Stand: September 2026

Datenschutzerklärung für die Banking to go App der ING

Weil wir Ihre persönlichen Daten respektieren und schützen.

1. Unsere Datenschutz-erklärung

Vorwort

Mit unserer App Banking to go können Sie Ihr Online-Banking so erledigen, wie Sie wollen – unterwegs oder zu Hause, auf dem Smartphone oder Tablet. Damit die App reibungslos läuft und Sie alle Funktionen nutzen können, verarbeitet Banking to go personenbezogene Daten. Welche das sind und wie wir Ihre Daten schützen, erfahren Sie hier.

Unsere allgemeine Datenschutzerklärung finden Sie auf https://www.ing.de/datenschutz/

Wer sind wir?

Die ING-DiBa AG, im Folgenden „ING“ genannt, ist ein deutsches Kreditinstitut mit Sitz in Frankfurt am Main.

Als verantwortliche Stelle ergreifen wir alle gesetzlich erforderlichen Maßnahmen, um Ihre personenbezogenen Daten zu schützen:

ING-DiBa AG
Theodor-Heuss-Allee 2
60486 Frankfurt am Main

Bei Fragen zu dieser Datenschutzerklärung wenden Sie sich bitte an unseren Datenschutzbeauftragten:

ING-DiBa AG
Datenschutzbeauftragter
Theodor-Heuss-Allee 2
60486 Frankfurt am Main
E-Mail: datenschutz@ing.de

Wir informieren Sie des Weiteren, dass die ING-DiBa AG ein Tochterunternehmen der ING Bank N.V. ist. Die ING Bank N.V. ist ein europäisches Finanzinstitut, das den Datenschutzvorschriften der europäischen Datenschutz-Grundverordnung (Verordnung (EU) 2016/679) (DSGVO) unterliegt. Zur Einhaltung der DSGVO hat die ING Bank N.V. weltweite Datenschutzprinzipien über ihre Globalen Datenschutzrichtlinien (GDSR) eingeführt. Die GDSR sind weltweit für alle Unternehmen der ING Group, d.h. Tochtergesellschaften, Filialen, Vertretungen und Zweiggesellschaften bindend und wurden von den europäischen Datenschutzbehörden genehmigt. Daher hat die ING Group beschlossen, dass sämtliche ihrer globalen Unternehmen, Tochtergesellschaften, Filialen, Vertretungen und Zweiggesellschaften – unabhängig von ihrem Standort, ihren Zielmärkten oder -kunden – zusätzlich zu den nationalen Datenschutzgesetzen und -vorschriften die GDSR einhalten müssen.

2. Für wen gilt diese Daten-schutzerklärung?

Wir bei der ING sind uns bewusst, wie wichtig Ihnen Ihre personenbezogenen Daten sind. Diese Datenschutzerklärung erklärt auf einfache und transparente Weise, welche personenbezogenen Daten wir im Rahmen der Nutzung der Banking to go App erheben, erfassen, organisieren, ordnen, speichern, anpassen oder verändern, auslesen, abfragen, verwenden, durch Übermittlung offenlegen, verbreiten oder in einer andere Form bereitstellen, abgleichen oder verknüpfen, einschränken, löschen oder vernichten, sowie wie wir das tun.

Diese Datenschutzerklärung gilt für unsere Kunden, welche die Banking to go App verwenden.

87.839/09.26/3038/14

3. Welche personenbezogenen Daten erheben wir und wofür nutzen wir Ihre Daten?

Personenbezogene Daten sind alle Informationen, die uns etwas über Sie sagen oder die wir mit Ihnen in Verbindung bringen können. Dazu zählen unter anderem Ihr Name, Ihre Anschrift, Ihr Geburtsdatum, Ihre Kontonummer, IP-Adresse oder Informationen zu Zahlungen, die von einem Bankkonto aus erfolgen. Mit „Verarbeiten" meinen wir das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

Die Sicherheit Ihrer Daten hat für uns oberste Priorität. Im Sinne der zweiten Zahlungsdienstrichtlinie (EU) („PSD2") ist eine sogenannte starke Kundenauthentifizierung vorgeschrieben. Hierbei müssen mindestens zwei der folgenden drei Merkmale eingesetzt werden: **Wissen** (bspw. ein Passwort oder eine PIN), **Besitz** (bspw. ein eindeutig authentifiziertes Smartphone) und **Inhärenz** (ein Merkmal, das dem Benutzer persönlich oder körperlich zu Eigen ist, bspw. ein Fingerabdruck). Zu diesem Zweck beachten Sie bitte folgende Informationen:

3.1 Installation der App

Um die App installieren zu können, müssen Sie zuvor mit einem Drittanbieter (Google Inc., Apple Inc, nachfolgend als „Drittanbieter" bezeichnet) eine Nutzungsvereinbarung über den Zugang zu einem Portal oder Online-Shop des jeweiligen Drittanbieters (Google Play Store, Apple App Store, nachfolgend als „Drittportal" bezeichnet) abschließen. Die ING ist nicht Partei einer derartigen Vereinbarung und hat keinen Einfluss auf die Datenverarbeitung durch den Drittanbieter. Welche Daten auf welche Art und Weise der Drittanbieter Im Rahmen der Registrierung zu dem Drittportal verarbeitet werden, können Sie der Datenschutzerklärung des Drittanbieters entnehmen.

3.2 Nutzung der App

Bei Nutzung der Banking to go App erheben wir die nachfolgend beschriebenen personenbezogenen Daten, um die komfortable Nutzung der Funktionen zu ermöglichen. Wenn Sie unsere mobile App nutzen möchten, erheben wir Daten, die für uns technisch erforderlich sind, um Ihnen die Funktionen unserer mobilen App anzubieten und die Stabilität und Sicherheit zu gewährleisten.

