



Datenschutzinformationen - Oberbank Apps

Mit den folgenden Informationen möchten wir Ihnen einen Überblick über die Verarbeitung Ihrer personenbezogenen Daten durch uns bei Verwendung der Oberbank Apps (Banking App, Business App und Security App) und Ihre Rechte aus dem Datenschutzrecht geben. Allgemeine Informationen zum Datenschutz in der Oberbank finden Sie [hier](#).

1. Wer ist für die Datenverarbeitung verantwortlich und an wen kann ich mich wenden?

Verantwortliche Stelle ist:

Unseren Datenschutzbeauftragten erreichen Sie unter:

Oberbank AG

Untere Donaulände 28, A-4020 Linz

Telefon: +43 (0732) 7802-0

E-Mail: datenschutz@oberbank.at

3 Banken IT GmbH

Datenschutzbeauftragte:r

Untere Donaulände 28, 4020Linz

Telefon: +43 (0732) 7802-0

E-Mail: datenschutz@oberbank.at

2. Welche Daten verarbeiten wir und welche Quellen nutzen wir?

Wir verarbeiten jene personenbezogenen Daten, die wir bei der Verwendung der Oberbank Apps bzw. der Services von Ihnen erhalten und relevant sind. Relevante personenbezogenen Daten sind dabei z.B. Ihre Personalien, Authentifikationsdaten, Legitimationsdaten etc.

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

Wir verarbeiten personenbezogene Daten im Einklang mit den Bestimmungen der europäischen Datenschutz-Grundverordnung (DSGVO) und dem Datenschutzgesetz.

3.1. Zur Erfüllung vertraglicher Pflichten (Art. 6 Abs. 1 lit. b DSGVO)

3.1.1. Banking App

Sofern Sie über ein Oberbank Kundenportal (Internetbanking) verfügen und die Banking App auf Ihr Smartphone mit Betriebssystem IOS oder Android herunterladen, verarbeiten wir Ihre Daten im Rahmen der von Ihnen in Auftrag gegebenen Services.

Folgende Services bieten wir Ihnen an:

- Finanzübersicht über alle Ihre Konten, privaten Kreditkarten und Depots bei der Oberbank
- SEPA-Überweisungen innerhalb Europas (ausschließlich mit dem sicheren Verfahren der Security App)
- Mit dem QR-Code Reader bzw. IBAN-Scanner zahlungsrelevante Empfängerdaten automatisch von einer Zahlungsanweisung oder Rechnung übernehmen
- GeoControl: Freischalten der Debitkarte für Bargeldbehebungen außerhalb Europas



- e) Kartenverwaltung: Anpassen des Limits der Debitkarte „Gold“; Nachbestellung Debitkarte / PIN; Debitkarte / Kreditkarte sperren
- f) Elektronisches Postfach
- g) Kontaktdaten bearbeiten
- h) Finanzmanager: Nach Kundenaktivierung des Finanzmanagers bietet dieser eine Kategorisierung der Zahlungsverkehrsumsätze nach verschiedenen Ausgabenkategorien.

Im Rahmen der oben genannten Zwecke verarbeiten wir Ihre Daten wie Personenstammdaten, Adressdaten, Kontaktdaten, Nutzungsdaten, Identifikationsdaten, Umsatzdaten, etc.

3.1.2. Business App

Sofern Sie als Firmenkund:in über eine aktive Kommunikationsberechtigung für ELBA (MBS) oder MultiCash (EBICS) oder Fremdsoftware (die den EBICS-Standard unterstützt) verfügen und die Business App auf Ihr Smartphone / Tablet mit Betriebssystem IOS oder Android herunterladen, verarbeiten wir Ihre Daten im Rahmen der von Ihnen in Auftrag gegebenen Services.

Folgende Services bieten wir Ihnen an:

- a) Saldenübersicht über alle in der App integrierten Banken mit den jeweils zugehörigen Konten
- b) Kontoauszug einsehen, als PDF-Dokument per Mail senden, speichern oder drucken
- c) Umsatzübersicht über tagesaktuelle Umsätze oder Umsätze der letzten 365 Tage
- d) Umsatzsuche
- e) Signatur/Autorisierung von zuvor im ELBA, MultiCash etc. erfassten Aufträgen

Im Rahmen der oben genannten Zwecke verarbeiten wir Ihre Daten wie Stammdaten, Kontaktdaten, Nutzungsdaten, Finanzdaten (Zahlungsinformationen des Nutzers) und Geräte-IDs.

