen des Kunden oder der Bank;**
- **im Falle einer Schließung oder Sperrung der Konten oder wenn der Kunde seinen gesetzlichen, rechtlichen oder vertraglichen Verpflichtungen in Bezug auf die angebotenen Dienstleistungen nicht nachkommt;**
- **auf Antrag einer Justizbehörde;**
- **im Falle des Todes einer der Kontoinhaber;**
- **wenn es sich bei dem Zugang zu den E-Banking-Diensten um einen Zugang zu einem Konto mit einer von der Bank eingeräumten Kontoüberziehung handelt und ein deutlich erhöhtes Risiko besteht, dass der Kunde nicht in der Lage ist, seinen Zahlungsverpflichtungen im Rahmen einer Kreditlinie nachzukommen.**

In diesen Fällen informiert die Bank den Kunden unmittelbar nach einer Sperrung über diese Sperrung und deren Gründe, es sei denn, dies ist aus Sicherheitsgründen nicht akzeptabel oder im Rahmen geltender gesetzlicher Bestimmungen untersagt. Die Bank hebt die Sperrung des Zugangs auf oder ersetzt ihn durch einen neuen Zugang, sobald die Gründe für die Sperrung nicht mehr vorliegen.

3.4. Zugang und Sicherheit

Die Verbindung zu den E-Banking-Diensten ist durch eine Verschlüsselungs- und Kundenidentifizierungslösung geschützt.

Der Kunde bestätigt, von der Bank sämtliche zweckmäßigen Erläuterungen bezüglich dieser Sicherheitsvorkehrungen, ihrer Wirksamkeit und ihrer Grenzen erhalten zu haben. Er akzeptiert sie als zufriedenstellend und entbindet die Bank ausdrücklich von jeglicher Haftung in Bezug auf die Folgen einer Verletzung der Sicherheitsvorkehrungen durch einen unbefugten Dritten. Er bevollmächtigt die Bank ferner, die praktische und technische Funktionsweise der E-Banking-Dienste und insbesondere die Sicherheitsvorkehrungen zum Zugang zu den E-Banking-Dienste zu ändern, insbesondere um technologischen Entwicklungen Rechnung zu tragen. Der Kunde wird auf einem von der Bank für geeignet erachteten Wege darüber ordnungsgemäß in Kenntnis gesetzt.

Der Kunde verpflichtet sich, die Zugangsverfahren zu den E-Banking-Diensten der Bank in der von der Bank vorgegebenen Form sowie sämtliche in den E-Banking-Diensten angezeigten oder auf anderem Weg mitgeteilten Benutzungshinweise strikt zu befolgen. Bei jedem Zugang überprüft der Kunde, ob die Verbindung gesichert ist. Im Falle der Nichtbeachtung des Verfahrens oder der Benutzungshinweise wie auch im Falle eines Zugangsversuchs zu den E-Banking-Diensten mit Hilfe einer falschen Benutzerkennung behält sich die Bank das Recht vor, dem Kunden jeden weiteren Zugang zu den E-Banking-Diensten zu verweigern.

Im gemeinsamen Einverständnis der Vertragsparteien gilt jeder mit Hilfe der Benutzerkenndaten des Kunden erfolgte Zugang zu den E-Banking-Diensten als vom Kunden erfolgt. Als Beleg hierfür gilt das von der Bank angefertigte Verbindungsprotokoll.

Ebenso gilt jeder Zugang zu den E-Banking-Diensten durch einen Bevollmächtigten oder Vertreter des Kunden mit Hilfe einer der Benutzerkenndaten dieses Bevollmächtigten oder Vertreters als von diesem im Namen und für Rechnung des Kunden erfolgt. Der Kunde bleibt in vollem Umfang für Handlungen und Unterlassungen, auch unbeabsichtigter Art, seiner Bevollmächtigten oder Vertreter im Rahmen der Nutzung der E-Banking-Dienste verantwortlich, bis dieser Zugang auf Initiative des Kunden, seiner Bevollmächtigten oder Vertreter oder der Bank widerrufen wurde.

Außer in Fällen eines groben Verschuldens oder Fahrlässigkeit ihrerseits übernimmt die Bank keinerlei Haftung und kann ins-

besondere nicht der Verletzung ihrer Geheimhaltungspflicht bezichtigt werden, falls es einem Dritten gelingen sollte, Zugang zu den abfragbaren Konten des Kunden zu erlangen oder durch die E-Banking-Website und/oder die BL-Mobile-Banking-App der Bank oder über das Internet Informationen über dessen Geschäftsbeziehung mit der Bank einzuholen.

4. Über die E-Banking-Dienste zugängliche Informationen

Dem Kunden stehen über die E-Banking-Dienste verschiedene Finanz- und Wirtschaftsinformationen zur Verfügung, die von der Bank und/oder von Dritten stammen und insbesondere die Finanzmärkte und Investmentfonds zum Thema haben.

Die Bank gibt, soweit möglich, das jeweilige Erscheinungs- bzw. Abfassungsdatum der über die E-Banking-Dienste veröffentlichten Informationen an und aktualisiert diese ebenso schnell wie die auf Papier veröffentlichten Informationen.

Im Rahmen seiner Wertpapieranlagen kann der Kunde über die E-Banking-Dienste Kapitalmaßnahmen (nachfolgend „KM") einsehen und auf elektronischem Wege gemäß Artikel 6.2 der vorliegenden Bedingungen diesbezügliche Aufträge erteilen.

Alle über die E-Banking-Dienste veröffentlichten Informationen dienen ausschließlich der Information und sind auf keinen Fall mit einer Beratung durch die Bank gleichzustellen. Der Kunde verpflichtet sich, diese Informationen verantwortungsbewusst und kritisch zu nutzen.

