

Grundsätze für die Verarbeitung personenbezogener Daten

Die Bank in ihrer Eigenschaft als „Verantwortlicher“ (d. h. als die Einrichtung, die die Zwecke der Verarbeitung personenbezogener Daten und die diesbezüglichen Mittel festlegt) erfasst und verarbeitet die personenbezogenen Daten (d. h. alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen, die „personenbezogenen Daten“) die sich auf jeden Kunden beziehen. Die vorliegenden Grundsätze gelten für alle Kunden (d. h. sowohl für Kunden, die natürliche Personen sind, und ihre Bevollmächtigten, als auch für Vertreter/wirtschaftliche Eigentümer von juristischen Personen), sowie für Interessenten und potenzielle Kunden, die Interesse an den von der Bank angebotenen Produkten und Dienstleistungen zeigen.

Diese Grundsätze für die Verarbeitung personenbezogener Daten (i) beschreiben die Pflichten der Bank als Verantwortlicher, (ii) geben die Rechte jedes Kunden und potenziellen Kunden in Bezug auf die Verarbeitung ihrer personenbezogenen Daten an und (iii) enthalten die entsprechenden gesetzlich vorgeschriebenen Informationen.

Die Bank verarbeitet die personenbezogenen Daten im Einklang mit der Verordnung Nr. 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung, nachfolgend: die „Verordnung“).

Die Bank verpflichtet sich, die personenbezogenen Daten ihrer Kunden und Interessenten sowie aller natürlichen Personen, für die die Bank personenbezogene Daten verarbeitet, nicht zu verkaufen.

1 Kategorien von personenbezogenen Daten, die von der Bank verarbeitet werden

Im Rahmen der Erfüllung ihrer Aufgaben erhebt und verarbeitet die Bank die folgenden Kategorien von personenbezogenen Daten von Kunden und potenziellen Kunden, die im Zusammenhang mit den Dienstleistungen stehen, die sie in Anspruch genommen haben oder die sie im Begriff sind, in Anspruch zu nehmen:

- (i) personenbezogene Identifizierungsdaten (z. B. Name, Anschrift, Telefonnummern);
- (ii) persönliche Angaben (z. B. Geschlecht, Geburtsdatum);
- (iii) von Behörden ausgegebene Identifizierungsdaten (z. B. die Personalausweisnummer, die Steueridentifikationsnummer (TIN));
- (iv) elektronische Identifizierungsdaten (z. B. E-Mail-Adresse, IP-Adresse, elektronische Signatur);
- (v) biometrische Identifizierungsdaten (z. B. die dynamische Signatur);
- (vi) Bank- und Finanzidentifikationsdaten bei der BIL oder einem anderen Kreditinstitut oder Zahlungsdienstleister (z. B. Kontonummern, Kreditkartenummern);
- (vii) Finanzgeschäfte; bei der BIL oder einem anderen Kreditinstitut oder Zahlungsdienstleister durchgeführte Finanztransaktionen;
- (viii) Daten über die Finanzsituation des Kunden bei der BIL oder einem anderen Kreditinstitut oder Zahlungsdienstleister (z. B. Einkünfte, Vermögen, Vermögenswerte, Kredite, Ausgaben);
- (ix) Versicherungsdaten (z. B. Versicherungsgesellschaft, Versicherungstyp, Versicherungssumme);

- (x) Daten über die Tätigkeit der betroffenen Person (z. B. die Identität der Bevollmächtigten und andere Geschäftskontakte);
- (xi) Daten in Bezug auf die Gewohnheiten und Vorlieben (z. B. Daten, die bei Besuchen in einer Geschäftsstelle, bei der Navigation auf unserer Website www.bil.com und bei der Nutzung unserer Online-Formulare, bei der Anmeldung in unserem Online-Banking-Portal BILnet oder aufgrund von Schreiben, die von Kunden und potenziellen Kunden eingegangen sind, erhoben werden);
- (xii) Aufzeichnungen von elektronischen Mitteilungen, aufgrund derer Transaktionen getätigt werden oder getätigt werden sollen;
- (xiii) Videoaufzeichnungen aus Videoüberwachungssystemen, die in oder in der Nähe von Gebäuden und Anlagen, einschließlich der Geldautomaten, installiert sind;
- (xiv) Aufzeichnungen von Telefongesprächen.

