

## Informationen zum Datenschutz

Wir informieren Sie hiermit über die Verarbeitung Ihrer personenbezogenen Daten und die Ihnen zustehenden datenschutzrechtlichen Ansprüche und Rechte. Inhalt und Umfang der Datenverarbeitung richten sich maßgeblich nach den jeweils von Ihnen beantragten bzw. mit Ihnen vereinbarten Produkten und Dienstleistungen.

### 1. Wer ist für die Datenverarbeitung verantwortlich und an wen können Sie sich wenden?

#### Verantwortliche Stelle

Alpen Privatbank AG  
Walsersstraße 61  
6991 Riezlern, Österreich  
T +43 (5517) 350-0  
info@alpenprivatbank.com  
www.alpenprivatbank.com

#### Datenschutzbeauftragter

Alpen Privatbank AG  
Datenschutzbeauftragter  
Walsersstraße 61  
6991 Riezlern, Österreich  
T +43 (5517) 350-0  
datenschutz@alpenprivatbank.com.

### 2. Welche Daten werden verarbeitet und aus welchen Quellen stammen diese?

(Datenschutzinformation gem. Art. 14 DSGVO im Falle indirekter Datenerhebung)

Wir verarbeiten neben jenen personenbezogenen Daten, die wir von Ihnen insbesondere im Rahmen unserer Geschäftsbeziehung erhalten, auch Daten, die wir aus öffentlich zugänglichen Quellen (z. B. Firmenbuch, Vereinsregister, Grundbuch oder Medien) von Finanzauskunfteien und Schuldnerverzeichnissen zulässigerweise erhalten haben oder die uns von anderen, mit der Bank verbundenen Unternehmen oder von sonstigen Dritten berechtigt übermittelt werden.

Zu den personenbezogenen Daten zählen Ihre persönlichen Detailangaben und Kontaktdaten (z. B. Name, Adresse, Geburtstag und -ort, Staatsangehörigkeit etc.) oder Legitimationsdaten (z. B. Daten zu Identitäts- und Reisedokumenten) und Authentifikationsdaten (z. B. Unterschriftsprobe).

Darüber hinaus können darunter auch

- Zahlungsverkehrs- und Clearing-Daten (z. B. Zahlungsaufträge, Umsatzdaten im Zahlungsverkehr),
- Bonitätsdaten (z. B. Art und Höhe der Einkünfte),
- wiederkehrende Zahlungsverpflichtungen für Ausbildungskosten der Kinder (Kredittilgungen, Mieten),
- Versicherungs- und Schadensdaten,
- Daten zu Marketing und Vertrieb, zu Kreditgeschäften, elektronische Protokoll- und Identifikationsdaten (Apps, Cookies etc.),
- Finanzidentifikationsdaten (Daten von Kredit-, Debit-, Prepaidkarten)
- AML- (Anti Money Laundering) und Compliance-Daten sowie
- andere, mit den genannten Kategorien vergleichbare Daten, fallen.

### 3. Für welche Zwecke und auf welcher Rechtsgrundlage werden die Daten verarbeitet?

(Datenschutzinformation gem. Art. 13 und 14 DSGVO)

Wir verarbeiten Ihre personenbezogenen Daten im Einklang mit den Bestimmungen der Europäischen Datenschutzgrundverordnung (DSGVO) und dem Datenschutzgesetz 2018.

#### – Zur Erfüllung vertraglicher Pflichten (Art. 6 Abs. 1b DSGVO)

Die Verarbeitung (Art. 4 Z 2 DSGVO) personenbezogener Daten (Art. 4 Z 1 DSGVO) erfolgt zur Erbringung und Vermittlung von Bankgeschäften, Finanzdienstleistungen sowie Versicherungs-, Leasing- und Immobiliengeschäften, insbesondere zur Durchführung unserer Verträge mit Ihnen und der Ausführung Ihrer Aufträge, sowie zur Durchführung vorvertraglicher Maßnahmen.

Die Zwecke der Datenverarbeitung richten sich in erster Linie nach dem konkreten Produkt (z. B. Konto, Kredit, Wertpapiere, Einlagen, vermittelte Produkte, wie etwa Versicherungspolizzen, Leasing- oder Bausparverträge). Diese können u. a. Bedarfsanalysen, Beratung, Angebot- oder Antragserstellung, Vermögensverwaltung und -betreuung sowie die Durchführung von Transaktionen umfassen. Derartige Datenverarbeitungen erfolgen z. B. im Zusammenhang mit Debitkarten (auch „Bankomatkarten“), die die Bank Ihnen zur Verfü-

---

gung stellt und mit denen es Ihnen insbesondere möglich ist, Zahlungstransaktionen bei Händlern an POS-Terminals („Bankomatkassen“) und im Internet (E-Commerce-Zahlungen im Online-Shop) durchzuführen, Bargeld an dafür vorgesehenen Geldausgabeautomaten (auch „Bankomat“) zu beheben oder Transaktionen zwischen Debitkarten („ZOIN“) durchzuführen. Diese Transaktionen müssen den Kreditinstituten des Karteninhabers und Zahlungsempfängers zugeordnet werden können, damit diese untereinander die Transaktionen abrechnen können. Nahezu alle in Österreich tätigen Institute haben zu diesem Zweck gemeinsam mit der Payment Services Austria GmbH (PSA) einen Vertrag abgeschlossen (PSA-Vertrag).

