Informationen zur Datenverarbeitung

Fassung April 2020

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

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

Für die Datenverarbeitung verantwortlich:

Raiffeisenkasse Haidershofen eGenmbH (nachfolgend „Bank")
4431 Haidershofen, Haidershofen 100, FN 77703w LG St. Pölten, BLZ 32278
Telefon +43 7252 37827-0
E-Mail info.32278@32278.at

Der Datenschutzbeauftragte der Bank:

datenschutz.32278@32278.at
Telefon +43 7252 37827-0
4431 Haidershofen, Haidershofen 100

Welche Daten werden verarbeitet und aus welchen Quellen stammen diese?

Wir verarbeiten jene personenbezogenen Daten, die wir von Ihnen, insbesondere im Rahmen unserer Geschäftsbeziehung, erhalten. Zudem verarbeiten wir Daten, die wir von Auskunfteien (CRIF GmbH), Schuldnerverzeichnissen (Kreditschutzverband von 1870) und aus öffentlich zugänglichen Quellen (z.B. Firmenbuch, Vereinsregister, Grundbuch oder Medien) zulässigerweise erhalten haben oder die uns von anderen, mit der Bank verbundenen Unternehmen berechtigterweise übermittelt werden.

Zu den personenbezogenen Daten zählen Ihre persönlichen Detailangaben und Kontaktdaten (z. B. Name, Adresse, Geburtsdatum und -ort, Staatsangehörigkeit etc.) oder Daten zu Identitäts- und Reisedokumenten (z. B. Unterschriftsprobe, Ausweisdaten). 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), Daten zu Marketing und Vertrieb, zu Kreditgeschäften, Bild- und/oder Tonaufzeichnungen (z. B. Video-, Telefonaufzeichnungen), elektronische Protokoll- und Identifikationsdaten (Apps, Cookies etc.), Finanzidentifikationsdaten (Daten von Kredit-, Debit-, Prepaidkarten) oder AML(Anti Money Laundering)- und Compliance-Daten fallen, sowie andere, mit den genannten Kategorien vergleichbare Daten.

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

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 personenbezogener Daten (Art. 4 Nr. 2 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, Bausparen, Wertpapiere, Einlagen, Vermittlung) und können u. a. Bedarfsanalysen, Beratung, Vermögensverwaltung und -betreuung sowie die Durchführung von Transaktionen umfassen.

  Derartige Datenverarbeitungen erfolgen zum Beispiel im Zusammenhang mit Debitkarten (auch „Bankomatkarten"), die die Bank Ihnen zur Verfügung stellt und mit denen es Ihnen insbesondere möglich ist, Zahlungstransaktionen bei Händlern an POS-Terminals („Bankomat-Kassen") und im Internet (E-Commerce-Zahlungen im Online-Shop) durchzuführen, Bargeld an dafür vorgesehenen Geldausgabeautomaten (auch „Bankomat") zu beheben und Transaktionen zwischen Debitkarten („ZOIN") durchzuführen. Diese Transaktionen müssen den Kreditinstituten des Karteninhabers und des Zahlungsempfängers zugeordnet werden können, damit diese untereinander die Transaktionen abrechnen können. Nahezu alle in Österreich tätigen Institute haben zu diesem Zweck gemeinsam mit der PSA Payment Services Austria GmbH (PSA) einen Vertrag abgeschlossen (PSA-Vertrag). Ziel dieses Vertrages 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 Ab-wicklung 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 zwischen dem Institut und dessen Kunden (z. B. Girokontovertrag, Kartenvertrag). 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 hier angesprochenen Datenverarbeitungen können Sie den jeweiligen Vertragsunterlagen und Geschäftsbedingungen entnehmen.