Zur Erfüllung ihrer rechtlichen Verpflichtungen hinsichtlich der Bekämpfung von Geldwäsche und Terrorismusfinanzierung sowie ihrer Sorgfaltspflichten bei der Feststellung der Kundenidentität („know your customer“) und in den Fällen, in denen dies unbedingt erforderlich ist, verarbeitet die Bank Daten in Verbindung mit Verurteilungen und Straftaten und der Ausübung eines öffentlichen Amtes.

Die von der Bank verarbeiteten personenbezogenen Daten können (i) direkt vom Kunden oder Interessenten oder gegebenenfalls (ii) aus öffentlichen Quellen stammen, um ihren Sorgfaltspflichten gegenüber ihren Kunden nachzukommen.

2 Zweck der Verarbeitung personenbezogener Daten

Die personenbezogenen Daten werden oder können von der Bank verarbeitet werden, je nachdem, welche Dienstleistungen der Kunde oder potenzielle Kunde in Anspruch nimmt oder im Begriff ist, in Anspruch zu nehmen:

- (i) soweit diese Verarbeitung für die Erfüllung der Verträge zwischen der Bank und dem Kunden oder zur Durchführung von vorvertraglichen Maßnahmen auf Antrag des Kunden oder potenziellen Kunden notwendig ist. Die personenbezogenen Daten werden insbesondere im Hinblick auf die Aufnahme, Führung und Verwaltung der vertraglichen Beziehung sowie die Aktualisierung von Informationen über die Kunden oder potenziellen Kunden verarbeitet;
- (ii) soweit diese Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung der Bank erforderlich ist. Dies umfasst insbesondere die Bestimmungen über (i) die vorvertragliche Information des Kunden oder potenziellen Kunden über Anlagendienstleistungen in Bezug auf Finanzinstrumente (MiFID), (ii) die Berichtspflichten gegenüber den zuständigen luxemburgischen oder ausländischen Behörden, (iii) das angemessene Risikomanagement durch die Bank, (iv) Maßnahmen zur Verhinderung der Geldwäsche und Terrorismusfinanzierung (v) die Verpflichtung, „den Kunden zu kennen“ (KYC), (vi) die Verpflichtung, betrügerische Transaktionen aufzudecken, (vii) die Verpflichtung, Marktmissbrauch zu verhindern und (viii) die Verpflichtung zur Verhinderung jeglicher Betrugsversuche;
- (iii) soweit diese Verarbeitung notwendig ist für das berechnete Interesse der Bank, hochwertige

Dienstleistungen anzubieten, die immer besser auf die Anforderungen ihrer Kunden zugeschnitten sind, und zur Entwicklung von Geschäftsstrategien, aber auch im Rahmen der IT-Funktion der Bank, um ihre Tätigkeiten zu unterstützen;

- (iv) soweit diese Verarbeitung notwendig ist für das berechnete Interesse der Bank, die Sicherheit ihrer Mitarbeiter, ihrer Kunden und potenziellen Kunden zu gewährleisten, sowie die Vermögenswerte, für die sie verantwortlich ist, zu schützen, aber auch, um Unfälle aller Art zu verhindern;
- (v) soweit diese Verarbeitung auf der Einholung von Einwilligungen zu Prospektions- und Marketingzwecken in Bezug auf Bank-, Finanz- und Versicherungsprodukte oder andere von der Bank beworbene Produkte basiert.

3 Aufzeichnung von Telefongesprächen

Die Bank ist verpflichtet, Telefongespräche aufzuzeichnen, aufgrund derer Transaktionen getätigt werden oder getätigt werden sollen, um mehrere Verpflichtungen zu erfüllen:

- (i) Aufbewahrung des Belegs der Transaktionen, Überprüfung und/oder Bestätigung der telefonisch erteilten Aufträge und Anweisungen und/oder Klärung der Missverständnisse oder Berichtigung der Fehler bei der Annahme und Weiterleitung der Anweisungen;
- (ii) Nachweis, dass die Bank ihre Verpflichtungen gegenüber ihren Kunden gemäß der Richtlinie 2014/65/EU vom 15. Mai 2014 über Märkte für Finanzinstrumente („MiFID“) eingehalten hat; und
- (iii) Aufdecken jedes Verhaltens in Verbindung mit Insider-Geschäften und Marktmanipulationen gemäß der Verordnung Nr. 596/2014 vom 16. April 2014 über Marktmissbrauch.