Ziel dieses Vertrags ist es, die wechselseitigen Rechte und Pflichten der Institute und der PSA zu regeln. Darin vereinbaren die Institute die Bedingungen, zu denen Transaktionen (z. B. Geldbehebungen) fremder Bankkunden auf eigenen Geldausgabeautomaten oder Zahlungstransaktionen an POS-Terminals akzeptiert werden. PSA obliegt die technische Abwicklung der Transaktionen mit einsetzbaren Karten mit den Instituten. Darüber hinaus betreibt PSA auch eigene Geldausgabeautomaten. Zur Abwicklung der Transaktionen und zur Verrechnung zwischen den Instituten müssen die Institute Daten ihrer eigenen Kunden verarbeiten. Die Rechtsgrundlagen der Datenverarbeitung sind eine Vielzahl von Gesetzen, wie z. B. das Bankwesengesetz, das Zahlungsdienstegesetz, das Finanzmarkt-Geldwäschegesetz etc., zu deren Einhaltung die Vertragspartner des PSA-Vertrags verpflichtet sind, und der Vertrag, der zwischen dem Institut und dessen Kunden (z. B. Girokontovertrag, Kartenvertrag) abgeschlossen wurde. Zur Ausübung Ihrer Rechte im Zusammenhang mit den in diesem Absatz angesprochenen Datenverarbeitungen wenden Sie sich bitte an Ihre Bank.

Die konkreten Einzelheiten zum Zweck der Datenverarbeitungen können Sie den jeweiligen Vertragsunterlagen und Geschäftsbedingungen entnehmen.

– **Zur Erfüllung rechtlicher Verpflichtungen (Art. 6 Abs. 1c DSGVO) oder im öffentlichen Interesse (Art. 6 Abs. 1e DSGVO)**

Eine Verarbeitung personenbezogener Daten kann zum Zweck der Erfüllung unterschiedlicher gesetzlicher Verpflichtungen und öffentlicher Interessen (wie etwa aus dem Bankwesen- oder Finanzmarkt-Geldwäschegesetz, dem Wertpapieraufsichts- oder Börsegesetz, der Gewerbeordnung, den Standesregeln für Versicherungsvermittler, dem Versicherungsvertragsgesetz) sowie aufgrund aufsichtsrechtlicher Vorgaben (z. B. der Europäischen Zentralbank, der Europäischen Bankenaufsicht, der Österreichischen Finanzmarktaufsicht), welchen die Bank als österreichisches Kreditinstitut unterliegt, erforderlich sein.

Beispiele für solche Fälle sind:

- Meldungen an die Geldwäschemeldestelle in bestimmten Verdachtsfällen (§ 16 FM-GwG).

Die Bank hat gem. FM-GwG u. a. die Identität von Kunden, wirtschaftlichen Eigentümern von Kunden oder allfälligen Treugebern des Kunden festzustellen und zu prüfen, den vom Kunden verfolgten Zweck und die vom Kunden angestrebte Art der Geschäftsbeziehung zu bewerten, Informationen über die Herkunft der eingesetzten Mittel einzuholen und zu prüfen sowie die Geschäftsbeziehung und die in ihrem Rahmen durchgeführten Transaktionen kontinuierlich zu überwachen. Die Bank hat insbesondere Kopien der erhaltenen Dokumente und Informationen, die für die Erfüllung der beschriebenen Sorgfaltspflichten erforderlich sind, und die Transaktionsbelege und -aufzeichnungen, die für die Ermittlung von Transaktionen erforderlich sind, aufzubewahren.

Das FM-GwG räumt der Bank die gesetzliche Ermächtigung im Sinne der DSGVO zur Verwendung der genannten Daten der Kunden im Rahmen der Ausübung der Sorgfaltspflichten zur Verhinderung von Geldwäscherei und Terrorismusfinanzierung ein, zu denen die Bank gesetzlich verpflichtet ist und die dem öffentlichen Interesse dienen. Die Datenverarbeitungen im Rahmen der beschriebenen Sorgfaltspflichten beruhen auf einer gesetzlichen Verpflichtung der Bank.