3.1.3. Security App

Sofern Sie über das Oberbank Kundenportal (Internetbanking) oder die Banking App verfügen, können Sie die Security App herunterladen und verwenden. Dabei verarbeiten wir Ihre Daten im Rahmen der von Ihnen in Auftrag gegebenen Services. Die Oberbank Security App benötigt bei der Aktivierung Informationen aus dem Telefonstatus, um sich mit der/dem Oberbank Internetbanking Verfüg:erin verbinden zu können.

Bei den folgenden Services welche im Kundenportal, in der Banking App oder im eShop angeboten werden, ist die Kundenauthentifizierung mittels Security App erforderlich:

- a) Änderung von persönlichen Daten
- b) Erfassung eKYC
- c) Limitänderungen
- d) Einbindung von Fremdkonten
- e) Einrichtung Wallet
- f) Vertragsabschlüsse im eShop
- g) Aktivierung von mobile payments
- h) Aktivierung von Services und Funktionen

Im Rahmen des oben genannten Zwecks verarbeiten wir Ihre Umsatzdaten, Identifikationsdaten und Geräteinformationen.



3.2. Zur Erfüllung gesetzlicher Vorgaben (Art. 6 Abs. 1 lit. c DSGVO)

Die Verarbeitung personenbezogener Daten kann aufgrund diverser gesetzlicher oder aufsichtsrechtlicher Vorgaben, denen wir als Bank unterliegen, erforderlich sein. Details dazu entnehmen Sie unserer [allgemeinen Datenschutzhinweise](#).

3.2.1. Security App

§ 87 Abs. 1 ZaDiG schreibt vor, dass bei den folgenden Services, welche im Kundenportal oder in der Banking App zur Verfügung stehen, eine starke Kundenauthentifizierung zu verlangen ist, welche mittels Security App erfolgt:

- a) (Tourliche) Freigabe bei Zugriff auf das Zahlungskonto
- b) Freigabe von Transaktionen
- c) Freigabe bei Ansicht älterer Kontoumsätze

Im Rahmen der oben genannten Zwecke verarbeiten wir Ihre Daten wie Transaktionsdaten, Identifikationsdaten und Geräteinformationen.

3.3. Aufgrund Ihrer Einwilligung (Art. 6 Abs. 1 lit. a DSGVO)

Soweit Sie uns eine Einwilligung zur Verarbeitung Ihrer personenbezogenen Daten für bestimmte Zwecke erteilt haben, ist die Rechtmäßigkeit dieser Verarbeitung auf Basis Ihrer Einwilligung gegeben. Umfang und Inhalt dieser Datenverarbeitung ergibt sich immer aus der jeweiligen Einwilligung. Ihre freiwillige und jederzeit mit Wirkung für die Zukunft widerrufbare Einwilligung benötigen wir vor allem für die folgenden Zwecke:

3.3.1. Banking App

a) **Filialfinder:** Der Filialfinder (API/Programmierschnittstelle) ermöglicht die Filialsuche in einer Kartenansicht oder alternativ auch nach Adressen. Um die nächstgelegene Filiale am schnellsten zu finden, ist die Standortfreigabe des Smartphones erforderlich. Dafür verwenden wir den von Google LLC (USA) betriebenen Dienst Google Maps. Durch die Nutzung des Filialfinder erklären Sie sich mit der Erfassung, Bearbeitung sowie der Nutzung der automatisch erhobenen sowie der von Ihnen eingegebenen Daten durch Google LLC einverstanden. Weitere Informationen darüber, wie Google LLC Ihre Daten verarbeitet finden Sie unter: www.google.at/intl/de/policies/privacy.

Wenn Sie dieses API nicht aktivieren, kann keine Kartenansicht in Anspruch genommen werden. Die Filialsuche erfolgt sodann nach Adressen.

b) **Feedback Button:** Der Medallia Feedback Button ist ein interaktives Online-Tool, mit dem Sie die einfache Möglichkeit haben, Feedback zu geben und Ihre Meinung und Kommentare schnell und einfach mit uns zu teilen. Um den Medallia Feedback Button nutzen zu können, müssen die entsprechenden SDKs in der App aktiviert sein. Der Feedback Button erfasst die IP-Adresse des Benutzers, um die Verbindung herzustellen, diese wird jedoch sofort verworfen und nicht dauerhaft gespeichert.

Sie können beim Erfassen des Feedbacks auswählen, ob zudem ein Kontaktwunsch Ihrerseits besteht. Wenn kein Kontaktwunsch besteht, werden die gesammelten Feedbacks in anonymer Form gespeichert, so dass die Privatsphäre der Benutzer geschützt bleibt. Geben Sie an, dass Sie kontaktiert werden möchten, dann ist die Eingabe personenbezogener Daten (Name, Telefonnummer oder E-Mail-Adresse) nötig. Diese personenbezogenen Daten werden nach 3 Jahren anonymisiert. Falls Sie bei Ihrem Feedback im Kommentar personenbezogene Daten angeben, werden diese ebenso gespeichert. An der Erhebung und Speicherung der Feedbacks haben wir ein berechtigtes Interesse (Art. 6 Abs. 1 lit. f DSGVO), da uns dies ermöglicht die



Kundenzufriedenheit zu verbessern und die Produkte und Dienstleistungen besser auf die Bedürfnisse der Kund:innen abzustimmen.