Folgende Informationen zu Ihren Endgeräten werden durch die App an die Bank übermittelt und dort gespeichert:

- Version der App
- Gerätemodell
- Das auf dem Gerät installierte Betriebssystem inkl. der Version
- Gerätename
- Zeitpunkt der Registrierung des Geräts

Die genannten Daten werden zum Zweck des Supports und zur Unterscheidung von verschiedenen Geräten in der Geräteverwaltung genutzt. Für das Messaging gelten ein paar Sorgfaltspflichten:

- Um zu vermeiden, dass Dritte Ihre Messages lesen, sollten Sie anderen keinen Zugriff auf Ihr Gerät geben.
- Grundsätzlich ist es immer möglich, dass Messages durch Schad-Software auf Ihrem mobilen Endgerät ausgelesen werden. Deshalb sind Sie zum sorgfältigen Umgang mit Ihrem Gerät verpflichtet – und dazu, die Sicherheitshinweise zum Internetbanking auf https://www.ing.de/hilfe/internetbanking/kundenservice/
- zu beachten, insbesondere die empfohlenen Maßnahmen zum Schutz Ihrer Hard- und Software.
- Die erforderlichen Einstellungen auf Ihrem Smartphone oder Tablet machen Sie selbst.

Für die im Folgenden unter dieser Ziffer dargestellten Verarbeitungsvorgänge (einschließlich Übermittlungen an Dritte) ist Ihr kartenausgebendes Institut bzw. die jeweilige Akzeptanzstelle verantwortliche Stelle; soweit die ING in diesem Zusammenhang Daten verarbeitet, handelt sie dabei lediglich als technischer Dienstleister des entsprechenden Instituts.

Im Rahmen der App werden durch folgende Funktionen Daten verarbeitet:

a) Anmeldung in der App

Um die App zu registrieren benötigen Sie ihre Zugangsnummer und die Internetbanking PIN. Wenn Sie sich nun anmelden wollen, vergeben Sie eine selbstgewählte mobile PIN. Um die mobile PIN freizuschalten, müssen Sie dies durch Eingabe zweier iTANs oder durch Eingabe eines per SMS erhaltenen Einmalpassworts oder durch Freigabe aus einer bereits auf dem Zugang registrierten App erledigen. Nach der Registrierung benötigen Sie für zukünftige Autorisierungen nur noch die mobile PIN bzw. das biometrische Merkmal. Je nach Gerät kann die Möglichkeit bestehen, sich mit einem biometrischen Merkmal anzumelden und/oder dadurch Transaktionen freizugeben. Wenn Sie sich für die Nutzung eines biometrischen Merkmals entscheiden, tritt dieses an die Stelle der mobile PIN. Die ING hat keinen Zugriff auf die biometrischen Merkmale. Die Erkennung und Verarbeitung übernimmt das lokal auf Ihrem mobilen Endgerät ausgeführte Betriebssystem (iOS bzw. Android). Die mobile PIN und das biometrische biometrische Merkmal werden somit nicht an unsere Server übermittelt und auch nicht durch die ING gespeichert.

b) Nutzung der physischen Karten als digitale Karte in der App

Für die Nutzung Ihrer Karte der ING als digitale Karte in der App wird, wie für die Anmeldung in der App, die mobile PIN bzw. das biometrische Merkmal benötigt. Diese werden hierbei für Autorisierungen, z.B. für die

Bestätigung von VISA-Zahlungen verwendet. Die Karten müssen von Ihnen nicht extra in unserer App hinterlegt werden. Diese werden genauso wie die Kontenübersicht oder die Umsatzliste anhand des registrierten Zugangs ermittelt und bei jedem Login neu von unseren Systemen geladen. Bei der Nutzung des Services werden die folgenden personenbezogenen Daten verarbeitet:

- Stammdaten – bspw. Vor- und Nachname
- Adressdaten – bspw. Ihre PLZ
- Vertragsdaten – bspw. IBAN
- Daten zu Ihrer Kreditkarte – bspw. die Kreditkartennummer

In der App werden Ihnen bei der Girocard die IBAN sowie der Name des Karteninhabers angezeigt. Bei der VISA Card werden die letzten 4 Stellen der Kartennummer, der Name des Karteninhabers sowie das Ablaufdatum angezeigt. Diese Daten werden durch die ING in gleicher Weise wie bei einem allgemeinen Zugriff auf Ihre Onlinebanking-Anwendung verarbeitet.

Wenn Sie eine Ersatzkarte bestellen, wird innerhalb einer Session die Information gespeichert, ob Sie bereits eine Karte bestellt haben oder nicht. Die Speicherung erfolgt bis Sie sich aus der App ausloggen, sobald Sie sich ausgeloggt haben wird diese Information wieder gelöscht. Gespeichert werden folgenden Daten: Bestellung ja/nein, Karten-ID (verschlüsselte Kartennummer).

c) Zusätzliche Bestimmungen für Debitkarten

Des Weiteren sind besondere Bestimmungen für die von der ING ausgegebenen Karten in Form von Debitkarten der VISA Europe Services Inc. zu beachten, die im Folgenden erläutert werden:

Bei VISA Europe Ltd. handelt es sich um ein Unternehmen mit Hauptsitz in London (Großbritannien) und somit außerhalb der EU. Daten betreffend die Abwicklung einer Zahlung werden von VISA Europe Ltd. somit ggf. außerhalb der EU verarbeitet (mit Blick auf die entsprechenden Verarbeitungen durch VISA Europe Ltd. ist diese die verantwortliche Stelle im datenschutzrechtlichen Sinne). Teilweise werden hierbei mit den Datenschutzbehörden abgestimmte sog. verbindliche interne Datenschutzvorschriften (Binding Corporate Rules) verwendet, die sicherstellen, dass ein angemessenes Datenschutzniveau mit Blick auf die in Großbritannien verarbeiteten Daten besteht. Soweit VISA Europe Ltd. personenbezogene Daten des Nutzers außerhalb der EU verarbeitet, wird darüber hinaus ein angemessenes Datenschutzniveau regelmäßig dadurch sichergestellt, dass entsprechende sog. EU-Standardvertragsklauseln verwendet werden, die sicherstellen, dass ein entsprechendes Schutzniveau erreicht wird.