- Datenverarbeitung aufgrund des Gemeinsamen Meldestandard-Gesetzes (GMSG)

Das GMSG verpflichtet die Bank, die steuerliche/n Ansässigkeit/en ihrer Kunden festzustellen und dabei die Daten ihrer Kunden (natürliche und juristische Personen) zu prüfen bzw. steuerliche Selbstauskünfte ihrer Kunden einzuholen. Bei Feststellung einer steuerlichen Ansässigkeit in einem anderen Staat, der am automatischen Informationsaustausch zur Bekämpfung der Steuerhinterziehung teilnimmt, sind von der Bank bestimmte Daten des Kunden (z. B. Identitätsdaten, Kontaktdaten, Daten zu Konto und Depot) an die österreichischen Finanzbehörden zu melden, die diese an die zuständigen ausländischen Finanzbehörden weiterleiten. Bei juristischen Personen umfasst eine Meldung zusätzlich die Identitäts- und Kontaktdaten der den Kunden allenfalls beherrschenden Personen.

- Auskunftserteilung an die FMA nach dem WAG und dem BörseG, z. B. um die Einhaltung der Bestimmungen über den Marktmissbrauch von Insiderinformationen zu überwachen,
- Auskunftserteilung an Finanzstrafbehörden im Rahmen eines Finanzstrafverfahrens wegen eines vorsätzlichen Finanzvergehens,
- Auskunftserteilung an Abgabenbehörden des Bundes gem. § 8 des Kontenregister- und Konteneinschaugesetzes,
- Bewertung und Steuerung von bankgeschäftlichen Risiken,

- Maßnahmen zu Betrugsprävention und -bekämpfung (Fraud Transaction Monitoring), zur Bekämpfung von Geldwäsche, Terrorismusfinanzierung und vermögensgefährdenden Straftaten. Dabei werden auch Datenauswertungen (u. a. im Zahlungsverkehr) vorgenommen. Diese Maßnahmen dienen zugleich auch Ihrem Schutz.
- Aufzeichnung von Bild- und Tonaufnahmen und sonstiger elektronischer Kommunikation bei Wertpapiergeschäften gem. MiFID II,
- Datenübermittlung an unser Einlagensicherungs- und Anlegerentschädigungssystem (§ 93 BWG),
- Bonitätsprüfung (Kredit-Scoring) bei Kreditvergabe.

Bei diesem Kredit-Scoring wird mithilfe statistischer Vergleichsgruppen das Ausfallrisiko von Kreditsuchenden bewertet. Der errechnete „Score-Wert“ soll eine Prognose ermöglichen, mit welcher Wahrscheinlichkeit ein beantragter Kredit voraussichtlich zurückbezahlt wird. Zur Berechnung dieses Score-Werts werden Ihre Stammdaten (Familienstand, Anzahl Kinder, Dauer der Beschäftigung, Arbeitgeber), Angaben zu den allgemeinen finanziellen Verhältnissen (Einkommen, Vermögen, monatliche Ausgaben, Höhe der Verbindlichkeiten, Sicherheiten etc.) und zum Zahlungsverhalten (ordnungsgemäße Kreditrückzahlungen, Mahnungen, Daten von Kreditauskunfteien) herangezogen. Ist das Ausfallrisiko zu hoch, kann es zu einer Ablehnung des Kreditantrags kommen.

#### – Im Rahmen Ihrer Einwilligung (Art. 6 Abs. 1a DSGVO)

Wenn Sie uns eine Einwilligung zur Verarbeitung Ihrer personenbezogenen Daten für bestimmte Zwecke (z. B. Weitergabe von Daten an die in der Einwilligung genannten Empfänger, Benachrichtigungen per ELBA-Mailbox) erteilt haben, erfolgt eine Verarbeitung nur gemäß den in der Zustimmungserklärung festgelegten Zwecken und im darin vereinbarten Umfang. Eine erteilte Einwilligung kann mit Wirkung für die Zukunft jederzeit widerrufen werden. Der Widerruf der Einwilligung berührt nicht die Rechtmäßigkeit der bis zum Widerruf verarbeiteten Daten.

Beispiele für solche Fälle sind:

- die Auswertung Ihrer Daten (z. B. Name, Alter, Kontoumsatzdaten und dergleichen) und die Abfrage externer Bonitätsdatenbanken (Kreditschutzverband von 1870, CRIF GmbH), um für Kreditangebote, die Ihnen die Bank aus eigenem stellt, vorweg Ihre Kreditwürdigkeit zu beurteilen.
- die Auswertung von Daten zu Ihren Geschäftsbeziehungen mit anderen Banken (Konten, Kredite, Veranlagungen) und zu Ihrem daraus ableitbaren Zahlungsverhalten, auf die die Bank zugreifen kann, weil Sie von der Möglichkeit Gebrauch gemacht haben, diese Geschäftsbeziehungen in Ihr Electronic Banking bei der Bank einzubeziehen.