- c) **Chatbot Mia:** Mia ist eine interaktive Online-Assistentin, die in der App für Sie erreichbar ist. Der Chatbot beantwortet viele Fragen und ist rund um die Uhr erreichbar. Wenn Mia keine Antwort auf Ihre Frage hat, werden Sie automatisch zu unserem Kundenservicecenter weitergeleitet. Um den Chatbot nutzen zu können, müssen die entsprechenden SDKs in der App aktiv ausgewählt werden.

Bei der Nutzung des Chatbot wird Ihre IP-Adresse erhoben, um die Verbindung herzustellen. Die IP-Adresse wird sofort verworfen und nicht permanent gespeichert. Die Chats mit MIA werden in anonymer Form gespeichert. Die Eingabe von personenbezogenen Daten ist für die Nutzung von MIA nicht erforderlich. Falls Sie bei Ihrer Interaktion dennoch personenbezogene Daten angeben, werden diese ebenso gespeichert. An der Erhebung und Speicherung Ihrer Daten haben wir ein berechtigtes Interesse (Art. 6 Abs. 1 lit. f DSGVO), da diese für die bedarfsgerechte Gestaltung unseres Chatbots, zur Gewährleistung eines störungsfreien Dienstes und zur Beantwortung Ihres Anliegens erforderlich sind. Nach 6 Wochen werden Ihre Daten automatisch gelöscht.

3.4. Im Rahmen der Interessenabwägung (Art. 6 Abs. 1 lit. f DSGVO)

Soweit erforderlich, werden wir Ihre Daten über die eigentliche Erfüllung des Vertrages hinaus zur Wahrung berechtigter Interessen der Oberbank AG oder Dritter verarbeiten. Beispiele dafür sind:

- Maßnahmen zur Weiterentwicklung von Dienstleistungen und Produkten
- Maßnahmen zum Prozess- und Qualitätsmanagement
- Gewährleistung der IT-Sicherheit / Systemsicherheit
- Anfrage-/Beschwerdemanagement auch im Hinblick auf die Abgabe von Bewertungen

Im Rahmen der oben genannten Zwecke verarbeiten wir Ihre Daten, wie etwa das Datum, den Typ des benutzten Endgeräts, Typ und Version des genutzten Betriebssystems und den Typ, die Version des genutzten Browsers, Personenstammdaten, Geburtsdatum, Adressdaten und Kontaktdaten.

Widerspruchsrecht nach Art 21 DSGVO

Sie haben das Recht, aus Gründen, die sich aus Ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung Sie betreffender personenbezogener Daten, die aufgrund von Art. 6 Abs. 1 lit. f DSGVO (Datenverarbeitung auf der Grundlage einer Interessensabwägung) erfolgt, Widerspruch einzulegen. Legen Sie Widerspruch ein, werden wir Ihre personenbezogenen Daten nicht mehr verarbeiten; es sei denn, wir können zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die Ihre Interessen, Rechte und Freiheiten überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

4. Wer erhält meine Daten?

Innerhalb der Oberbank AG erhalten diejenigen Stellen und Mitarbeiter:innen Zugriff auf Ihre Daten, die diese zur Erfüllung der vertraglichen, gesetzlichen und aufsichtsrechtlichen Pflichten oder aufgrund berechtigter Interessen benötigen. Zudem erhalten von uns beauftragte Dienstleister (Auftragsverarbeiter nach Art. 28 DSGVO) Ihre Daten, sofern diese zur Erfüllung der jeweiligen Dienstleistung benötigt werden. Das sind z.B. Unternehmen in den Kategorien IT-Dienstleistungen, Telekommunikation und Marketing sowie Datenspeicherung in sicheren Rechenzentren.



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

Eine Datenübermittlung an Stellen in Staaten außerhalb der Europäischen Union (sogenannte Drittstaaten) findet statt, soweit dies zur Ausführung Ihrer Aufträge (z. B. Zahlungs- und Wertpapieraufträge) erforderlich ist, gesetzlich vorgeschrieben ist, Sie uns Ihre ausdrückliche Einwilligung erteilt haben oder einer der Ausnahmetatbestände der Art. 44 ff DSGVO erfüllt ist. Über Einzelheiten werden wir Sie, sofern gesetzlich vorgegeben, gesondert informieren.