Weitere Informationen zu den entsprechenden Regelungen erhalten Sie von Visa Europe Ltd. unter folgendem Datenschutzhinweis hier: https://www.ing.de/dokumente/datenschutzinformationen-visa/.

Eine Übermittlung der Zahlungsabwicklungsdaten an diese Unternehmen ist für die Abwicklung entsprechender Debitkartenzahlungen erforderlich.

d) Allgemeine Nutzung der Dienste

Sobald Sie über die App einen der Dienste nutzen oder den Versuch unternehmen, dies zu tun, stellt Ihr mobiles Endgerät eine Online-Verbindung zu dem Server der Dienstleister der Bank her. Die Übermittlung von Daten an den Server ist erforderlich, damit Sie Inhalte auf Ihrem mobilen Endgerät abrufen können. Die Bank führt das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, die Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung der personenbezogenen Daten der Nutzer grundsätzlich nur dann und nur in dem Umfang aus, wie es zur Erbringung der Dienste erforderlich ist.

Während Ihrer Nutzung der App verarbeitet der Servicedienstleister der Bank Daten (z.B. Kreditkartenumsatzanfragen, Kreditkartenumsätze, IP-Adresse, Beginn und Ende der Nutzung, aufgerufene Funktionen/Einstellungen), die für den bestimmungsgemäßen Zugang zu den Diensten und deren bestimmungsgemäße Nutzung erforderlich sind.

Ihnen können in der App ggf. bestimmte Informationen zu den von Ihnen durchgeführten Transaktionen zur Verfügung gestellt werden (insbesondere Bezahlbetrag und Bezahldatum), damit Sie einen Überblick über die bereits getätigten Transaktionen erhalten. Die entsprechenden Daten werden Ihnen von der ING zur Verfügung gestellt. Bitte beachten Sie hierbei: Diese Transaktionshistorie stellt keinen rechtsgültigen Kontoauszug dar. Rechtsverbindliche Buchungen und Rechnungsabschlüsse erfolgen nur nach Maßgabe der Allgemeinen Geschäftsbedingungen der ING.

e) Fotoüberweisung

Für Sie besteht im Rahmen der App auch die Möglichkeit eine Überweisung mittels eines Scans über ihre Kamera zu tätigen. Für die Fotoüberweisung benötigt die App die Berechtigung für den Zugriff auf die Kamera. Diesbezüglich können Sie nach Installation der App deren Zugriff auf die Kamera freigeben. Zusätzlich kann die App den Zugriff auf „Fotos und Medien“ erfordern, wenn Sie hierfür bereits aufgenommene Fotos oder PDFs verwenden möchten.

Diese Zugriffsberechtigung ist für die Nutzung dieses Dienstes erforderlich und wird nach Erteilung anhand eines sog. Flags (Kennzeichnung) im Betriebssystem Ihres jeweiligen mobilen Endgerätes gespeichert und muss für jedes neue Gerät erneut gegeben werden. Vor der ersten Nutzung der Fotoüberweisung bekommen Sie einen Hinweis „Datenschutzrechtliche Einwilligungserklä-

rung“ angezeigt. Dieser muss akzeptiert werden, damit die Fotoüberweisung genutzt werden kann. Bei Erteilung der Einwilligung wird diese in der App gespeichert, so dass dieser Hinweis bei der nächsten Nutzung nicht noch einmal angezeigt wird. Wollen Sie sodann eine Fotoüberweisung durchführen, so scannen Sie die Daten der Überweisung oder eines QR-Codes auf der Überweisung mittels der Kamera, sodass diese in die Überweisungsvorlage übernommen werden. Alternativ können Sie ein PDF oder bereits vorhandenes Foto der Überweisung hochladen, sodass die Daten in die Überweisungsvorlage übernommen werden.

Das Auslesen der Daten erfolgt bei unserem Dienstleister DTI GmbH. Rechtsgrundlage für diese Verarbeitung ist Art. 6 Abs. 1 Buchst. a DSGVO. Sie haben dann, wie bei jeder Überweisung, noch einmal die Möglichkeit, die Daten zu überprüfen und mit der Freigabe der Transaktion werden die Daten, wie gewohnt, zum Zwecke der Durchführung der Transaktion an die ING übermittelt.

Die Einwilligung kann jederzeit über das Zurücksetzen der App widerrufen werden. Außerdem haben Sie die Möglichkeit, die Einwilligung jederzeit in den Einstellungen im Bereich „Fotoüberweisung“ zu widerrufen.

f) Funktion „Wero“

Die Funktion „Wero“ (im Folgenden: „der Dienst“) ermöglicht Ihnen, Geld an Ihre Kontakte aus dem Adressbuch Ihres Smartphones zu überweisen, ohne deren IBAN zu kennen, Geld von diesen Kontakten anzufordern, oder bei teilnehmenden Händlern online über Browser oder App zu bezahlen. Die Zahlung ist nur möglich, wenn Sie und Ihr Kontakt bzw. der Händler jeweils bei Ihrem Kreditinstitut für den Dienst registriert sind. Wie die Registrierung funktioniert, sehen Sie weiter unten. Die Abwicklung der Zahlung ist nur möglich, wenn die ING App Sie und Ihre Kontakte oder den Händler als Teilnehmer des Dienstes identifiziert. Die Identifikation erfolgt anhand eines Abgleiches der bei der Registrierung des Dienstes angegebenen Nutzerkennung und der Nutzerkennung ihrer Kontakte oder des Händlers. Die Nutzerkennung kann Ihre Mobilfunknummer, Ihre E-Mail-Adresse oder ein QR-Code mit einer Ihrem Konto zugewiesenen Identifikationszahl sein.