4 Profiling und automatisierte Entscheidungen

Im Rahmen ihrer Tätigkeiten und um im besten Interesse ihrer Kunden zu handeln, beansprucht die Bank Profiling und trifft automatisierte Entscheidungen.

Das Profiling umfasst mehrere automatisierte Verarbeitungen von personenbezogenen Daten, die folgende Ziele verfolgen:

- (i) die Suche und die Bestimmung gemeinsamer Merkmale von Kunden, die sich für ein bestimmtes Bankprodukt oder eine bestimmte Bankdienstleistung (ob neuartig oder bereits vorhanden) interessieren könnten;
- (ii) die Suche und die Bestimmung einer Kundengruppe, die sich in Bezug auf die gehaltenen Produkte und/oder ihre Bankgeschäfte relativ gleichartig verhalten, sodass die Bank ihr Geschäft und ihre Kundschaft besser verstehen und ihr Angebot genauer anpassen kann;
- (iii) die Erfassung und Analyse von Informationen über die Kenntnisse und Finanzerfahrung von Kunden, ihre Risikotoleranz sowie ihre wirtschaftliche Situation, um ihnen entsprechend unseren aufsichtsrechtlichen Verpflichtungen in Bezug auf den Anlegerschutz ein Profil zuzuweisen und geeignete Anlageprodukte vorzuschlagen;
- (iv) die Steuerung des Risikos, dem die Bank ausgesetzt ist, anhand einer Analyse des Bankverhaltens der Kunden (beispielsweise die Verwendung von Kreditkarten im Vergleich zur Rückzahlungsfähigkeit) sowie einer besseren Inkenntnissetzung der Kunden in Bezug auf ihre Finanzsituation und das Risiko, mit dem bestimmte ihrer Anträge verbunden sind (darunter Anträge auf die Erhöhung des Kreditkartenlimits); und

- (v) die Bekämpfung von Betrug, Geldwäsche und Terrorismusfinanzierung anhand einer Analyse der Bankgewohnheiten der Kunden (u. a. Transaktionsverlauf), die auf einer Reihe vordefinierter Kriterien (beispielsweise Zielländer der in den vorangegangenen sechs Monaten getätigten Transaktionen) basiert und mittels derer verdächtige Verhaltensweisen aufgedeckt werden können.

Die Bank hat bestimmte Entscheidungsfindungsprozesse automatisiert, um die Bearbeitung von Anträgen zu beschleunigen und ihre Objektivität sicherzustellen. Dies gilt für Anträge auf Änderung des Kartenlimits sowie das Überziehungsmanagement. Die der Entscheidung zugrunde liegende Logik basiert demnach auf einer Analyse des Bankverhaltens des Kunden sowie seinen Vermögenswerten und Verbindlichkeiten.

Im Rahmen dieser automatisierten Entscheidungen hat der Kunde das Recht, von der Bank die erneute Prüfung seiner Situation zu verlangen durch das Recht auf menschliches Eingreifen.

5 Personenbezogene Daten über Dritte

Ein Kunde, der der Bank personenbezogene Daten in Bezug auf Dritte (beispielsweise seine Verwandten, Bevollmächtigte, gesetzliche Vertreter, Mitarbeiter, Gesellschafter, Manager, Verwalter oder sogar wirtschaftliche Eigentümer) mitteilt, muss hierzu von diesen Dritten ermächtigt werden und diese informieren, dass die Bank zum selben Zweck und nach denselben Modalitäten, wie in den vorliegenden Grundsätzen für die Verarbeitung personenbezogener Daten aufgeführt, eine Verarbeitung der personenbezogenen Daten vornimmt.

6 Erfassung und Verarbeitung personenbezogener Daten

Die Bank erfasst lediglich die Informationen, die der Pflege der Kundenbeziehung dienen, und dies unter Einhaltung der gesetzlichen Verpflichtungen.