Er entlastet die Bank ausdrücklich von jeglicher Haftung hinsichtlich des Inhalts, der Zuverlässigkeit, der Aktualität, der Vollständigkeit und der Genauigkeit der von Dritten stammenden und als solche gekennzeichneten Informationen. Er bestätigt, dass er sich darüber im Klaren ist, dass die KM auf von externen Quellen bezogenen Informationen beruhen und nicht von der Bank überprüft wurden.

Der Kunde verzichtet ausdrücklich auf jegliche Online-Beratung seitens der Bank bezüglich der über die E-Banking-Dienste veröffentlichten Informationen und verpflichtet sich, Beratung in Bezug auf seine Anlagen und die Verwaltung seines Portfolios direkt bei einem Kundenberater seiner Wahl einzuholen.

Der Kunde verpflichtet sich, die Eigentumsrechte an den über die E-Banking-Dienste zugänglichen Informationen zu respektieren. Er verpflichtet sich, diese Informationen weder an Dritte weiterzuleiten noch sie zu veröffentlichen oder in irgendeiner Form oder Weise zu verbreiten noch die E-Banking-Dienste ganz oder auszugsweise wiederzugeben. Sofern dem nicht schriftlich widersprochen wird, bevollmächtigt der Kunde die Bank, Mitteilungen, auch kommerzieller Art, über die E-Banking-Dienste oder per E-Mail an ihn zu richten.

5. Abfrage der abfragbaren Konten

Der Kunde kann über die E-Banking-Dienste den Stand der abfragbaren Konten, die ggf. laufenden Kauf- und Verkaufsvorgänge auf diesen Konten abfragen. Er bevollmächtigt die Bank, ihm sämtliche Informationen bezüglich der abfragbaren Konten und der auf diesen Konten abgewickelten Vorgänge über die Website mitzuteilen; dies gilt unbeschadet einer eventuellen Vereinbarung mit der Bank, der zufolge alle an den Kunden gerichtete Korrespondenz in den Geschäftsräumen der Bank verbleiben soll.

Kunden, die sich entschieden haben, die abfragbaren Konten, deren Inhaber oder Vertreter sie sind, ausschließlich online über die E-Banking-Dienste einzusehen, verpflichten sich dazu, dies mindestens einmal pro Quartal zu tun. Wenn die abfragbaren Konten über einen Zeitraum von sechs Monaten nicht eingesehen wurden, deaktiviert die Bank den Zugang zu den E-Banking-Diensten und schickt dem Kunden auf seine Kosten die Kontoauszüge, die Kontoübersichten und die Korrespondenz der abfragbaren Konten an die bei der Kontoeröffnung oder zu einem späteren Zeitpunkt durch den Kunden mitgeteilten Postanschrift.

Die Bank behält sich das Recht vor, dem Kunden den Zugang zu einem oder mehreren abfragbaren Konten über die E-Banking-Dienste zu verweigern, wenn nach ihrem eigenen Ermessen ein triftiger Grund hierfür vorliegt.

6. Elektronische Aufträge des Kunden

Die E-Banking-Dienste ermöglichen dem Kunden, der Bank Überweisungsaufträge sowie Aufträge über den Kauf oder Verkauf von Finanzinstrumenten sowie alle Aufträge im Zusammenhang mit KM bezüglich seiner Anlagen (nachfolgend die „elektronischen Aufträge") zu erteilen, die zu den gleichen Bedingungen wie seine anderen Aufträge ausgeführt werden, und seine elektronische Unterschrift auf ihm von der Bank übermittelten Dokumenten anzubringen. Diese elektronische Unterschrift hat denselben Wert wie eine handgeschriebene Unterschrift.

Bei jedem an die Bank gerichteten elektronischen Auftrag verpflichtet sich der Kunde, alle zur ordnungsgemäßen Ausführung des Auftrags notwendigen Angaben zu machen. Die vom Kunden eingegebenen Informationen werden dabei von der Bank auf dem Bildschirm des Kunden angezeigt.

Sofern dem Kunden nicht im Rahmen einer eingeräumten Kontoüberziehung von der Bank eine entsprechende Genehmigung erteilt wurde, darf der Kunde das Konto ausschließlich auf Guthaben-Basis und im Rahmen einer ausreichenden Kontodeckung nutzen. Der Kunde verpflichtet sich, für ausreichende Deckung des Girokontos zu sorgen, damit das Guthaben auf diesem Konto ausreicht, um die Ausführung der elektronischen Aufträge im Rahmen der festgelegten Nutzungslimits zu ermöglichen. Der Kunde erklärt sich damit einverstanden, dass bei mangelnder Deckung des Kontos Sollzinsen gemäß Artikel 15 der Allgemeinen Geschäftsbedingungen der Bank erhoben werden. Die Bank behält sich das Recht vor, jeder elektronische Auftrag abzulehnen, wenn das Konto nicht ausreichend gedeckt ist.

Der Kunde haftet für alle unter Verwendung seiner Benutzerkenndaten übermittelten Aufträge so lange, bis er der Bank mitgeteilt hat, diese gemäß dem in Artikel 3.3 oben beschriebenen Verfahren als ungültig zu betrachten, und die Bank in der Lage ist, solche Aufträge abzulehnen.

Der Kunde ist für alle von ihm selbst, seinem Bevollmächtigten oder seinem Vertreter über die E-Banking-Dienste übermittelten elektronischen Aufträge verantwortlich, auch wenn die Vollmacht zugunsten eines Bevollmächtigten oder eines Vertreters widerrufen wurde.