Registrierung

Zur Nutzung des Dienstes ist eine Registrierung in unserer ING App erforderlich. Sie wählen zuerst Ihr gewünschtes Girokonto als Referenzkonto für den Dienst aus. Falls Sie eine Nutzerkennung in Form einer Mobilfunknummer oder E-Mail-Adresse angeben möchten, erhalten Sie eine SMS mit einem Bestätigungscode an die von Ihnen zwecks Registrierung angegebene Nutzerkennung damit wir diese verifizieren und Ihren Zugang zum Dienst freischalten können. Die für die Registrierung genutzte Nutzerkennung kann von den in Ihren Stammdaten gegebenenfalls hinterlegten Kontaktdaten abweichen, das heißt, die Registrierung führt nicht zur Änderung Ihrer Stammdaten. Infolge der Registrierung werden bestimmte erforderliche Daten verarbeitet, z.B. Ihr Name, Ihre Kundennummer, die IBAN des gewählten Referenzkontos und ihre Nutzerkennung. Diese müssen an den zentralen Wero-Dienst bei EPI Company SE übermittelt werden. EPI Company SE erhält nur die für die Registrierung und den Betrieb des Dienstes notwendigen personenbezogenen Daten von Ihnen, welche zur Vertragserfüllung erforderlich sind.

Synchronisieren von Kontakten

Bei der erstmaligen Nutzung des Dienstes und bei jedem Aufruf des Dienstes werden von der ING App die Kontaktdaten aus dem Adressbuch Ihres Smartphones (gespeicherte Nutzerkennungen samt Kontaktnamen) zwecks Abgleiches und Synchronisierung abgerufen, sofern Sie der App dazu die Freigabe erteilt haben. Die App erstellt Prüfsummen (sogenannte Hash-Werte) aus den Nutzerkennungen Ihrer Kontakte sowie Ihrer Mobilfunknummer. Ausschließlich diese Prüfsummen werden für die Kontaktsynchronisierung an den zentralen Wero-Dienst (von EPI Company SE) übermittelt. Anhand der Prüfsummen werden durch den zentralen Wero-Dienst registrierte Teilnehmer am Wero-Verfahren ermittelt und an Sie in der App rückbestätigt und angezeigt. Ausschließlich identifizierte Wero- Kontakte stehen Ihnen in der Funktion als Empfänger für Geld-Sendungen und Geld-Anforderungen zur Verfügung. Sie werden in der im Wero Dienst dargestellten Kontaktliste mit den Kontaktnamen entsprechend Ihrem Adressbuch angezeigt. Für andere aktive Wero Nutzer ist im Rahmen ihrer Wero Nutzung folglich auch sichtbar, dass Sie am Wero Verfahren teilnehmen, jedoch nur, wenn diese Nutzer Ihre für Wero registrierte Nutzerkennung in ihrem Adressbuch hinterlegt haben oder diese manuell über das vorgegebene Suchfeld suchen. Die Prüfsummen der Nutzerkennungen Ihrer Kontakte, die ebenfalls den Dienst nutzen, sowie deren Namen aus Ihrem Adressbuch, werden auf dem Server der ING Group gespeichert. Das ist erforderlich, um den Dienst nutzen zu können und den Vertrag mit Ihnen zu erfüllen. Außerdem ist es notwendig, um etwaige Wero-Nachrichten zuordnen zu können, wenn Sie den Dienst auf unterschiedlichen Mobilfunkgeräten nutzen und ihre Adressbücher unterschiedliche Kontakte aufweisen, da jeweils Kontaktdaten zu den bereits erfolgten Wero-Nachrichten fehlen könnten. Können wir anhand ihrer Kontakte keine Zuordnung zu einer erhaltenen Wero-Zahlung treffen, zeigen wir Ihnen den Namen des Nutzers gemäß dessen Wero-Registrierung an. Dies kann der Fall sein, wenn ein Nutzer Ihre Nutzerkennung als Kontakt im Adressbuch hinterlegt hat, sie diesen jedoch nicht.

Welche personenbezogenen Daten verarbeiten wir und wofür?

- Vollständiger Name: dient der Identifikation des Kunden
- Daten zur Identifizierung des zugehörigen Kontos und weiteren Support (Nutzerkennungen wie die Telefonnummer oder E-Mail-Adresse des Nutzers)

- IBAN: wird als Zielkonto mit der Nutzerkennung verknüpft und für Zahlungseingänge und Zahlungsausgänge genutzt
- Telefonbuchkontakte (in anonymisierter Form): dient dem Abgleich der Empfängerinformationen und der Identifikation der über Wero erreichbaren Kontakte

Geld an Kontakte senden oder von Kontakten anfordern

Sie wählen einen Kontakt aus der im Wero Dienst dargestellten Kontaktliste aus oder suchen diesen manuell über das zur Verfügung gestellte Suchfeld. In den Folgeschritten geben Sie einen zu überweisenden Geldbetrag ein und können einen optionalen Begleittext definieren. Zur Bestätigung wird Ihnen der Name Ihres Kontaktes, der zu überweisende Betrag und der von Ihnen gewählte Begleittext angezeigt. Nach einer Freigabe mittels zweiten Faktors wird eine Wero-Nachricht an den Empfänger übermittelt und die zugehörige SEPA Echtzeitüberweisung ausgelöst. Der Kontakt wird gemäß der verfügbaren Benachrichtigungsoptionen des teilnehmenden Kreditinstituts und den gewählten, persönlichen App-Einstellungen über die Initiierung der Zahlung informiert. Eine Geld-Anforderung von einem Kontakt erfolgt analog einer Geld-Sendung. Eine gesonderte Freigabe ist hierfür nicht erforderlich. Zwecks Durchführung einer Überweisung wird die Giro-IBAN verarbeitet.