Die personenbezogenen Daten werden beim Kunden (z. B. bei der Kontoeröffnung, per Fragebogen) und bei Dritten (je nach Dienstleistung z. B. bevollmächtigte Rechtsanwälte, bevollmächtigte Notare oder bestimmte nationale Behörden) erhoben.

Die Weigerung, der Bank die personenbezogenen Daten mitzuteilen, und ein der Bank gegenüber ausgesprochenes Verbot zur Verarbeitung dieser Daten, das im freien Ermessen des Kunden liegt, könnten die Fortsetzung einer Geschäftsbeziehung mit der Bank oder die Bereitstellung bestimmter Produkte oder Dienstleistungen durch die Bank verhindern.

7 Personen, die ein Zugriffsrecht auf die personenbezogenen Daten haben, und Zweck dieses Zugriffsrechts

Die personenbezogenen Daten können von der Bank an die folgenden Kategorien von Empfängern übermittelt werden:

- (i) andere Finanzinstitute, einschließlich Banken, Versicherungsgesellschaften, Steuerberatungsgesellschaften, Herausgeber von Zahlungs- und Kreditkarten, Verwalter von Plattformen für den Nachrichtenaustausch zwischen Banken, Anbieter von Online-Zahlungslösungen; dabei handeln sämtliche dieser Institutionen als Verantwortliche im Rahmen der von der Bank angebotenen Dienstleistungen und Produkte (z. B. Abwicklung einer Transaktion mit einem Finanzinstrument, Angebot eines Versicherungsprodukts, Bereitstellung einer Kreditkarte, Ausführung von Tätigkeiten als Wertpapierverwahrstelle, Intervention als Bank des Empfängers einer Überweisung sowie Erstellung eines Steuerberichts);

- (ii) externe Dienstleister, deren Heranziehung im Rahmen der den Kunden erbrachten Dienstleistungen, insbesondere im Bereich der Banken-Schnittstellen (zum Beispiel Einordnung der Transaktionen in Kategorien und Konten-Aggregation), im Bereich Informationstechnologien (zum Beispiel Verwaltung der operativen IT-Aufgaben sowie Verwaltung und Hosting der technischen Infrastruktur), im Bereich der physischen Sicherheit (zum Beispiel Bargeldtransport oder Verwaltung der Videoüberwachungstätigkeiten), in den Bereichen Druck (zum Beispiel Ausdrucken der Kontoauszüge), Dokumenten- und Datenmanagement (zum Beispiel sichere Vernichtung von Dokumenten, Qualitätskontrolle und Aufbewahrung von Dokumenten und Daten), im Bereich Beratung (zum Beispiel im Rahmen der Entwicklung von neuen Produkten und Dienstleistungen) sowie im Bereich Kommunikation (zum Beispiel Verwaltung der Mailings) erforderlich ist; dabei handeln sämtliche dieser Dienstleister als Auftragsverarbeiter für Rechnung der Bank;
- (iii) externe Dienstleister, deren Heranziehung im Rahmen der gesetzlichen und regulatorischen Verpflichtungen der Bank, insbesondere hinsichtlich der Feststellung der Kundenidentität („know your customer“) (zum Beispiel über Berichte, in welchem Fall der Dienstleister als Verantwortlicher handelt), der Identifizierung von Kunden, die möglicherweise Aktionäre bestimmter Unternehmen sind, sowie zur leichteren Ausübung ihrer Stimmrechte (z. B. durch die Übermittlung von Positionsaufstellungen an europäische Emittenten und von Informationen zu den Hauptversammlungen an die Kunden), der Meldepflichten (zum Beispiel Aufbereitung der Transaktionsberichte für die Finanzaufsichtsbehörde, in welchem Fall der Dienstleister als Auftragsverarbeiter handelt) und der Pflichten der Abschlussprüfung und der Bestätigung der ordnungsgemäßen Rechnungslegung der Bank (in welchem Fall der Abschlussprüfer als Verantwortlicher handelt), erforderlich ist.

Diese Empfänger personenbezogener Daten sind verpflichtet, die gesetzlichen und vertraglichen Verpflichtungen im Bereich des Schutzes personenbezogener Daten einschließlich des Berufsgeheimnisses oder der einschlägigen Geheimhaltungspflichten einzuhalten.