Die Vertragsparteien erkennen elektronischen Aufträgen sowie über die E-Banking-Dienste der Bank elektronisch unterschriebenen Dokumenten die gleiche Beweiskraft zu wie einer privatschriftlichen Urkunde gemäß Art. 1322 ff. des Luxemburgischen „Code Civil" und akzeptieren ihre Rechtswirksamkeit für den Kunden und die Bank ungeachtet des Betrags oder der Tragweite.

6.1. Aufträge über Finanzinstrumente

Es wird davon ausgegangen, dass Aufträge über den Kauf oder Verkauf von Finanzinstrumenten als einfache Ausführungsorder gemäß Artikel 12 der allgemeinen Geschäftsbedingungen der Bank ausgeführt und/oder erhalten und übertragen werden sollen.

6.2. Aufträge in Verbindung mit Kapitalmaßnahmen

Wenn der Kunde nach dem Einsehen einer KM über die E-Banking-Dienste einen Auftrag (der „Auftrag") erteilen muss, erklärt er, dass er sich darüber im Klaren ist, dass die E-Banking-Dienste der einzige Kommunikationskanal sind.

Der Kunde erklärt sich damit einverstanden, dass sich die Bank nicht der Konformität des Auftrags mit anwendbaren Gesetzen und Vorschriften und/oder anderen geltenden Einschränkungen verge-

wissert. Er bestätigt damit, dass er alle Konsequenzen trägt, die sich aus dem Auftrag ergeben.

Der Kunde erklärt sich damit einverstanden, dass mithilfe seiner persönlichen Codes über die E-Banking-Dienste übermittelte Aufträge auf sein eigenes Risiko ausgeführt werden, und stellt die Bank in dieser Hinsicht ausdrücklich von jeder Haftung frei für Folgen, die sich aus einem fahrlässigen oder schuldhaften Verhalten seinerseits sowie der Nichtbeachtung der in den vorliegenden Bedingungen und ihren Anhängen genannten Wohlverhaltensregeln ergeben.

Insbesondere entbindet der Kunde die Bank von jeglicher Haftung, die sich aus einer Verspätung der Mitteilung der KM und/oder der Übermittlung des Auftrags ergibt.

6.3. Überweisungsaufträge

6.3.1. Risikoakzeptanzerklärung

Der Kunde erklärt, dass er sich über alle mit der Ausführung von Überweisungen über die E-Banking-Dienste verbundenen Risiken, die im Anhang „Hinweise zu den Risiken von Überweisungen über die E-Banking-Dienste (Online-Banking)" dargelegt sind, bewusst ist.

Der Kunde ist sich dessen bewusst, dass mit höheren Limits für Überweisungen über die E-Banking-Dienste ein höheres Risiko verbunden ist. Sind mit einem BL Web User mehrere Konten verbunden, entspricht das Limit des BL Web Users der Summe der einzelnen für die jeweiligen Konten festgesetzten Limits.

Der Kunde erklärt sich damit einverstanden, dass alle mit Hilfe seiner persönlichen Zugangscodes über die E-Banking-Dienste beauftragten Überweisungen auf sein eigenes Risiko ausgeführt werden, und stellt die Bank in dieser Hinsicht ausdrücklich von jeder Haftung frei für Folgen, die aus einem fahrlässigen oder schuldhaften Verhalten seinerseits sowie der Nichtbeachtung der in diesem Dokument und seinen Anhängen genannten Wohlverhaltensregeln folgen.

6.3.2. Zustimmung zu und Widerruf von Überweisungsaufträgen, Ausführungsfristen

Ein Überweisungsauftrag gilt als genehmigt, wenn der Kunde mit einem von den E-Banking-Diensten verlangten Authentifizierungs- und Bestätigungsverfahren seine Zustimmung zu dessen Ausführung erteilt hat. Liegt eine solche Zustimmung nicht vor, gilt der Überweisungsauftrag als nicht genehmigt.

Die Bestimmungen in Bezug auf den Zeitpunkt des Eingangs und auf den Widerruf des Überweisungsauftrags sowie auf die maximale Ausführungsfrist, die in Artikel 9 der Allgemeinen Geschäftsbedingungen der Bank dargelegt sind, gelten in vollem Umfang.

6.3.3. Haftung des Kunden im Falle von nicht genehmigten Überweisungsvorgängen

Vom Verbraucher kann verlangt werden, bis zur Anzeige eines Verlusts, Diebstahls oder einer Fälschung seiner Benutzerkenndaten für die E-Banking-Dienste, Verluste bis zu einem Betrag von 50 EUR zu tragen, die durch nicht genehmigte Überweisungsvorgänge infolge der Nutzung oder missbräuchlichen Verwendung seiner Benutzerkenndaten für die E-Banking-Dienste entstehen. Diese Bestimmung findet keine Anwendung, wenn der Verlust, der Diebstahl oder die missbräuchliche Verwendung des Zugangs vor der Zahlung vom Kunden nicht bemerkt werden konnte, es sei denn, der Kunde handelte in betrügerischer Absicht oder der Verlust wurde durch Handlungen oder Unterlassungen eines Angestellten, eines Vertreters oder einer Niederlassung der Bank, von LuxTrust oder des Anbieters einer alternativen Authentifizierungslösung verursacht.

Die Obergrenze von maximal 50 EUR gilt nur für Verbraucher.