Eine Online-Zahlung über Wero durchführen

Wenn Sie über ihren Internetbrowser Ihren Online-Einkauf mit Wero bezahlen möchten, wird Ihnen beim Check-out Prozess ein Wero QR-Code angezeigt. Dieser muss mit Ihrer Handy-Kamera oder dem zur Verfügung gestellten Scanner in der ING App gescannt werden. Bei Ihrer ersten Online-Zahlung müssen Sie Ihr Kreditinstitut auswählen, bevor der QR-Code generiert wird. Bei der Auswahl können Sie Ihre entsprechende Banking-App als Standard festlegen. Im Anschluss wird Ihnen nach Anmeldung in der ING App eine bereits ausgefüllte Bezahlungsmaske angezeigt. Sofern alles korrekt ist, können Sie die Zahlung mit Hilfe des zweiten Faktors bestätigen und eine SEPA Echtzeitüberweisung durchführen.

Wenn Sie Ihr Mobilgerät für Ihren Online-Einkauf mit Wero nutzen, werden Sie nach Auswahl der Zahlungslösung Wero direkt in Ihre ING App weitergeleitet. Bei Ihrer ersten Zahlung müssen sie Ihr Kreditinstitut auswählen und können Ihre entsprechende Banking-App als Standard festlegen. Im Anschluss wird Ihnen nach Anmeldung in der ING App eine bereits ausgefüllte Bezahlungsmaske angezeigt. Sofern alles korrekt ist, können Sie die Zahlung mit Hilfe des zweiten Faktors bestätigen und eine SEPA Echtzeitüberweisung durchführen.

Wofür nutzen wir Ihre Daten und auf welcher Rechtsgrundlage?

Für die Nutzung des Wero-Dienstes werden Daten insbesondere zum Zwecke der Vertragsanbahnung (Registrierung) sowie -durchführung (Geld senden, anfordern oder Online-Zahlung), zur Erfüllung von gesetzlichen Vorgaben (Transaktionsscreening, Fraud Checks) sowie auf Basis einer Interessensabwägung (Erstellung von aggregierten Reports für die Verbesserung und Entwicklung des Wero-Dienstes).

Näheres finden Sie außerdem hier:
Wero Datenschutzhinweise der EPI Company SE (https://wero-wallet.eu/de/datenschutzcenter).

g) Geolokalisierung

Die Geolokalisierung wird in der App ausschließlich für die Geldautomatensuche verwendet. Hierbei handelt es sich um unsere Website https://www.ing.de/kundenservice/geldautomatensuche/maps2/, die in die App eingebunden ist. Bei der Nutzung dieses Dienstes erhalten Sie einen (ausblendbaren) Hinweis, dass für die Kartendarstellung und die -ermittlung der nächstgelegenen Geldautomaten der Karten- und Lokalisierungsdienst von Google verwendet wird. Bei der Nutzung fordert die Website den Standort über die App an. Zu diesem Zweck können Sie der App eine Berechtigung zur Standortermittlung über einen Systemdialog Ihres Android-Betriebssystems oder iOS geben und diese in den Systemeinstellungen auch wieder entfernen.

Wenn sie sich dazu entscheiden, diese Berechtigung zu geben, dann leitet das Betriebssystem Ihres mobilen Endgeräts die geographischen Koordinaten (Längen- und Breitengrad) an die App weiter und diese reicht die Koordinaten sowie die IP-Adresse weiter an den Kartendienst Yellowmap. Dieser wird dort lediglich für die Ermittlung der nächst gelegenen Standorte und der benötigten Kartenausschnitte verwendet und danach verworfen. Der Standort wird weder an uns übermittelt, noch wird dieser dauerhaft in der App gespeichert.

Einen Hinweis noch: Sie können die Geldautomatensuche auch ohne die Vergabe der entsprechenden Berechtigung durchführen. Ihnen werden dann jedoch nicht direkt die Geldautomaten in ihrer Umgebung angezeigt, sondern Sie müssen zunächst im Suchfeld die Stadt eingeben, für die und deren Umgebung Sie diese Information wünschen.

h) Cookies

Die Seite zur Geldautomatensuche nutzt wie auch die ING-Website mehrere Arten von Cookies. Technische und funktionale Cookies werden zwingend benötigt, damit bei Ihrem Besuch der Website alles gelingt. Darüber hinaus werden Marketing-Cookies verwendet, damit wir Sie auf der Seite wiedererkennen und den Erfolg unserer Kampagnen messen können, sowie Personalisierungs-

Cookies, mit denen wir Sie auch außerhalb unserer Websites besser ansprechen können.

Weitere Informationen über Cookies erhalten Sie auch auf unserer Website unter https://www.ing.de/datenschutz/cookies/.

i) Feedback

Wir möchten unsere mobilen Applikationen regelmäßig verbessern und Ihren Bedürfnissen anpassen. Dazu sind wir auf Ihr Feedback angewiesen. Egal ob Lob oder Kritik – Wir freuen uns über Verbesserungsvorschläge jeder Art.