- **Zur Erfüllung rechtlicher Verpflichtungen (Art. 6 Abs. 1c DSGVO)**

  Eine Verarbeitung personenbezogener Daten kann zum Zweck der Erfüllung unterschiedlicher gesetzlicher Verpflichtungen (etwa aus dem Bankwesen- oder Finanzmarkt-Geldwäschegesetz, dem Wertpapieraufsichts- oder Börsegesetz) 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 gemäß 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 iSd 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 Finanzinstitute, die steuerliche(n) Ansässigkeit(en) ihrer Kunden festzustellen und dabei die Daten ihrer Kunden (natürliche Personen und Rechtsträger) zu prüfen und 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 passiven Rechtsträgern umfasst eine Meldung zusätzlich die melderelevanten Daten der melderelevanten wirtschaftlichen Eigentümer.
  - Datenverarbeitung aufgrund des Foreign Account Tax Compliance Act (FATCA)
    FATCA verpflichtet Finanzinstitute, die U.S.-Eigenschaft gem. FATCA ihrer Kunden festzustellen und dabei die Daten ihrer Kunden (natürliche Personen oder Rechtsträger) zu prüfen und steuerliche Selbstauskünfte ihrer Kunden einzuholen. Bei passiven Rechtsträgern umfass die Meldung zusätzlich die melderelevanten wirtschaftlichen Eigentümer mit U.S.-Eigenschaft. Bei Feststellung einer U.S.-Eigenschaft gem. FATCA ist eine Meldung personen- und kontobezogener Daten an die amerikanische Finanzbehörde durchzuführen.
  - 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 Risiken
  - 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 ermögli-chen, 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, kommt es zu einer Ablehnung des Kreditantrags.

- **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.

  Beispiele für solche Fälle sind

  - die Auswertung Ihrer Daten (wie zum Beispiel Name, Alter, Kontoumsatzdaten und dergleichen) und die Abfrage externer Bonitätsdatenbanken (Kreditschutzverband von 1870, CRIF GmbH), um für Kreditangebote, die Ihnen die Bank aus eigener Initiative 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 (Art. 6 Abs. 1f DSGVO) allgemein**

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

  Beispiele für solche Fälle sind:

- Konsultation von und Datenaustausch mit Auskunfteien (z. B. Österreichischer Kreditschutzverband 1870) zur Ermittlung von Bonitäts- bzw. Ausfallrisiken.
- Prüfung und Optimierung von Verfahren zur Bedarfsanalyse und direkten Kundenansprache.
- Videoüberwachungen zum Zweck des Eigenschutzes (Schutz des Eigentums und Schutz der Arbeitnehmer des Verantwortlichen), des Verantwortungsschutzes (Wahrnehmung von Verkehrssicherungspflichten, Vertragshaftung gegenüber Kunden etc.), zum Nachweis von Verfügungen und Einzahlungen (z. B. an Geldautomaten) sowie zum Zweck der Verhinderung, Eindämmung und Aufklärung strafrechtlich relevanten Verhaltens.

  Überwacht werden öffentlich zugängliche (Bank-)Räumlichkeiten (insbesondere Kassenräume, Saferäume, Foyers, Gänge, Stiegen, Aufzugsbereiche, Eingangsbereiche innen/außen, Fassaden, Garagen) sowie der vom Verantwortlichen betriebenen Geldausgabeautomaten (auch im Außenbereich der Bankgebäude).
- Bestimmte Telefonaufzeichnungen (für Qualitätssicherungsmaßnahmen oder bei Beschwerdefällen).
- Maßnahmen zur Geschäftssteuerung und Weiterentwicklung von Dienstleistungen und Produkten.
- Maßnahmen zum Schutz von Kunden und Mitarbeitern sowie des Eigentums der Bank.
- Maßnahmen zur 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.
- Datenverarbeitung für Zwecke der Rechtsverfolgung.
- Geltendmachung rechtlicher Ansprüche und Verteidigung bei rechtlichen Streitigkeiten.
- Gewährleistung der IT-Sicherheit und des IT-Betriebs der Bank.
- Verhinderung und Aufklärung von Straftaten.

- **zur Wahrung unseres berechtigten Interesses (Art. 6 Abs. 1f DSGVO) am Marketing unserer Dienstleistungen**

  Die Auswertung Ihrer bei der Bank verarbeiteten Daten zum Zweck:

  - Ihnen individuelle Informationen und Angebote der Bank und der unten genannten Unternehmen, deren Produkte und Dienstleistungen, welche die Bank vermittelt, bereitzustellen oder zu übermitteln,
  - Dienstleistungen und Produkte zu entwickeln, die auf Ihre Interessen und Lebenssituation abgestimmt sind, sowie
  - die Benutzerfreundlichkeit Ihrer Serviceeinrichtungen wie Mein ELBA, Apps, Selbstbedienungsgeräte und anderer weiter zu verbessern.

  beruht auf unserem berechtigten Interesse am Marketing unserer Dienstleistungen. Die Auswertung der Daten für diesen Zweck erfolgt nur solange, als Sie ihr nicht widersprochen haben.