#### – Zur Wahrung berechtigter Interessen der Bank oder Dritter (Art. 6 Abs. 1f DSGVO)

Soweit erforderlich, kann im Rahmen von Interessensabwägungen zugunsten der Bank oder Dritter eine Datenverarbeitung zur Wahrung berechtigter Interessen erfolgen.

Beispiele für solche Fälle sind:

- Konsultation der Finanzauskunfteien (z. B. Österreichischer Kreditschutzverband 1870) und Nutzung der eingemeldeten Daten zur Ermittlung von Bonitäts- bzw. Ausfallrisiken,
- Prüfung und Optimierung von Verfahren zur Bedarfsanalyse und direkter Kundenansprache,
- Aufbewahrung von Kundendaten im Rahmen der Vermittlung von Versicherungsprodukten zur Überprüfung von Kundenansprüchen aus der Beraterhaftung bei der Vermittlungstätigkeit,
- Übermittlung von allgemein gehaltenen banküblichen Auskünften nach § 38 Abs. 2 Z. 6 BWG bei unternehmerisch tätigen natürlichen Personen (z. B. Einzelunternehmer),
- Daten werden im Rahmen der Videoüberwachung der öffentlich zugänglichen (Bank-)Räumlichkeiten (insbesondere der Kassen- und Safe-Räume, Foyers, Gänge, Stiegen, Aufzugsbereiche, Eingangsbereiche innen/außen, Fassaden, Garagen) sowie der vom Verantwortlichen betriebenen Geldausgabeautomaten (auch im Außenbereich des Bankgebäudes) verarbeitet. Dies erfolgt zum Zweck des Eigenschutzes (Schutz des Eigentums und Schutz der Arbeitnehmer des Verantwortlichen) und des Verantwortungsschutzes (Wahrnehmung von Verkehrssicherungspflichten, Vertragshaftung gegenüber Kunden etc.) sowie zum Zweck der Verhinderung bzw. Eindämmung und Aufklärung strafrechtlich relevanten Verhaltens.
- bestimmte Telefonaufzeichnungen (für Qualitätssicherungsmaßnahmen oder bei Beschwerdefällen),
- Maßnahmen zur Geschäftssteuerung und Weiterentwicklung von Dienstleistungen und Produkten,
- Datenverarbeitung für Zwecke der Rechtsverfolgung, Geltendmachung fremder rechtlicher Ansprüche und eigener Interessen, Verteidigung bei rechtlichen Streitigkeiten,
- Gewährleistung der IT-Sicherheit und des IT-Betriebs der Bank,
- Marketing für Produkte und Dienstleistungen.

Folgende Daten, welche die Bank selbst erhoben hat oder welche Sie an die Bank übertragen haben, werden ausgewertet, um Ihnen individuelle Informationen und Angebote zu übermitteln und um die Dienstleistungen und Produkte der Bank weiterentwickeln zu können:

#### **Persönliche Daten/Stammdaten**

Geschlecht, Titel, Name, Geburtsdatum, Geburtsland, Staatsbürgerschaft, Familienstand, Steuerstatus, Ausbildung, Beruf, Arbeitgeber, Legitimationsdaten wie etwa Führerscheindaten, Einkommensdaten, Adress- und sonstige Kontaktdaten wie Telefonnummer oder E-Mail-Adresse und Postanschrift, geografische Standortinformationen, Wertpapier-Risikoklasse gem.

---

Anlegerprofil, Wohnsituation wie Miete oder Eigentum und Wohnung oder Haus, Familienbeziehungen (ohne personenbezogene Daten dieser Personen), Anzahl der Personen im Haushalt, bei Beratungsgesprächen bekanntgegebene Daten wie z. B. Hobbys und Interessen oder geplante Anschaffungen, Auto, Haushaltsrechnungen, interne Ratingeinstufungen wie die Bewertung der Einnahmen- und Ausgabensituation und der Vermögens- und Verbindlichkeiten-Situation durch die Bank.