Wenn Sie uns ein Feedback senden, werden zur weiteren Bearbeitung folgende Daten an uns übermittelt und bei der ING gespeichert:
- Modellname (zB Samsung Galaxy)
- verwendete Version der App (bei iOS und Android)
- Betriebssystem-Version (bei iOS und Android)
- Plattform für das Device (iPhone, iPad)
- iOS Systemname („iOS“)
- der Text, den Sie in das Formularfeld eingeben
- Ihr Name
- Ihre Partnernummer
- Ihre Kundennummer
- Die AccessUID
- Anschrift
- Geburtsdatum
- Kontonummer

j) Push-Mitteilungen/Benachrichtigungen

Mit unseren Push-Mitteilungen/Benachrichtigungen (kurz „Messaging“) können Sie sich jederzeit über Transaktionen auf Ihrem Girokonto informieren lassen. Einmal eingerichtet, schicken wir Ihnen bei relevanten Ereignissen Push-Benachrichtigungen („Messages“) auf Ihr mobiles Endgerät. So sind Sie immer gut informiert, ohne sich einloggen zu müssen.

Die Voraussetzungen für die Nutzung des Messagings sind:
- Eine Internetverbindung (mobiles Internet/WLAN)
- Zugangsdaten für das Internetbanking
- Ein mobiles Endgerät aktueller Banking to go App

Welche Messages Sie bekommen, können Sie in den Einstellungen Ihrer App selbst festlegen.

Sofern Sie sich dazu entscheiden Push-Mitteilungen/Benachrichtigungen zu erhalten, verarbeiten wir die dafür notwendigen Daten. Hierbei kann es sich u.a. um die Kundennummer, Partnernummer oder Kontonummer handeln.

Noch ein wichtiger Hinweis: Den Inhalt der Messages schützen wir mit einer TLS-Verschlüsselung, die dem aktuellen Industrie- und Sicherheitsstandard entspricht. Weil die Messages jedoch von Systemen großer Anbieter versendet werden, können wir nicht mit Sicherheit ausschließen, dass diese Kenntnis von einzelnen Messages bekommen. Wenn Sie damit nicht einverstanden sind, empfehlen wir Ihnen, den Dienst nicht zu verwenden. Nach vorherig erteilter Erlaubnis können Sie diese in den Einstellungen widerrufen.

k) IBM Trusteer

Was ist IBM Trusteer und wofür nutzen wir es?
Wir setzen IBM Trusteer (www.ibm.com/de-de/products/trusteer-mobile-sdk) zur Analyse von schadhaftem Verhalten in unserer App für ein sicheres E-Banking und Betrugsprävention ein. Hierbei werden beispielsweise technische Daten über das Gerät, die IP Adresse, die Wifi SSID, Browser Informationen, das Nutzerverhalten, geographische Merkmale, Geräteposition, Anrufstatus und die Zeitzone verarbeitet und gelöscht, sobald Sie für die Bearbeitung nicht mehr benötigt werden. Die Daten werden keinesfalls an Dritte weitergegeben. Rechtsgrundlage für die Datenverarbeitung zur Sicherstellung der App-Sicherheit ist die rechtliche Verpflichtung gem. Art. 6 Abs. 1 S. 1 lit. c) DSGVO. Weitere Informationen über Trusteer erhalten Sie auch auf unserer Website unter https://www.ing.de/datenschutz/cookies/

l) App-Analyse

Um unsere mobilen Applikationen für Sie regelmäßig zu verbessern und um Fehler zu beheben, setzen wir Analysedienste ein. Wir erklären Ihnen, welche Tools wir dafür verwenden.

Wie funktioniert der Analysedienst Mapp?

Für die Durchführung der App-Analyse kommt die Anwendung Mapp (www.mapp.com/de/) der Mapp Digital Germany GmbH in der App zum Einsatz. Es werden hierfür ausschließlich pseudonyme Daten verwendet, das heißt Daten, aus denen ein Dritter keinen Personenbezug herleiten kann. Die pseudonymen Daten dienen ausschließlich dazu, unsere App-Inhalte und -Funktionen für Sie zu verbessern. Sie werden keinesfalls an Dritte verkauft. Daten werden gelöscht, sobald sie für die Bearbeitung nicht mehr benötigt werden.

Widerspruchsrecht zum Analysedienst Mapp in der App

Sie können der Übermittlung und Speicherung der Mapp Analyse-Daten durch eine entsprechende Einstellung in unseren mobilen Applikationen verhindern. Sie finden diese Einstellung mit dem Namen „App-Analyse“ im Bereich „Profi l“ unter dem Menüpunkt „Analyse“.

Was ist App Center und wofür nutzen wir es?

Wir setzen die Anwendung App Center (www.appcenter.ms) von Microsoft zur Erstellung und Versendung von anonymen Fehlerberichten bei unplanmäßigem Verhalten der App, insbesondere bei Abstürzen, ein. Hierbei

werden die Geräte ID, technische Daten über das Gerät und Zeitpunkt des App-Absturzes anonymisiert verarbeitet und gelöscht, sobald sie für die Bearbeitung nicht mehr benötigt werden.

Die Daten werden keinesfalls an Dritte verkauft.

Widerspruchsrecht zu App Center in der App

Sie können die Übermittlung der Fehlerberichte durch eine entsprechende Einstellung in unseren mobilen Applikationen verhindern. Sie finden diese Einstellung mit dem Namen „Berichte senden“ im Bereich „Profil“ unter dem Menüpunkt „Analyse“.

m) Chat-Funktion

Über die Chat-Funktion können Sie jederzeit Kontakt zur ING aufnehmen, um beispielsweise Anliegen zu Ihrem Konto oder Fragen zu unseren Produkten zu adressieren. Bei Verwendung der Chat-Funktion werden folgende Daten verarbeitet und gespeichert:

- Chat-Konversation einschließlich Daten zur Konto- und Kundenbeziehung,
- Name,
- Zeitpunkte der Kontaktaufnahme

Die vorgenannten Daten werden ausschließlich zum Zwecke des Kundenkontakts und der Bearbeitung entsprechender Anliegen verwendet. Rechtsgrundlage für die Verarbeitung der Daten ist die Geschäftsbeziehung zwischen Ihnen und ING DiBa AG (Vertragserfüllung gemäß Art. 6 Abs. 1 Satz 1 lit. b) DSGVO). Im Rahmen der Nutzung der Chat-Funktion werden die Daten durch einen Telekommunikationsdienstleister im Rahmen einer Auftragsverarbeitung verarbeitet. Eine Übermittlung der Daten in ein Land außerhalb der EU bzw. des Europäischen Wirtschaftsraums findet nicht statt. Jede Chatkonversation samt vorgenannten Daten wird für jeweils 6 Jahre gespeichert und anschließend gelöscht.