Der Kunde (ob Verbraucher oder nicht) trägt alle Verluste infolge von nicht genehmigten Überweisungsvorgängen, wenn diese Verluste aus betrügerischen Handlungen seinerseits oder einer absichtlichen oder grob fahrlässigen Verletzung einer oder mehrerer in Artikel 3 der vorliegenden Bedingungen aufgeführten Verpflichtungen entstanden sind. In diesem Fall findet der vorstehend angegebene Höchstbetrag keine Anwendung. Als grobe Fahrlässigkeit gilt insbesondere, wenn der Kunde seine persönlichen Sicherheitsvorkehrungen, wie z. B. seine persönlichen Benutzerkenndaten oder andere Codes, in leicht erkennbarer Form notiert, sie einem Dritten mitgeteilt hat oder sie auf einem oder mehreren Geräten ungesichert gespeichert hat oder wenn er den Verlust oder Diebstahl nicht umgehend beim zentralen Sperr-Notruf anzeigt, sobald er hiervon Kenntnis erlangt. Bei der Prüfung, ob der Tatbestand der Fahrlässigkeit vorliegt, wird der Sachverhalt in seiner Gesamtheit berücksichtigt.

Für den Fall, dass die Bank dem Kunden den einem nicht genehmigten Vorgang entsprechenden Betrag erstattet hat und sie anschließend berechtigte Gründe für den Verdacht hat, dass der Kunde in betrügerischer Absicht handelte oder eine oder mehrere seiner vorstehend aufgeführten Pflichten vorsätzlich oder grob fahrlässig verletzte, behält sich die Bank das Recht vor, diesen Betrag vom Konto des Kunden abzubuchen und die Commission de Surveillance du Secteur Financier (CSSF) in L-1150 Luxemburg, 283, route d'Arlon, hierüber zu informieren.

6.3.4. Anspruch auf Erstattung, Mitteilung und Berichtigung nicht genehmigter oder fehlerhaft ausgeführter Überweisungsvorgänge

Die Bedingungen für den Anspruch auf Erstattung, Mitteilung und Berichtigung nicht genehmigter oder fehlerhaft ausgeführter Zahlungsvorgänge unterliegen den entsprechenden Bestimmungen von Artikel 9 der Allgemeinen Geschäftsbedingungen der Bank.

6.4. Kontobuchungen elektronischer Aufträge

Elektronische Aufträge werden durch Kontobuchungen ausgeführt und sind den Vorgängen gleichzusetzen, die in den Artikeln 9 und 12 der Allgemeinen Geschäftsbedingungen der Bank beschrieben sind. Eventuelle Buchungen einer nicht genehmigten Transaktion auf dem Konto, Fehler oder eventuelle andere Unregelmäßigkeiten in der Kontoverwaltung müssen der Bank unverzüglich angezeigt werden.

Die Bank verpflichtet sich, für eine Dauer von 10 Jahren ein Exemplar aller vom Kunden erteilten elektronischen Aufträge auf einem dauerhaften Datenträger aufzubewahren und alle Maßnahmen zu ergreifen, mit denen die Unveränderbarkeit dieser Aufzeichnungen gewährleistet wird. Der Kunde erkennt ausdrücklich an, dass die durch die Bank erfolgten Aufzeichnungen die Existenz, den Inhalt sowie das Datum und die Uhrzeit der Erteilung seiner elektronischen Aufträge belegen und zu diesem Zweck vor Gericht verwendet werden können. Die Bank stellt dem Kunden auf Anfrage eine Kopie sämtlicher Aufzeichnungen zur Verfügung.

7. Kundenbeanstandung

Die Bedingungen für Beanstandungen, einschließlich der außergerichtlichen Rechtsmittel, die dem Kunden offenstehen, sind in Artikel 7 der Allgemeinen Geschäftsbedingungen der Bank dargelegt.

8. Kontozusammenführungsdienst

Der Kontozusammenführungsdienst entspricht dem Konto-Informationsdienst gemäß den Bestimmungen von PSD2[1]. Er besteht darin, konsolidierte Informationen über das/die Zahlungskonto/-

1 Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates vom 25. November 2015 über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinien 2002/65/EG, 2009/110/EG und 2013/36/EU und der Verordnung (EU) Nr. 1093/2010 sowie zur Aufhebung der Richtlinie 2007/64/EG

konten, das/die vom Kunden bei einem oder mehreren vom Kunden benannten Zahlungsdienstleister(n) geführt und benannt werden, online zur Verfügung zu stellen, d. h. unter anderem den Saldo des/der Kontos/Konten und die in den vergangenen 90 Tagen über diese/s benannte/n Konto/Konten ausgeführten Zahlungsvorgänge.

Die Bank kann dem Kunden nur die von dem oder den vom Kunden benannten Zahlungsdienstleister(n) zur Verfügung gestellten Informationen übermitteln. Sie kann für einen durch diese/n Zahlungsdienstleister verursachten Mangel an Informationen nicht haftbar gemacht werden.

Der Kontozusammenführungsdienst hängt nicht vom Bestehen von vertraglichen Beziehungen zwischen der Bank und den anderen Zahlungsdienstleistern ab. Er wird auf der Grundlage der ausdrücklichen Zustimmung des Kunden und seiner ordnungsgemäßen Authentifizierung bei den anderen Zahlungsdienstleistern zur Verfügung gestellt, unter der Bedingung, dass die benannten Konten online zugänglich sind, und der Kunde Inhaber der abfragbaren Konten bei der Bank ist. Die Zustimmung des Kunden ist erforderlich, wenn er den Kontozusammenführungsdienst zum ersten Mal in Anspruch nimmt. Diese Zustimmung läuft nach 90 Tagen ab und muss dann erneuert werden.

Im Rahmen des Kontozusammenführungsdienstes genehmigt der Kunde der Bank ausdrücklich, seine persönlichen Sicherheitsdaten zu verwenden, um dem Kunden zu ermöglichen, sich auf sichere Weise bei dem oder den vom Kunden benannten Zahlungsdienstleister/n zu identifizieren. Die Bank trägt dafür Sorge, dass die persönlichen Sicherheitsdaten des Kunden keinen anderen Parteien als der Bank und dem Aussteller der besagten Daten zugänglich sind, und verwendet für die Übertragung dieser Daten sichere und effiziente Kanäle.