6. Wie lange werden meine Daten gespeichert?

Wir verarbeiten und speichern Ihre personenbezogenen Daten, solange es für die Erfüllung unserer vertraglichen und gesetzlichen Pflichten erforderlich ist. Sind Ihre personenbezogenen Daten nicht mehr erforderlich, werden diese regelmäßig gelöscht, es sei denn deren befristete Weiterverarbeitung ist zur Erfüllung handels- und steuerrechtlicher Aufbewahrungsfristen erforderlich. Die vorgegebenen Fristen zur Aufbewahrung bzw. Dokumentation betragen fünf bis zehn Jahre ab Ende der Geschäftsbeziehung. Die Aufbewahrung kann demnach auch erforderlich sein, wenn Sie nicht mehr unser/unsere Kund:in sind.

Zudem sind bei der Speicherdauer die gesetzlichen Verjährungsfristen zum Zwecke der Erhaltung von Beweismitteln für die Ausübung, Verteidigung oder Geltendmachung von Rechtsansprüchen maßgeblich, die z. B. nach dem Allgemeinen Bürgerlichen Gesetzbuch (ABGB) in der Regel drei Jahre, in gewissen Fällen aber auch bis zu 30 Jahre betragen können.

7. Inwieweit gibt es eine automatisierte Entscheidungsfindung im Einzelfall?

Im Rahmen der Banking App findet keine automatisierte Entscheidungsfindung einschließlich Profiling gemäß Art. 22 DSGVO statt. Sofern Profiling zu anderen Zwecken betrieben werden soll, benötigen wir hierfür eine gesonderte und ausdrückliche (jederzeit widerrufbare) Zustimmung. Ohne Ihre vorherige ausdrückliche Einwilligung werden Ihre personenbezogenen Daten nicht für andere Zwecke verwendet.

8. Datensicherheit

Wir bemühen uns um einen möglichst hohen Schutz und Sicherheit im digitalen Datenverkehr sowie darum, alle erforderlichen technischen und organisatorischen Maßnahmen zu treffen, um die Sicherheit der Datenverarbeitung zu gewährleisten. Dies vor allem zum Schutz Ihrer bei uns einlangenden sowie sich bereits bei uns befindlichen elektronischen Nachrichten samt Daten und Informationen. Ziel ist es, eine zeitgemäße, sorgfältige und auf einem hohen technischen Schutzniveau basierende Handhabung des digitalen Datenverkehrs gewährleisten zu können.

9. Welche Datenschutzrechte habe ich?

Jede betroffene Person hat das Recht auf Auskunft (Art. 15 DSGVO), Berichtigung (Art. 16 DSGVO), Löschung (Art. 17 DSGVO), Einschränkung der Verarbeitung (Art. 18 DSGVO), Datenübertragbarkeit (Art. 20 DSGVO), das Recht auf Widerspruch gegen die Datenverarbeitung (Art. 21 DSGVO) sowie das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden (Art. 22 DSGVO).



Wenn Sie ein Betroffenenrecht an uns richten, verlangen wir in Zweifelsfällen einen Identitätsnachweis von Ihnen. Auf diese Weise können wir sicherstellen, dass Ihre Daten nicht an unberechtigte Dritte weitergegeben werden und dient daher zu Ihrem Schutz.

Eine erteilte Einwilligung in die Verarbeitung personenbezogener Daten können Sie uns gegenüber jederzeit widerrufen. Dies gilt auch für Einwilligungserklärungen, die Sie uns vor der Geltung der Datenschutz-Grundverordnung erteilt haben. Bitte beachten Sie, dass der Widerruf erst für die Zukunft wirkt. Verarbeitungen, die vor Ihrem Widerruf erfolgt sind, sind davon nicht betroffen.

Wenn Sie der Meinung sind, dass die Verarbeitung Ihrer personenbezogenen Daten nicht den datenschutzrechtlichen Vorgaben entspricht, bitten wir Sie, mit uns Kontakt aufzunehmen, um Ihre Bedenken klären zu können.

Darüber hinaus haben Sie das Recht, Ihre Bedenken im Zusammenhang mit der Verarbeitung Ihrer personenbezogenen Daten an eine Aufsichtsbehörde in der EU heranzutragen. In Österreich ist die Aufsichtsbehörde die:

Österreichische Datenschutzbehörde

Barichgasse 40–42, 1030 Wien

Telefon: +43 (01) 52152-0

E-Mail: dsb@dsb.gv.at

10. Informationen zum Datenschutz

Laufende Informationen zum Datenschutz in der Oberbank AG können jederzeit unter www.oberbank.at/datenschutz abgerufen werden.

Stand: 08/2023