#### **Produkt- und Dienstleistungsdaten der Bank**

Daten zu den von Ihnen genutzten Dienstleistungen der Bank einschließlich

- von Ihnen verwendete Zahlungsmittel wie Bankomat- und Kreditkarten,
- Soll- und Haben- sowie Zahlungsrückstände zu Konten und Krediten,
- im Rahmen dieser Dienstleistungen verrechnete Zinssätze und Entgelte oder Spesen,
- Zahlungsverhalten einschließlich von Ihnen genutzter Möglichkeiten der Auftragserteilung (z. B. Mein ELBA),
- ein- und ausgehende Zahlungsverkehrstransaktionen, Empfänger, Absender und Zahlungsaufträge übermittelnde Dienstleister, Beträge, Verwendungszwecke und Zahlungsreferenzen, Auftraggeber-Referenzen,
- Häufigkeit und Art der Geldbewegungen, bei bargeldlosen Zahlungen, die Daten der Zahlungen erhaltenden Händler oder Dienstleister und Informationen zu diesen abgeschlossenen Geschäften,
- Daten aus Mein ELBA (das sind Nutzungs- und Inhaltsdaten aus Mein ELBA, dem Mein ELBA-Finanzplaner und der Mein ELBA-Mailbox),
- Sparverhalten, Wertpapiertransaktionen und Depotstände einschließlich Details zu gehaltenen Wertpapieren.

#### **Geräte- und Contact-Center-Daten**

##### **(Telefonservice inkl. Sprachsteuerungscomputer)**

Häufigkeit, Zeitpunkte und Orte der Nutzung von Selbstbedienungsgeräten und Contact-Centern (Telefonservices inkl. Sprachsteuerungscomputer) oder des Telefonservice der Bank sowie im Rahmen der Nutzung dieser Services unter Bezugnahme auf die jeweilige, dafür vorliegende Rechtsgrundlage angefertigte Audio- und Videoaufzeichnungen (z. B. im Rahmen der Teilnahmevereinbarung zu Mein ELBA).

#### **Daten aus Service, Webseite und Kommunikation**

Es werden Daten zur Nutzung von elektronischen Services und Internetseiten, verwendete Funktionen der Internetseiten, Apps und E-Mail-Nachrichten zwischen Ihnen und der Bank, Informationen über angesehene Internetseiten oder Inhalte und aufgerufene Links einschließlich externer Webseiten, Informationen zur Reaktionszeit auf Inhalte oder Downloadfehler und die Nutzungsdauer von Internetseiten und Informationen zur Nutzung und über Abonnements von Newslettern der Bank. Diese Informationen werden unter Verwendung automatisier-

ter Technologien, wie etwa Cookies oder Web-Beacons (Zählpixel, mit denen das Aufrufen von E-Mails oder Webseiten registriert wird) oder mittels „Webtracking“ (Aufzeichnung und Analyse des Surfverhaltens) auf der Webseite oder Mein ELBA und unter Einsatz externer Dienstleister oder Software erfasst.

#### **Online abgefragte Konten- und Depotdaten**

Daten zu online über Dienstleister abgefragte Informationen zu Konten und Depots, Daten dieser Dienstleister, Inhalt, Zweck und Häufigkeit der Abfragen und Inhalt der gegebenen Informationen.

#### **Technische Daten verwendeter Endgeräte**

Informationen über den Zugang zu Internetseiten oder Portalen und Apps oder sonstige Kommunikationsmöglichkeiten, benutzte Geräte und Systeme wie z. B. Internetprotokoll-Adressen oder Typen und Versionen der Betriebssysteme und Web-Browser sowie – zusätzlich – Geräte- und Werbe-Identifikationen oder Standortangaben und andere, vergleichbare Daten verwendeter Geräte und Systeme.

#### **Daten zu nutzergenerierten Inhalten**

Auf Internetseiten oder Apps der Bank hochgeladene Informationen, wie z. B. Kommentare, persönliche Einträge und Fotos oder Videos und Vergleichbares.

#### **Vermittelte Produkt- und Dienstleistungsdaten von (Sektor-)Unternehmen**

Daten der Ihnen von der Bank vermittelten Produkte und Dienstleistungen der mit der Bank verbundenen Unternehmungen: Raiffeisen Bausparkasse Gesellschaft mbH, Raiffeisen Bank International AG, UNIQA Österreich Versicherung AG, Raiffeisen Kapitalanlage GmbH, Raiffeisen Leasing GmbH, österreichische Raiffeisenbanken und Raiffeisenlandesbanken, Valida Holding AG, Raiffeisen Centrobank AG, Raiffeisen Factor Bank AG, Card Complete Service Bank AG, Raiffeisenversicherungsmakler Vorarlberg GmbH, Raiffeisen Immobilien GmbH, ländleticket marketing gmbh, TeamBank Österreich – Niederlassung der TeamBank AG in Nürnberg.