Die Bank greift nur auf Informationen zu, die von den vom Kunden benannten Konten und den mit ihnen verbunden Zahlungsvorgängen stammen. Die Bank nutzt, konsultiert oder speichert die Daten ausschließlich für die Zwecke des Kontozusammenführungsdienstes und gemäß den Datenschutzbestimmungen.

9. Verarbeitung und Schutz personenbezogener Daten

Der Zugang zu den E-Banking-Diensten ist mit der Verarbeitung der personenbezogenen Daten des Kunden durch die Bank zum Zweck der Erfüllung des vorliegenden Vertrags und der allgemeinen Verwaltung der Kundenbeziehung und der dazugehörigen Dienstleistungen verbunden.

Die mit Hilfe des Antrags auf Zugang zu den E-Banking-Diensten erhobenen Informationen können somit auf jeden Träger gebracht werden und werden von der Bank in einer Datenbank gespeichert und zu Zwecken der Identifikation und Verwaltung des Zugangs zu den E-Banking-Diensten, der Verwaltung der Konten und Vorgänge sowie der Überprüfung ihrer Regelmäßigkeit verarbeitet.

Um ihren gesetzlichen Pflichten insbesondere im Bereich der Rechtsvorschriften zur Bekämpfung der Geldwäsche und Terrorismusfinanzierung nachzukommen, kann die Bank gegebenenfalls die vom Kunden gelieferten Daten auf ihre Echtheit prüfen und diese an die staatlichen Behörden und die zuständigen Gerichtsbarkeiten weitergeben.

Die Bank darf die personenbezogenen Daten nur so lange speichern, wie es dem Erhebungszweck der Bank entspricht und wie es in den Allgemeinen Geschäftsbedingungen der Bank vorgesehen ist.

Zum Zweck der Erfüllung des vorliegenden Vertrags und der Bereitstellung von E-Banking-Diensten gibt die Bank die personenbezogenen Daten des Kunden an das Unternehmen LuxTrust und/oder den Anbieter der vom Kunden gewählten und von LuxTrust anerkannten alternativen Authentifizierungslösung sowie, im Rahmen des Kontozusammenführungsdienstes, an das Unternehmen LuxHub, den Verwalter der Schnittstelle (API), weiter, die die Daten in diesem Kontext ebenfalls verarbeiten, wozu der Kunde seine ausdrückliche Zustimmung gibt. Der Kunde hat das Recht, Zugang zu seinen personenbezogenen Daten sowie die Berichtigung, die Löschung und die Übertragung dieser Daten zu verlangen, sowie das Recht, Widerspruch gegen ihre Verarbeitung einzulegen oder auch eine Begrenzung für die Verarbeitung seiner personenbezogenen Daten festzulegen.

Der Kunde kann bestimmte persönliche Angaben über die E-Banking-Dienste abrufen und/oder ändern. Der Kunde beantragt, dass jede auf diese Weise der Bank mitgeteilte Änderung auf gleiche Weise behandelt wird wie jede andere Änderungsmitteilung.

Der Kunde verpflichtet sich, gegenüber der Bank korrekte und vollständige Angaben zu machen, die Bank unverzüglich über alle Änderungen dieser Angaben zu informieren und ihr auf einfache Anfrage alle Unterlagen zukommen zu lassen bzw. weitere Auskünfte zu erteilen, die nach Auffassung der Bank im Rahmen der laufenden Geschäftsbeziehung oder aufgrund von gesetzlichen Bestimmungen oder vergleichbaren Vorschriften erforderlich sind.

Um das Nutzererlebnis des Kunden im Rahmen der Überwachungspflicht der Bank gegenüber der Kundschaft (KYC) zu verbessern, kann die Bank mitunter die Dienste eines Subunternehmers in Anspruch nehmen, um zugelassenen Kunden eine Plattform zur Verfügung zu stellen, die die Zentralisierung und elektronische Verwaltung ihrer Identifizierungsdaten und -dokumente (der „Datenverwaltungsdienst“) ermöglicht. Damit diese Dienste erbracht werden können, übermittelt die Bank die personenbezogenen Daten des Kunden an das Subunternehmen. Dieser Datenverwaltungsdienst ermöglicht zugelassenen Kunden, ihre Identifizierungsdaten und -dokumente zu zentralisieren und zu verwalten, und die Kunden erhalten mitunter Benachrichtigungen vom Subunternehmen mit dem Ziel, sie darüber zu informieren, wenn ihre Daten oder Dokumente nicht mehr auf dem neusten Stand sind.

Zu diesem Dienst zugelassene Kunden werden darüber über ihren Zugang zu den E-Banking-Diensten informiert und verpflichten sich, die Nutzungsbedingungen dieses Datenverwaltungsdienstes des Subunternehmens zu akzeptieren, indem sie diesen aktivieren. Das Ausbleiben bzw. die Weigerung des Kunden, diese Nutzungsbedingungen zu akzeptieren, kann von der Bank als Hindernis für die Erbringung der E-Banking-Dienstleistungen oder sogar für die Aufrechterhaltung der Geschäftsbeziehungen mit der Bank angesehen werden.

Zu diesem Datenverwaltungsdienst zugelassene Kunden haben auch die Möglichkeit, sich für das Teilen bestimmter Identifizierungsdaten und -dokumente mit anderen Banken, mit denen sie ebenfalls eine Bankbeziehung haben und die dieselbe Plattform des Subunternehmens nutzen, zu entscheiden. Um diese gemeinsame Nutzung von Daten in Anspruch zu nehmen, muss der Kunde seinen Wunsch bestätigen, dies über die E-Banking-Dienste und/oder über gleichwertige Dienste der anderen Banken zu tun, mit denen der Kunde eine Geschäftsbeziehung unterhält und die dieselbe Plattform nutzen. Sofern sich der Kunde für diesen Datenaustauschdienst entscheidet, erklärt er, dass er von den Allgemeinen Nutzungsbedingungen dieses Datenaustauschdiensts sowie von allen anderen Bedingungen, die für ihn und/oder die Bank im Rahmen dieses Dienstes des Subunternehmens gelten, Kenntnis genommen hat und damit einverstanden ist.