  Folgende Daten, die die Bank selbst erhoben hat oder die Sie an die Bank übertragen haben lassen, werden dafür ausgewertet:

  - 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 gemäß 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 zum Beispiel Hobbys und Interessen oder geplante Anschaffungen und Auto, Haushaltsrechnungen, interne Ratingeinstufungen wie die Bewertung der Einnahmen- und Ausgabensituation und der Vermögens- und Verbindlichkeitensituation 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- und Zahlungsrückstände zu Konten und Krediten,
    - im Rahmen dieser Dienstleistungen verrechnete Zinssätze und Entgelte oder Spesen,
    - Zahlungsverhalten einschließlich von Ihnen genutzter Möglichkeiten der Auftragserteilung (zum Beispiel Mein ELBA),
    - ein- und ausgehende Zahlungsverkehrstransaktionen, Empfänger und Absender und Zahlungsaufträge übermittelnde Dienstleister, Betrag, Verwendungszwecke und Zahlungsreferenzen, Auftraggeber-Referenzen,
    - Häufigkeit und Art der Geldbewegungen, bei bargeldlosen Zahlungen die Daten der Zahlungen erhaltenden Händler oder Dienstleister und Informationen zu bei 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 (Telefonservice inkl. Sprachsteuerungscomputer) oder Telefonservices der Bank, sowie im Rahmen der Nutzung dieser Services unter Bezugnahme auf die jeweilige dafür vorliegende Rechtsgrundlage angefertigte Audio- und Videoaufzeichnungen (zum Beispiel im Rahmen der Teilnahmevereinbarung zu Mein ELBA).

- Daten aus Services, Website und Kommunikation
  Daten zur Nutzung von elektronischen Services und Internetseiten, verwendete Funktionen der Internetseiten und der Apps und E Mail Nachrichten zwischen mir und der Bank, Informationen über angesehene Internetseiten oder Inhalte und aufgerufene Links einschließlich externer Websites, Informationen zur Reaktionszeit auf Inhalte oder über Download-Fehler und die Nutzungsdauer von Internetseiten und Informationen zur Nutzung und über Abonnements von Newslettern der Bank. Diese Informationen werden unter Verwendung automatisierter Technologien wie etwa Cookies oder Web-Beacons (Zählpixel mit denen das Aufrufen von E-Mails oder Websites registriert wird), oder mittels Webtracking (Aufzeichnung und Analyse des Surfverhaltens) auf der Website oder in Mein ELBA und unter Einsatz externer Dienstleister oder Software (zum Beispiel Google Analytics) erfasst.

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

- Technische Daten verwendeter Endgeräte
  Informationen über für den Zugang zu Internetseiten oder Portalen und Apps oder sonstige Kommunikationsmöglichkeiten benutzter Geräte und Systeme wie zum Beispiel Internetprotokoll-Adressen oder Typen und Versionen der Betriebssysteme und Web-Browser und zusätzlich Geräte-Identifikationen 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 zum Beispiel Kommentare oder persönliche Einträge und Fotos oder Videos und Vergleichbares.

- Produkt- und Dienstleistungsdaten vermittelter Unternehmen
  Daten der Ihnen von der Bank vermittelten Produkte und Dienstleistungen der mit der Bank verbundenen Unternehmungen: Raiffeisen Bausparkasse Gesellschaft m.b.H., UNIQA Österreich Versicherung AG, Raiffeisen Kapitalanlage-Gesellschaft m.b.H., Raiffeisen-Leasing GmbH, Raiffeisen Reisebüro Ges.m.b.H, Raiffeisen Bank International AG, Valida Holding AG, Raiffeisen Immobilien Vermittlung Ges.m.b.H., Raiffeisen Centrobank AG, Raiffeisen Vorsorge Wohnung GmbH, Raiffeisen Factor Bank AG, Card Complete Service Bank AG, Raiffeisen Analytik Ges.m.b.H., Raiffeisen Beratung Direkt Ges.m.b.H., Raiffeisen Club und Zentrale Raiffeisenwerbung.

  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, schließen die ausgewerteten Daten auch mit ein: 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.

An wen werden meine personenbezogenen Daten weitergegeben?

Innerhalb der Bank erhalten jene Stellen bzw. Mitarbeiter 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 dazu verpflichtet, Ihre Daten vertraulich zu behandeln und nur im Rahmen der Leistungserbringung zu verarbeiten.