Diese Daten umfassen die persönlichen Daten und die Detaildaten der Produkte, wie Gegenstand der Geschäfte, Laufzeiten, Verzinsungen, Entgelte, Soll-, Haben- und Zahlungsrückstände. Sind die vermittelten Produkte Zahlungsinstrumente, werden auch folgende Daten in die Auswertung eingeschlossen:

Zahlungsverhalten, ein- und ausgehende Zahlungsverkehrstransaktionen, Empfänger und Absender, Zahlungsaufträge übermittelnde Dienstleister, Beträge, Verwendungszwecke, Zahlungsreferenzen, Auftraggeber-Referenzen, Häufigkeiten und Arten der Geldbewegungen, bei bargeldlosen Zahlungen die Daten der Händler oder Dienstleister und Informationen zu diesen abgeschlossenen Geschäften.

---

#### 4. An wen werden meine personenbezogenen Daten weitergegeben?

(Datenschutzinformation gem. Art. 13 und 14 DSGVO)

Innerhalb der Bank erhalten jene Stellen bzw. MitarbeiterInnen Zugriff auf Ihre Daten, die diese zur Erfüllung vertraglicher, gesetzlicher und/oder aufsichtsrechtlicher Pflichten sowie berechtigter Interessen benötigen.

Darüber hinaus erhalten von uns vertraglich gebundene Auftragsverarbeiter (insbesondere IT- und Backoffice-Dienstleister) Ihre Daten, sofern diese die Daten zur Erfüllung ihrer jeweiligen Leistung benötigen. Sämtliche Auftragsverarbeiter sind vertraglich verpflichtet, Ihre Daten vertraulich zu behandeln und nur im Rahmen der Leistungserbringung zu verarbeiten.

Weitere Datenempfänger können diejenigen Stellen sein, für welche Sie uns eine entsprechende Zustimmung erteilt haben (Einwilligung zur Datenverarbeitung, Befreiung vom Bankgeheimnis).

Bei Vorliegen einer gesetzlichen oder aufsichtsrechtlichen Verpflichtung können öffentliche Stellen und Institutionen (Europäische Bankenaufsichtsbehörde, Europäische Zentralbank, Österreichische Nationalbank, Österreichische Finanzmarktaufsicht, Finanzbehörden etc.) sowie unsere Bank- und Abschlussprüfer Empfänger Ihrer personenbezogenen Daten sein.

Empfänger personenbezogener Daten können andere Kredit- und Finanzinstitute oder vergleichbare Einrichtungen sein, sofern die Übermittlung zur Durchführung der Geschäftsbeziehung mit Ihnen erforderlich ist. Je nach Vertrag können diese Empfänger z. B. Korrespondenzbanken, Börsen, Depotbanken, Auskunftsteile oder andere, mit der Bank verbundene Unternehmen (aufgrund behördlicher oder gesetzlicher Verpflichtung) sein. Sofern Sie geförderte Bankprodukte in Anspruch nehmen, können auch die Förderstellen Empfänger Ihrer Daten sein (z. B. Landesregierung, Bundesministerium).

Im Rahmen der Angebots- bzw. Antragserstellung für Versicherungsprodukte, der Betreuung dieser Versicherungsprodukte und der Hilfestellung im Schadensfall werden die für die Bearbeitung erforderlichen Daten an die Raiffeisenversicherungsmakler Vorarlberg GmbH weitergegeben. Außerdem erfolgt eine Datenweitergabe an Versicherungsunternehmen, aus deren Produktportfolio ein Angebot oder Antrag für Sie erstellt wird, bzw. bei denen ein Versicherungsvertrag besteht, zu dem wir Ihnen im Schadensfall Hilfestellung bieten. Im Zusammenhang mit speziellen Versicherungsrahmenverträgen kann es auch erforderlich sein, Daten an andere Versicherungsmakler und Berater in Versicherungsangelegenheiten weiterzugeben.

Daten können im Einzelfall und bei Bedarf den zuständigen Behörden bzw. dem Gericht (zur Beweissicherung in Straf-

rechtssachen), Sicherheitsbehörden (zu sicherheitspolizeilichen Zwecken), Gerichten (zur Sicherung von Beweisen in Zivilrechtssachen), Mitarbeitern, Zeugen, Opfern (im Rahmen der Anspruchsdurchsetzung), Versicherungen (ausschließlich zur Abwicklung von Versicherungsfällen), Rechtsanwälten und sonstigen Stellen zum Zweck der Rechtsdurchsetzung übermittelt werden. Eine Übermittlung an Empfänger in einem Drittland (außerhalb der EU) oder an eine internationale Organisation ist grundsätzlich nicht vorgesehen.