4. Auf welcher Rechtsgrundlage werden die Daten erhoben?

Soweit erforderlich, verarbeiten wir Ihre Daten über die eigentliche Erfüllung des Vertrages hinaus (Art. 6 Abs. 1 Satz 1 Buchstabe b) DSGVO) sowie zur Wahrung berechtigter Interessen von uns oder Dritten (Art. 6 Abs. 1 Satz 1 Buchstabe f) DSGVO), z.B. zur Geltendmachung rechtlicher Ansprüche und Verteidigung bei rechtlichen Streitigkeiten oder zur Gewährleistung der IT-Sicherheit und des IT-Betriebs der Bank. Auch wollen wir die Risikosteuerung in unserem Konzern sowie die Weiterentwicklung von Dienstleistungen und Produkten für Sie auch in Zukunft weiter verbessern. Darüber hinaus verarbeiten wir Ihre Daten, soweit Sie uns Ihre Einwilligung gem. Art. 6 Abs. 1 Satz 1 Buchstabe a) DSGVO erteilt haben.

5. Wie lange speichern wir Ihre Daten?

Wir speichern Ihre Daten nicht länger, als wir sie für die jeweiligen Verarbeitungszwecke benötigen. Sind die Daten für die Erfüllung vertraglicher oder gesetzlicher Pflichten nicht mehr erforderlich, werden diese regelmäßig gelöscht, es sei denn, deren – befristete – Aufbewahrung ist weiterhin notwendig. Gründe hierfür können z.B. folgende sein:

- Die Erfüllung gesetzlicher Aufbewahrungspflichten: Zu nennen sind insbesondere das Handelsgesetzbuch, die Abgabenordnung, das Kreditwesengesetz, das Geldwäschegesetz und das Wertpapierhandelsgesetz. Die dort vorgegebenen Fristen zur Aufbewahrung bzw. Dokumentation betragen bis zu zehn Jahre.
- Das Erhalten von Beweismitteln für rechtliche Auseinandersetzungen im Rahmen der gesetzlichen Verjährungsvorschriften: Zivilrechtliche Verjährungsfristen können bis zu 30 Jahre betragen, wobei die regelmäßige Verjährungsfrist drei Jahre beträgt.

Sobald Ihre personenbezogenen Daten nicht mehr für den Zweck benötigt werden, für den sie verarbeitet werden, löschen oder anonymisieren wir sie entsprechend den einschlägigen Gesetzen und Rechtsvorschriften

6. Ihre Rechte

Wir wollen so schnell wie möglich auf alle Ihre Fragen antworten. Manchmal kann es aber trotzdem bis zu einem Monat dauern, ehe Sie eine Antwort von uns bekommen. Sollten wir länger als einen Monat für eine abschließende Klärung brauchen, sagen wir Ihnen selbstverständlich vorher Bescheid, wie lange es dauern wird.

In einigen Fällen können oder dürfen wir keine Auskunft geben. Sofern dies gesetzlich zulässig ist, teilen wir Ihnen in diesem Fall immer zeitnah den Grund für die Verweigerung mit.

Welche Rechte haben Sie als betroffene Person, wenn es um die Verarbeitung Ihrer Daten geht?

Ihr Recht auf Auskunft

Sie sind berechtigt, von uns eine Übersicht Ihrer von uns verarbeiteten personenbezogenen Daten zu verlangen. So können Sie z.B. eine Kopie der personenbezogenen Daten erhalten, die wir über Sie speichern.

Ihr Recht auf Berichtigung

Sollten Ihre Angaben nicht (mehr) zutreffend sein, können Sie eine Berichtigung verlangen. Sollten Ihre Daten unvollständig sein, können Sie eine Vervollständigung verlangen. Wenn wir Ihre Angaben an Dritte weitergegeben haben, informieren wir diese Dritten

über Ihre Berichtigung – sofern dies gesetzlich vorgeschrieben ist.

Ihr Recht auf Löschung

Aus folgenden Gründen können Sie die unverzügliche Löschung Ihrer personenbezogenen Daten verlangen:

- Wenn Ihre personenbezogenen Daten für die Zwecke, für die sie erhoben wurden, nicht länger benötigt werden
- Wenn Sie Ihre Einwilligung widerrufen und es an einer anderweitigen Rechtsgrundlage fehlt
- Wenn Sie der Verarbeitung durch schlüssige Begründung widersprechen und es keine überwiegenden, schutzwürdigen Gründe für eine Verarbeitung gibt
- Wenn Ihre personenbezogenen Daten unrechtmäßig verarbeitet wurden
- Wenn Ihre personenbezogenen Daten gelöscht werden müssen, um gesetzlichen Anforderungen zu entsprechen.