Die Bank kann außerdem personenbezogene Daten übermitteln, wenn sie dazu gemäß einer gesetzlichen oder regulatorischen Verpflichtung oder gemäß einer Auflage einer Behörde innerhalb der gesetzlichen Grenzen verpflichtet ist.

Gemäß den gesetzlichen und regulatorischen Verpflichtungen, die für den obligatorischen Informationsaustausch in Steuersachen mit den beteiligten Ländern gelten, kann die Bank bestimmte personenbezogene Daten des Kunden den luxemburgischen Steuerbehörden mitteilen. Die luxemburgischen Steuerbehörden können die von der Bank übermittelten Daten an jede gemäß den gesetzlichen und regulatorischen Verpflichtungen zuständige ausländische Steuerbehörde weiterleiten.

In bestimmten Ländern verlangen die geltenden gesetzlichen und regulatorischen Bestimmungen über Finanzinstrumente (bzw. Geschäfte mit Finanzinstrumenten) und ähnliche Vorschriften die Offenlegung der Identität der (in)direkten Inhaber oder der wirtschaftlich Begünstigten dieser Instrumente und ihrer Positionen in diesen Instrumenten. Die Nichteinhaltung dieser Verpflichtungen kann die Sperrung der Finanzinstrumente zur Folge haben (was dazu führen kann, dass die Stimmrechte nicht ausgeübt, Dividenden oder sonstige Erträge nicht eingestrichen oder Finanzinstrumente nicht verkauft oder anderweitig veräußert werden können) oder eine beliebige andere Strafe oder

Restriktion, die in den o.g. Bestimmungen vorgesehen ist, nach sich ziehen.

Im Falle der Anlage in dieser Art von Finanzinstrumenten muss der Kunde die geltenden gesetzlichen und regulatorischen Bestimmungen einhalten. In diesem Zusammenhang erteilt der Kunde der Bank ausdrücklich die Vollmacht, nach eigenem Ermessen die Identität des Kunden und/oder des wirtschaftlich Begünstigten sowie deren Positionen in den genannten Finanzinstrumenten offenzulegen.

Schließlich kann die Bank die personenbezogenen Daten auch auf Anweisung des Kunden übermitteln.

Grundsätzlich werden personenbezogene Daten von der Bank und ihren Dienstleistern innerhalb der Europäischen Union gespeichert.

Bei jeder Übermittlung personenbezogener Daten, die sich als notwendig erweist, stellt die Bank sicher, dass ein Angemessenheitsbeschluss der Europäischen Kommission vorliegt oder gegebenenfalls geeignete Garantien vorhanden sind (z. B. die Annahme der Einhaltung von Standarddatenschutzklauseln, der Einhaltung eines Verhaltenskodex oder auch der Erlangung einer Zertifizierung).

8 Rechte natürlicher Personen

Jede natürliche Person hat das Recht, den Zugang zu ihren personenbezogenen Daten zu verlangen und eine Kopie davon zu erhalten, und das Recht auf Berichtigung dieser personenbezogenen Daten, falls sie unzutreffend oder unvollständig sein sollten.

Darüber hinaus besitzt sie unter den Bedingungen und innerhalb der Grenzen, die von der Verordnung vorgesehen sind und sich insbesondere aus den gesetzlichen und vertraglichen Verpflichtungen der Bank ergeben, das Recht auf Einschränkung der Verarbeitung der personenbezogenen Daten, das Recht, ihrer Verwendung zu widersprechen, sowie das Recht, von dem Verantwortlichen ihre Löschung zu verlangen. Die natürliche Person kann in jedem Fall ohne Angabe von Gründen, die Einwilligung zu der Verarbeitung ihrer personenbezogenen Daten für Direktwerbung zurückziehen. Die Verwaltung der Einwilligung kann jederzeit über BILnet erfolgen.

Sie besitzt außerdem ein Recht auf Übertragbarkeit ihrer personenbezogenen Daten, d. h. das Recht, die sie betreffenden personenbezogenen Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten oder ihre Übermittlung an einen anderen Verantwortlichen zu verlangen.