Im Hinblick auf eine Datenweitergabe an sonstige Dritte möchten wir Sie darauf hinweisen, dass die Bank als österreichisches Kreditinstitut zur Einhaltung des Bankgeheimnisses gem. § 38 BWG und daher zur Verschwiegenheit über sämtliche kundenbezogenen Informationen und Tatsachen verpflichtet ist, die uns aufgrund der Geschäftsbeziehung anvertraut oder zugänglich gemacht wurden. Wir dürfen Ihre personenbezogenen Daten daher nur weitergeben, wenn Sie uns hierzu vorab schriftlich und ausdrücklich vom Bankgeheimnis entbunden und Sie in die Weitergabe der Daten eingewilligt haben oder wir gesetzlich bzw. aufsichtsrechtlich dazu verpflichtet oder wir beispielsweise aufgrund einer Interessenabwägung dazu befugt sind.

#### 5. Werden Daten in ein Drittland oder an eine internationale Organisation übermittelt?

(Datenschutzinformation gem. Art. 13 und 14 DSGVO)

Eine Datenübermittlung in Drittstaaten (Staaten außerhalb der Europäischen Union – EU bzw. des Europäischen Wirtschaftsraums – EWR) findet nur statt, soweit dies zur Ausführung Ihrer Aufträge (zB Zahlungs- und Wertpapieraufträge) erforderlich ist, gesetzlich vorgeschrieben ist, Sie uns Ihre Einwilligung erteilt haben oder einer der Ausnahmetatbestände der Art 44 ff DSGVO erfüllt ist. Darüber hinaus wird sichergestellt, dass im Einzelfall ein ausreichendes Schutzniveau gewährleistet ist, etwa durch weitere Sicherheitsmaßnahmen. Beispielsweise können Zahlungen und Bargeldbehebungen mit Debit- und Kreditkarten zur notwendigen Einbeziehung internationaler Kartenorganisationen und damit allenfalls zur Datenverarbeitung durch diese Kartenorganisationen in Drittstaaten führen. Über Einzelheiten werden wir Sie, sofern gesetzlich vorgegeben, gesondert informieren.

#### 6. Wie lange werden meine Daten gespeichert?

(Datenschutzinformation gem. Art. 13 und 14 DSGVO)

Wir verarbeiten Ihre personenbezogenen Daten, soweit dies für die Erfüllung vertraglicher und gesetzlicher Pflichten erforderlich ist, und bewahren diese für die Dauer gesetzlicher Aufbewahrungs- und Dokumentationspflichten, die sich u. a. aus dem Unternehmensgesetzbuch (UGB), der Bundesabgaben-

---

ordnung (BAO), dem Bankwesengesetz (BWG), dem Finanzmarkt-Geldwäschegesetz (FM-GwG), dem Wertpapieraufsichtsgesetz (WAG) und der Gewerbeordnung (GewO) ergeben, auf. Zudem sind bei der Speicherdauer die gesetzlichen Verjährungsfristen, die z. B. nach dem Allgemeinen Bürgerlichen Gesetzbuch (ABGB) in bestimmten Fällen bis zu 30 Jahre betragen können, zu berücksichtigen. Daten aus der Videoüberwachung der Bank werden spätestens nach 90 Tagen gelöscht, es sei denn, sie werden für die mit der Videoüberwachung verfolgten Zwecke benötigt.

#### 7. Welche Datenschutzrechte stehen mir zu?

(Datenschutzinformation gem. Art. 13 und 14 DSGVO)

Sie haben das Recht auf Auskunft, Berichtigung, Löschung oder Einschränkung der Verarbeitung Ihrer gespeicherten Daten, ein Widerspruchsrecht gegen die Verarbeitung sowie ein Recht auf Datenübertragbarkeit gem. den Voraussetzungen des Datenschutzrechts.

Darüber hinaus können Sie Beschwerde bei der zuständigen Datenschutzbehörde einlegen. Beschwerden können an die zuständige Datenschutzbehörde gerichtet werden: [www.dsb.gv.at](http://www.dsb.gv.at)

Sofern Sie eine Einwilligung zur Verarbeitung personenbezogener Daten erteilt haben, können Sie diese jederzeit der Bank gegenüber widerrufen. Dies gilt insbesondere für Einwilligungen, die vor Geltung der DSGVO erteilt wurden. Der Widerruf entfaltet Wirkung für die Zukunft. Datenverarbeitungen, die bis zum Widerruf erfolgt sind, sind davon nicht betroffen.

#### 8. Bin ich zur Bereitstellung von Daten verpflichtet?

Im Rahmen der Geschäftsbeziehung müssen Sie diejenigen personenbezogenen Daten bereitstellen, die für die Aufnahme und Durchführung der Geschäftsbeziehung erforderlich sind und zu deren Erhebung wir gesetzlich verpflichtet sind. Wenn Sie uns diese Daten nicht zur Verfügung stellen, werden wir den Abschluss des Vertrags oder die Ausführung des Auftrags in der Regel ablehnen oder einen bestehenden Vertrag nicht mehr durchführen können und somit beenden müssen. Dazu kann die Bank insbesondere aus geldwäscherechtlichen Vorgaben verpflichtet sein, wenn es der Bank nicht möglich sein sollte, die Person, mit der die Geschäftsbeziehung begründet werden sollte, nach gesetzlichen Vorgaben zu identifizieren. Sie sind jedoch nicht verpflichtet, hinsichtlich für die Vertragserfüllung nicht relevanter bzw. gesetzlich oder regulatorisch nicht erforderlicher Daten eine Einwilligung zur Datenverarbeitung zu erteilen.