Bei Vorliegen einer gesetzlichen oder aufsichtsrechtlichen Verpflichtung können öffentliche Stellen und Institutionen (Europäische Bankenaufsichtsbehörde, Europäische Zentralbank, Oesterreichische Nationalbank, Österreichische Finanzmarktaufsicht, Finanzbehörden etc.) sowie unsere Bank- und Abschlussprüfer Empfänger Ihrer personenbezogenen Daten sein. In Hinblick auf eine Datenweitergabe an sonstige Dritte möchten wir darauf hinweisen, dass die Bank als österreichisches Kreditinstitut zur Einhaltung des Bankgeheimnisses gemäß § 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 haben oder wir gesetzlich bzw. aufsichtsrechtlich dazu verpflichtet oder ermächtigt sind. Empfänger personenbezogener Daten können in diesem Zusammenhang andere Kredit- und Finanzinstitute oder vergleichbare Einrichtungen sein. Wir übermitteln Daten, die wir zur Durchführung der Geschäftsbeziehung mit Ihnen benötigen. Je nach Vertrag können diese Empfänger z. B. Korrespondenzbanken, Börsen, Depotbanken, Auskunfteien 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.

Daten aus der Videoüberwachung der Bank können im Einzelfall und bei Bedarf zuständigen Behörden bzw. dem Gericht (zur Beweissicherung in Strafrechtssachen), 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.

Werden Daten in ein Drittland oder eine internationale Organisation übermittelt?

Eine Datenübermittlung in Drittstaaten (Staaten außerhalb des Europäischen Wirtschaftsraums – EWR) findet nur statt, soweit dies zur Ausführung Ihrer Aufträge (zum Beispiel Zahlungs- und Wertpapieraufträge) erforderlich, gesetzlich vorgeschrieben ist oder Sie uns Ihre Einwilligung erteilt haben. Zahlungen und Bargeldbehebungen mit Debit- und Kreditkarten können zur notwendigen Einbeziehung internationaler Kartenorganisationen und damit allenfalls zur Datenverarbeitung durch diese Kartenorganisationen in Drittstaaten führen. Beispielsweise sind unter www.mastercard.us/content/dam/mccom/global/documents/mastercard-bcrs.pdf die von Mastercard dazu getroffenen Datenschutzmaßnahmen („Binding Corporate Rules“) abrufbar.

Über Einzelheiten werden wir Sie, sofern gesetzlich vorgegeben, gesondert informieren.

Wie lange werden meine Daten gespeichert?

Wir verarbeiten Ihre personenbezogenen Daten, soweit erforderlich, für die Dauer der gesamten Geschäftsbeziehung (von der Anbahnung, Abwicklung bis zur Beendigung eines Vertrags) sowie darüber hinaus gemäß den gesetzlichen Aufbewahrungs- und Dokumentationspflichten, die sich u. a. aus dem Unternehmensgesetzbuch (UGB), der Bundesabgabenordnung (BAO), dem Bankwesengesetz (BWG), dem Finanzmarkt-Geldwäschegesetz (FM-GwG) und dem Wertpapieraufsichtsgesetz (WAG) ergeben. Zudem sind bei der Speicherdauer die gesetzlichen Verjährungsfristen, die z.B. nach dem Allgemeinen Bürgerlichen Gesetzbuch (ABGB) in bestimmten Fällen bis zu 30 Jahre (die in der Praxis relevanteste Verjährungsfrist beträgt drei Jahre) betragen können, zu berücksichtigen. Daten aus der Videoüberwachung der Bank werden spätestens nach 90 Tagen gelöscht, wenn sie für die mit der Videoüberwachung verfolgten Zwecke nicht mehr benötigt werden.

Welche Datenschutzrechte stehen mir zu?

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 gemäß den Voraussetzungen des Datenschutzrechts. Beschwerden können an die zuständige Datenschutzbehörde gerichtet werden (www.dsb.gv.at).

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. Sie sind jedoch nicht verpflichtet, hinsichtlich für die Vertragserfüllung nicht relevanter bzw. gesetzlich oder regulatorisch nicht erforderlicher Daten eine Einwilligung zur Datenverarbeitung zu erteilen.

Inwieweit gibt es eine automatisierte Entscheidungsfindung?

Zur Begründung und Durchführung der Geschäftsbeziehung nutzen wir grundsätzlich keine vollautomatisierte Entscheidungsfindung nach Artikel 22 DSGVO. Im Zusammenhang mit online abzuschließenden Produkten kann es zu einer automatisierten Ablehnung des Online-Abschlusses kommen, wenn Ihre Angaben den für das Produkt definierten Anforderungen nicht entsprechen. In diesen Fällen wenden Sie sich bitte an einen Kundenbetreuer. Sollten wir diese Verfahren in anderen Einzelfällen einsetzen, werden wir Sie hierüber gesondert informieren, sofern dies gesetzlich vorgesehen ist.