Die natürliche Person kann die Einwilligung, die sie erteilt hat, falls die Bank zuvor eine Einwilligung zur Verarbeitung ihrer personenbezogenen Daten verlangt hat, jederzeit widerrufen. Die Rechtmäßigkeit der Verarbeitung, die auf der vor dem Widerruf erteilten Einwilligung basiert, wird davon nicht berührt.

Natürliche Personen können von ihren Rechten mittels schriftlichem, unterzeichnetem Antrag unter Beifügung eines Identitätsnachweises Gebrauch machen:

- über die sichere E-Mail-Plattform in BILnet mit dem Betreff „Datenschutz – Antrag zur Ausübung von Rechten“
- per E-Mail an die Adresse dpo@bil.com
- mittels dem Formular auf BIL.com der unter dem folgenden Link verfügbar ist :
<https://survey.bil.com/?e=328967&d=l&h=7FB269DAC3609B7&l=de>
- per Post an folgende Anschrift: Client Care Center, 69, route d'Esch, L-2953 Luxembourg.

Im Falle einer offensichtlich unbegründeten oder übermäßigen Anfrage behält sich die Bank jedoch das Recht vor, die Zahlung

angemessener Gebühren zu verlangen, die den Verwaltungsaufwand berücksichtigen, der durch die Bereitstellung der Informationen, die Durchführung der Mitteilungen oder die Ergreifung der angeforderten Maßnahmen entsteht. Ab dem dritten Antrag im laufenden Jahr, beginnend mit dem Zeitpunkt des ersten Antrags, gilt jede zusätzliche Anfrage als überhöht. Die Bank kann daher die Zahlung von Gebühren verlangen, die den Recherchegebühren entsprechen, die in ihrer auf BIL.com verfügbaren Preisliste festgelegt sind.

Wenn die erhaltene Antwort für sie nicht ganz zufriedenstellend war oder noch Fragen zum Datenschutz bestehen, hat die natürliche Person die Möglichkeit, sich an den Datenschutzbeauftragten zu wenden, indem sie ihm entweder eine Nachricht über die sichere E-Mail-Plattform in BILnet sendet oder per E-Mail an die folgende Adresse : dpo@bil.com oder per Post an die folgende Adresse: Datenschutzbeauftragter, 69 route d'Esch L-2953 Luxemburg.

Ferner kann auch bei der Nationalen Kommission für den Datenschutz per Post unter der Anschrift 15, boulevard du Jazz, L-4370 Belvaux Beschwerde eingereicht werden, oder indem das Online-Formular auf der Website der CNPD im Bereich „Ihre Rechte“ -> „Ihre Rechte geltend machen“ ausgefüllt wird.

9 Speicherfrist personenbezogener Daten

Die personenbezogenen Daten werden von der Bank nicht länger als für die von der Bank verfolgten Zwecke notwendig und im

Einklang mit ihren gesetzlichen Verpflichtungen gespeichert, d. h. 10 Jahre nach der Beendigung der Geschäftsbeziehung mit den Kunden.

Die personenbezogenen Daten von potenziellen Kunden werden für einen Zeitraum von 2 Jahren ab dem Datum ihrer Erhebung gespeichert.

In Ausnahmefällen (gesetzliche Unterbrechung und Aussetzung der Aufbewahrungsfristen) kann die Bank die Daten über die oben genannten Zeiträume hinaus speichern, wobei sie die geltenden gesetzlichen Bestimmungen einhalten muss.

10 Sicherheit der personenbezogenen Daten

Die Bank schützt die personenbezogenen Daten und wahrt ihre Vertraulichkeit. Dazu setzt die Bank organisatorische und technische Maßnahmen um, darunter:

- die Information und Schulung der Mitarbeiter der Bank in Bezug auf ihre Verpflichtungen im Bereich Datenschutz;
- die Berücksichtigung der Auswirkungen im Bereich Datenschutz bereits bei der Konzeption der von der Bank angebotenen Produkte, Dienstleistungen und Systeme;
- die Einführung von Rahmenbedingungen für die Gewährleistung der Informationssicherheit;
- die vertragliche Pflicht, dass die Auftragsverarbeiter der Bank ein Datenschutzniveau bieten und umsetzen, das mit dem von der Datenschutz-Grundverordnung vorgeschriebenen vergleichbar ist.