Die vorliegenden Bestimmungen bezüglich der Verarbeitung und des Schutzes personenbezogener Daten des Kunden ergänzen Artikel 22 der Allgemeinen Geschäftsbedingungen der Bank und die Data Privacy Policy, die der Kunde hiermit genehmigt und annimmt.

10. Zugang zu den E-Banking-Diensten

Die Bank behält sich das Recht vor, den Zugang zu den E-Banking-Diensten zeitweilig, vor allem aus technischen Gründen, auszusetzen.

Falls die Bank die zeitweilige Nichtverfügbarkeit der E-Banking-Dienste vorhersehen kann, wird sie sich bemühen, den Kunden im

Voraus mit allen geeigneten Mitteln hierüber zu informieren, u. a. durch eine Mitteilung über die E-Banking-Dienste selbst.

Der Kunde entlastet die Bank von allen Konsequenzen, die eine vorübergehende Nichtverfügbarkeit der E-Banking-Dienste haben kann, unabhängig von den zugrunde liegenden Ursachen. Ebenso entlastet er die Bank von allen Konsequenzen einer Verlangsamung, einer Störung oder einer Fehlfunktion der E-Banking-Dienste, der Infrastruktur der Informatik der Bank, einer Verbindungsunterbrechung zu den E-Banking-Diensten oder aus irgendeinem anderen technischen Grund, selbst wenn dieser von der Bank verschuldet wird.

11. Vertraulichkeit der Mitteilungen

Die Parteien erkennen den über die E-Banking-Dienste ausgetauschten Mitteilungen den Charakter einer privaten Korrespondenz zu.

12. Zuordnung des Austauschs

Die zwischen der Bank und dem Kunden hergestellten Verbindungen sowie alle über die E-Banking-Dienste initiierten und durchgeführten Vorgänge gelten als direkt bei der Bank, zu dem auf dem Server der Bank angezeigten Datum und Uhrzeit, erfolgt. Als Nachweis gilt das Verbindungsprotokoll der Bank.

13. Vernichtung der Benutzerkenndaten und Zertifikate

Für den Fall, dass der Kunde die E-Banking-Dienste nicht mehr für den Zugang zu seinen abfragbaren Konten nutzt, verpflichtet er sich, alle von der Bank erhaltenen Mittel zur Authentifizierung zu vernichten.

14. Haftung

Mit der Bereitstellung der E-Banking-Dienste übernimmt die Bank gegenüber dem Kunden lediglich eine Sorgfaltspflicht. Gemäß Artikel 21 der Allgemeinen Geschäftsbedingungen der Bank kann die Haftung der Bank nur im Falle eines groben Verschuldens geltend gemacht werden.

Die Bank haftet weder im Falle höherer Gewalt noch in Fällen, in denen sie durch andere geltende gesetzliche Verpflichtungen gebunden ist.

Beim Zugang zu den E-Banking-Diensten aus dem Ausland verpflichtet sich der Kunde, die geltenden gesetzlichen Bestimmungen oder vergleichbaren Vorschriften des Landes einzuhalten, von dem aus der Zugang erfolgt.

Die Bank kann keine Haftung für Fehler der Authentifizierungslösungen des Anbieters der vom Kunden gewählten Authentifizierungslösung übernehmen.

15. Änderung der Zugangs- und Nutzungsbedingungen der E-Banking-Dienste

Die Bank kann die vorliegenden Zugangs- und Nutzungsbedingungen der E-Banking-Dienste gemäß den Modalitäten in Artikel 23 der Allgemeinen Geschäftsbedingungen jederzeit ändern, indem sie dies dem Kunden auf beliebigem Wege schriftlich mitteilt, unter anderem durch eine über die E-Banking-Dienste übermittelte oder angezeigte Mitteilung.

Jede Nutzung der E-Banking-Dienste nach Mitteilung der Änderungen gilt als offizielle Annahme dieser Änderungen durch den Kunden.

Die Nichtigkeit oder Nichtanwendbarkeit einer der Bestimmungen der vorliegenden Zugangs- und Nutzungsbedingungen der E-Banking-Dienste beeinträchtigt in keiner Weise die Gültigkeit der übrigen Bestimmungen; diese bleiben auch ohne die gegebenenfalls für nichtig erklärten Bestimmungen weiterhin gültig.

16. Laufzeit und Kündigung des Vertrags

Der Vertrag über den Zugang und die Nutzung der E-Banking-Dienste ist unbefristet.

16.1. Kündigung durch den Kunden

Der Kunde kann seinen Zugang zu den E-Banking-Dienste jederzeit kostenlos und ohne Angabe von Gründen kündigen. Die Kündigung des Zugangs durch den kontoinhabenden Kunden zieht nicht die rechtsgültige Kündigung der mit seinen Bevollmächtigten oder Vertretern vereinbarten Zugänge nach sich. Zudem ist der Kunde für alle Transaktionen verantwortlich, die zum Zeitpunkt der Kündigung des Zugangs noch nicht auf dem Konto verbucht waren, ungeachtet dessen, ob sie von ihm selbst oder von seinem Vertreter oder Bevollmächtigten angewiesen wurden.