#### 9. Inwieweit gibt es eine automatisierte Entscheidungsfindung?

(Datenschutzinformation gem. Art. 13 und 14 DSGVO)

Zur Begründung und Durchführung der Geschäftsbeziehung nutzen wir grundsätzlich keine vollautomatisierte Entscheidungsfindung nach Art. 22 DSGVO. Sollte der Abschluss eines Online-Produkts nicht möglich sein, wenden Sie sich bitte an Ihren Kundenberater.

#### 10. Profiling

Ihre Daten werden teilweise automatisiert verarbeitet. Dies hat zum Ziel, bestimmte persönliche Aspekte zu bewerten (Profiling). Aufgrund gesetzlicher und regulatorischer Vorgaben sind wir mitunter dazu verpflichtet.

- Das kann insbesondere bei der Bekämpfung von Geldwäsche, Terrorismusfinanzierung und vermögensgefährdenden Straftaten der Fall sein. Zu diesem Zweck nehmen wir Datenauswertungen – u. a. im Zahlungsverkehr – vor, nicht zuletzt deswegen, um auch Sie durch diese Maßnahmen zu schützen.
- Ebenso bedienen wir uns des Profillings mitunter bei der Kreditwürdigkeitsprüfung. Zur Beurteilung Ihrer Kreditwürdigkeit nutzen wir das Scoring. Dabei berechnen wir die Wahrscheinlichkeit, mit der Sie Ihren Zahlungsverpflichtungen vertragsgemäß nachkommen werden. In die Berechnung können beispielsweise Einkommensverhältnisse, Ausgaben, bestehende Verbindlichkeiten, Beruf, Arbeitgeber, Beschäftigungsdauer, Erfahrungen aus der bisherigen Geschäftsbeziehung, vertragsgemäße Rückzahlung früherer Kredite sowie Informationen von Kreditauskunfteien einfließen. Das Scoring beruht auf einem mathematisch-statistisch anerkannten und bewährten Verfahren. Die errechneten Werte unterstützen uns bei der Entscheidungsfindung im Rahmen von Produktabschlüssen und gehen in das laufende Risikomanagement mit ein.

#### Information über Ihr Widerspruchsrecht gemäß Artikel 21 DSGVO

##### 1. Einzelfallbezogenes Widerspruchsrecht

Aus Gründen, die sich aus Ihrer besonderen Situation ergeben, haben Sie das Recht, jederzeit gegen die Verarbeitung Sie betreffender personenbezogener Daten, die aufgrund von Artikel 6 Absatz 1 Buchstabe e DSGVO (Datenverarbeitung im öffentlichen Interesse) und Artikel 6 Absatz 1 Buchstabe f DSGVO (Datenverarbeitung auf der Grundlage einer Interessenabwägung) erfolgt, Widerspruch einzulegen. Das gilt ebenso für ein auf diese Bestimmung gestütztes Profiling im Sinne von Artikel 4 Nr. 4 DSGVO.

---

Legen Sie Widerspruch ein, werden wir Ihre personenbezogenen Daten nicht mehr verarbeiten, es sei denn, dem stehen nachweislich zwingende schutzwürdige Gründe entgegen, welche Ihren Interessen, Ihre Rechte und Freiheiten überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

## **2. Widerspruchsrecht gegen eine Verarbeitung von Daten für Zwecke der Direktwerbung**

In Einzelfällen verarbeiten wir – vorbehaltlich einer vorliegenden Einwilligung – Ihre personenbezogenen Daten, um Direktwerbung zu ermöglichen. Sie haben das Recht, jederzeit Widerspruch gegen die Verarbeitung personenbezogener Daten, die Sie betreffen, einzulegen. Das gilt ebenso für das Profiling, soweit es mit solcher Direktwerbung in Verbindung steht. Widersprechen Sie der Verarbeitung für Zwecke der Direktwerbung, so verarbeiten wir Ihre personenbezogenen Daten nicht mehr für diese Zwecke.

Der Widerspruch kann formfrei erfolgen und sollte möglichst gerichtet werden an:

Alpen Privatbank AG  
Walsersstraße 61  
6991 Riezlern, Österreich  
T +43 (5517) 350-0  
info@alpenprivatbank.com