Ihr Recht auf Einschränkung der Verarbeitung

Sie haben das Recht, aus einem der folgenden Gründe eine Einschränkung der Verarbeitung Ihrer personenbezogenen Daten zu verlangen:

- Wenn die Richtigkeit Ihrer personenbezogenen Daten von Ihnen bestritten wird und wir die Möglichkeit hatten, die Richtigkeit zu überprüfen
- Wenn die Verarbeitung nicht rechtmäßig erfolgt und Sie statt der Löschung eine Einschränkung der Nutzung verlangen
- Wenn wir Ihre Daten nicht mehr für die Zwecke der Verarbeitung benötigen, Sie diese jedoch zur Geltendmachung, Ausübung oder Verteidigung gegen Rechtsansprüche brauchen
- Wenn Sie Widerspruch eingelegt haben, solange noch nicht feststeht, ob Ihre Interessen überwiegen

Ihr Recht auf Datenübertragbarkeit

Sie haben das Recht, eine Kopie der Sie betreffenden Daten in einem strukturierten und allgemein gebräuchlichen übertragbaren Format zu erhalten und diese Daten an andere Organisationen weiterzuleiten. Sie haben auch das Recht, uns aufzufordern, Ihre personenbezogenen Daten direkt an andere von Ihnen genannte Organisationen weiterzuleiten. Wir übermitteln Ihre personenbezogenen Daten, soweit technisch möglich und nach einschlägigen nationalen Rechtsvorschriften zulässig.

Ihr Recht auf Widerspruch

Soweit wir Ihre Daten nur aufgrund von berechtigten Interessen oder im öffentlichen Interesse verarbeiten, haben Sie das Recht, der Verarbeitung Ihrer Daten bei Vorliegen einer besonderen Situation zu widersprechen. Wenn wir Ihre Daten für Direktmarketing- oder Werbeaktivitäten nutzen, können Sie der Verarbeitung ohne eine Begründung widersprechen.

Sie können jedoch nicht von uns verlangen, Ihre personenbezogenen Daten zu löschen, wenn

- wir zu deren Speicherung weiterhin rechtlich verpflichtet sind;
- dies für die Erfüllung eines Vertrags mit Ihnen erforderlich ist.

Bitte beachten Sie unseren gesonderten Hinweis im Abschnitt „Informationen über Ihr Widerspruchsrecht“.

Ihr Beschwerderecht

In einzelnen Fällen kann es passieren, dass Sie nicht zufrieden mit unserer Antwort auf Ihr Anliegen sind. Dann sind Sie berechtigt, beim Datenschutzbeauftragten der ING sowie bei der zuständigen Datenschutzaufsichtsbehörde Beschwerde einzureichen.

Einzelheiten zu Ihren Rechten ergeben sich aus den jeweiligen Regelungen der Datenschutz-Grundverordnung (Artikel 15 bis 22 DSGVO).

7. Wie wir Ihre personenbezogenen Daten schützen

Wir ergreifen geeignete technische und organisatorische Maßnahmen (Richtlinien und Verfahren, IT-Sicherheit usw.), um die Vertraulichkeit und Integrität Ihrer personenbezogenen Daten und ihrer Verarbeitung zu gewährleisten. Wir wenden unternehmensweit einen internen Rahmen an Richtlinien und Mindeststandards an, um Ihre personenbezogenen Daten zu schützen. Diese Richtlinien und Standards werden regelmäßig aktualisiert, um sie an die aktuellen Rechtsvorschriften und Marktentwicklungen anzupassen.

Zudem unterliegen ING-Mitarbeiterinnen und -Mitarbeiter der Schweigepflicht und dürfen Ihre personenbezogenen Daten nicht rechtswidrig oder unnötig offenlegen. Wenn Sie vermuten, dass Ihre personenbezogenen Daten in falsche Hände geraten sind, sollten Sie sich immer an die ING wenden, um uns beim dauerhaften Schutz Ihrer personenbezogenen Daten zu unterstützen.

8. Änderungen dieser Datenschutzerklärung

Wir können diese Datenschutzerklärung ändern, um Gesetzesänderungen zu entsprechen und/oder zu berücksichtigen, wie unser Unternehmen personenbezogene Daten verarbeitet. Wir ändern dann das Überarbeitungsdatum auf der ersten Seite entsprechend.

Wir empfehlen jedoch, diese Erklärung regelmäßig zu überprüfen, um stets darüber informiert zu sein, wie wir Ihre personenbezogenen Daten verarbeiten und schützen.

Informationen über Ihr Widerspruchsrecht

1. Einzelfallbezogenes Widerspruchsrecht

Sie haben das Recht, aus Gründen, die sich aus Ihrer besonderen Situation ergeben, gegen die Verarbeitung Ihrer personenbezogenen Daten Widerspruch einzulegen. Voraussetzung hierfür ist, dass die Datenverarbeitung im öffentlichen Interesse oder auf der Grundlage einer Interessenabwägung erfolgt. Dies gilt auch für ein Profiling. Im Falle eines zulässigen Widerspruchs werden wir Ihre personenbezogenen Daten nicht mehr verarbeiten. Es sei denn,

- wir können zwingende schutzwürdige Gründe für die Verarbeitung dieser Daten nachweisen, die Ihre Interessen, Rechte und Freiheiten überwiegen oder
- Ihre personenbezogenen Daten dienen der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

2. Widerspruch gegen die Verarbeitung Ihrer Daten für unsere Direktwerbung

In Einzelfällen nutzen wir Ihre personenbezogenen Daten für unsere Direktwerbung. Sie haben das Recht, jederzeit Widerspruch dagegen einzulegen; dies gilt auch für das Profiling, wenn es mit einer Direktwerbung in Verbindung steht. Im Falle eines Widerspruchs verarbeiten wir Ihre personenbezogenen Daten nicht mehr für diese Zwecke.

3. Kontakt

Der Widerspruch kann formfrei erfolgen und sollte möglichst gerichtet werden an:
ING-DiBa AG
Datenschutzbeauftragter
Theodor-Heuss-Allee 2
60486 Frankfurt am Main
E-Mail: datenschutz@ing.de