Die Kündigung des Zugangs zu den E-Banking-Diensten durch einen Bevollmächtigten oder Vertreter führt nicht zur Kündigung des Zugangs, der mit dem kontoinhabenden Kunden und gegebenenfalls mit anderen Bevollmächtigten oder Vertretern vereinbart wurde. Der kontoinhabende Kunde hat das Recht, den Zugang einer seiner Bevollmächtigten oder Vertreter zu kündigen. In solchen Fällen bleibt der kontoinhabende Kunde gesamtschuldnerisch und gemeinschaftlich für die von diesem Bevollmächtigten oder Vertreter bis zur Kündigung dieses Zugangs ausgeführten Vorgänge haftbar.

16.2. Kündigung durch die Bank

Die Bank kann den Zugang des Kunden zu den E-Banking-Diensten jederzeit kostenlos und ohne Angabe von Gründen fristlos kündigen. Bei Verbrauchern kann die Bank diesen Zugang unter Wahrung einer Kündigungsfrist von mindestens zwei Monaten kündigen.

Wenn die Bank den Zugang des Kunden kündigt, setzt sie den Kunden auf beliebigem Wege, den sie für angemessen hält, hiervon in Kenntnis.

Der Kunde ist für alle Transaktionen verantwortlich, die zum Zeitpunkt der Kündigung des Zugangs noch nicht auf dem Konto verbucht waren.

17. Annahme der Allgemeinen Geschäftsbedingungen von LuxTrust

Sofern sich der Kunde für einen LuxTrust-Zugang entscheidet, erklärt er, dass er von den Allgemeinen Geschäftsbedingungen sowie allen anderen Bedingungen, die für ihn und/oder die Bank in ihrer Geschäftsbeziehung zu LuxTrust im Rahmen dieses Zugangsverfahrens gelten (und auf der Website www.luxtrust.lu zur Verfügung stehen), Kenntnis genommen hat und damit einverstanden ist. Sofern sich der Kunde für einen alternativen, von LuxTrust anerkannten Zugang entscheidet, erklärt er, dass er von den Allgemeinen Geschäftsbedingungen sowie allen anderen Bedingungen seines Anbieters, die für ihn und/oder die Bank in ihrer Geschäftsbeziehung zu diesem Anbieter im Rahmen dieses Zugangsverfahrens gelten, Kenntnis genommen hat und damit einverstanden ist.

Anhang:
Hinweise zu den Risiken von Überweisungen über die E-Banking-Dienste (Online-Banking)

Hinweise zu den Risiken von Überweisungen über die E-Banking-Dienste (Online-Banking)

Diese Hinweise dienen der Information des Kunden über Risiken im Zusammenhang mit der Ausführung von elektronischen Überweisungen ohne Anspruch auf Vollständigkeit.

„Phishing“

„Phishing“ ist eine Methode von Onlinebetrügern, die sich als die Bank ausgeben, mit dem Ziel, an vertrauliche Informationen von Kunden zu gelangen.

Phishing per E-Mail oder SMS:
Mit dieser Technik imitieren Betrüger Mitteilungen oder Seiten von Websites, um an vertrauliche Daten zu Ihren Bankkonten wie etwa Ihre Kontonummer oder Ihre Zugangscodes zu gelangen. In einer E-Mail oder SMS an das potenzielle Opfer geben sie vor, sich im Auftrag einer Bank oder offiziellen Einrichtung an den Kunden zu wenden. Anlass sei angeblich die technische Aktualisierung der Website oder eine Überprüfung der persönlichen Daten. Der Empfänger soll auf einen in der E-Mail enthaltenen Hyperlink klicken und wird dann auf eine die offizielle Website der Bank imitierende Website geleitet. Hier soll er persönliche Benutzerkenndaten und Passwörter eingeben.

Verschickt werden auch E-Mails von fiktiven Lotterien, in denen dem potenziellen Opfer ein Gewinn angekündigt wird. Um diesen Gewinn zu erhalten, müsse dieser – so die Betrüger – lediglich seine persönlichen Bankdaten angeben.

Manche E-Mails fordern den Empfänger auch dazu auf, bei der Überweisung von Geldern behilflich zu sein. Der Absender bittet, das Konto des Empfängers als Durchgangskonto für einen größeren Geldbetrag nutzen zu können und verspricht eine prozentuale Beteiligung an der Summe. All diese Anfragen und Aufforderungen sind betrügerisch. Gehen Sie nicht darauf ein!

Phishing per Telefon:
Sie werden von einer Person angerufen, die vorgibt, ein Mitarbeiter der Bank zu sein.

Diese teilt Ihnen mit, Ihr Konto müsse aufgrund technischer Probleme geschlossen werden, wenn Sie ihr nicht persönliche Daten wie Kontonummer und Passwort mitteilen.

Identitätsdiebstahl

In diesen Fällen benutzt ein Betrüger absichtlich die Identität einer anderen Person, um betrügerische Handlungen vorzunehmen.

Um die Identität einer anderen Person annehmen zu können, muss er zuvor an persönliche und vertrauliche Informationen des Betrugsopfers gelangen.

Identitätsdiebstahl kann schwerwiegende Folgen haben und z. B. für Dokumentenfälschung, Kontobetrug und andere betrügerische Handlungen missbraucht werden.

So kann sich z. B. ein Betrüger, der Ihre E-Mail-Adresse stiehlt, Zugang zu Ihren E-Mails verschaffen und unter Ihrem Namen und unter Gebrauch Ihrer Ausdrucksweise Nachrichten an Ihre gespeicherten Kontakte senden, und somit das Vertrauen Ihrer Bekannten missbrauchen.

Schadsoftware

Schadsoftware, auch „Malware“, ist Software, die dazu entwickelt wurde, einem Computersystem vorsätzlich zu schaden oder Daten des Nutzers ohne sein Wissen abzugreifen.

Hiervon gibt es zahlreiche Formen: Viren, Würmer und Trojaner sind die bekanntesten Varianten (Viren werden installiert, wenn Sie eine infizierte Website besuchen oder wenn Sie einen Anhang in einer E-Mail oder einer SMS öffnen. Der Virus zeichnet dann z. B. Tastaturanschläge auf, um diese automatisch an die Betrüger weiterzuleiten).

Mit dem Fortschritt der Technologie wird auch diese Software immer komplexer.

Was Sie tun können:
Sicherheitshinweise zur Vermeidung von Risiken im Internet

Geben Sie Ihr Passwort oder Ihre persönlichen Benutzerkenndaten niemals an Dritte weiter!

Die Bank wird ihre Kunden nie auffordern, ihre Zugangscodes (Passwort, One Time Password oder sonstige vertrauliche Informationen) mitzuteilen – weder per E-Mail noch telefonisch, per SMS oder auf anderem Wege.

Schützen Sie Ihr Passwort!

Wählen Sie ein sicheres Passwort aus mindestens 8 Zeichen, mit Zahlen, Ziffern und Sonderzeichen, und ändern Sie es regelmäßig. Nutzen Sie für die verschiedenen Websites, die Sie besuchen (Online-Banking in anderen Banken, E-Mail, E-Commerce, soziale Netzwerke, Foren etc.), stets unterschiedliche Passwörter.

Schützen Sie Ihr Gerät!

Nutzen Sie zum Schutz ihres Zugangs zur E-Banking-Website oder der BL-Mobile-Banking-App immer ein vertrauenswürdiges Gerät (Computer, Smartphone, Tablet oder sonstiges), dessen Sicherheit Sie selbst bestimmen, und meiden Sie öffentliche Computer.

Wir empfehlen Ihnen daher:

– Installieren Sie eine Virenschutz- und Antispyware-Software, die regelmäßig automatisch aktualisiert wird.
– Installieren Sie aktuelle Updates Ihres Betriebssystems und Ihres Internetbrowsers.
– Verwenden Sie ausschließlich vertrauenswürdige Software.
– Aktivieren Sie Ihre Firewall.

So können Sie sicher sein, dass Sie sich wirklich auf der Online-Banking-Website der Bank befinden

Greifen Sie immer direkt auf die Website der Bank zu, indem Sie die Adresse https://www.banquedeluxembourg.com selbst in die Adresszeile Ihres Browsers eingeben und die Eingabe auf Tippfehler überprüfen, oder speichern Sie die Adresse in Ihren Favoriten und rufen Sie sie von dort aus auf. Folgen Sie niemals einem Link, der in einer E-Mail oder einer SMS enthalten ist.

– Klicken Sie auf „KUNDENZUGANG“ und wählen Sie dann Ihre Authentifizierungsoption aus.
– Überprüfen Sie, ob die Adresse mit „https“ beginnt.
– Überprüfen Sie, ob das Symbol eines Vorhängeschlosses oben oder unten auf der gesicherten Seite angezeigt wird.
– Doppelklicken Sie auf das Vorhängeschloss.
– In einem neuen Fenster wird das digitale Zertifikat der Bank angezeigt.
– Überprüfen Sie, ob der Name des Zertifikats wirklich „BANQUEDELUXEMBOURG.COM“ enthält.

Loggen Sie sich auf sichere Art aus und überprüfen Sie Ihre letzte Verbindung

Beenden Sie jede Verbindung mit dem Kundenbereich der E-Banking-Dienste, indem Sie auf „ABMELDEN“ klicken, und schließen Sie nach dem Besuch der E-Banking-Dienste und der Abfrage Ihrer Konten das Browserfenster. Datum und Uhrzeit der letzten Verbindung, die mit Ihren Benutzerkenndaten ausgeführt wurde, werden unter der Schaltfläche „ABMELDEN“ angezeigt. Denken Sie bitte auch daran, Ihre Kontobewegungen regelmäßig zu überprüfen.

Schützen Sie sich vor Phishing-Angriffen

Internetbetrüger imitieren E-Mails oder Websites vertrauenswürdiger Institutionen, um an vertrauliche Informationen wie Kreditkartennummer, Benutzerkenndaten, Passwort, Name, Vorname, Geburtsdatum, Anschrift, Telefonnummer etc. zu gelangen.

Meist geschieht dies durch gefälschte E-Mails, die angeblich von Banken oder offiziellen Stellen stammen und die angeblich einer technischen Aktualisierung der entsprechenden Website oder einer Überprüfung der persönlichen Daten dienen. Folgen Sie dem in der E-Mail angegebenen Hyperlink, werden Sie auf eine Seite weitergeleitet, die der offiziellen Seite einer vertrauenswürdigen Institution nachgebildet ist. Dort werden Sie aufgefordert, persönliche Daten einzugeben.

Um sich vor Phishing-Attacken zu schützen, lesen Sie die E-Mail und ihren Inhalt sowie die Absenderangaben gründlich.

Wir erinnern daran, dass die Bank – wie generell alle anderen Finanzinstitute – Kunden niemals per E-Mail oder telefonisch auffordern wird, Passwörter, Benutzerkenndaten oder ihr „One Time Password“ mitzuteilen.

Wenn Sie Ihre Zugangscodes verloren haben oder Fragen haben

Wenn Sie Ihre Zugangscodes verloren haben, kontaktieren Sie bitte umgehend LuxTrust (www.luxtrust.lu) bzw. den Anbieter Ihrer Authentifizierungslösung. Für andere Fragen zu Ihrem Konto und der BL-Mobile-Banking-App wenden Sie sich bitte an unser BL-Support-Team unter (+352) 26 20 26 30. Sie erreichen sie Montag bis Freitag von 8 bis 18 Uhr.