

# DATENSCHUTZERKLÄRUNG

## EINLEITUNG

Wir freuen uns über Ihr Interesse zum Thema Datenschutz bei der card complete Service Bank AG (card complete). Es ist uns ein großes Anliegen, dass Sie sich während des Besuchs unserer Website als auch im Zuge sämtlicher Geschäftsvorgänge mit uns sicher fühlen.

Sobald Sie Produkte und/oder Dienstleistungen der card complete in Anspruch nehmen, vertrauen Sie uns als datenschutzrechtlichem Verantwortlichen Ihre personenbezogenen Daten an, welchen wir einen besonders hohen Schutzwert beimessen. Daher informieren wir Sie ausführlich darüber welche personenbezogenen Daten wir von Ihnen erfassen, wie wir diese verarbeiten und an wen wir diese allenfalls weiterleiten. Des Weiteren möchten wir Ihnen mitteilen, welche Vorkehrungen wir treffen, um Ihre personenbezogenen Daten zu schützen, welche Rechte Sie in diesem Zusammenhang besitzen und an wen Sie sich bei datenschutzrechtlichen Anliegen wenden können. Im Hinblick auf die verwendeten Begrifflichkeiten, wie z. B. „Verarbeitung“, „personenbezogene Daten“, etc., verweisen wir auf die Definitionen gemäß der Datenschutz-Grundverordnung („DSGVO“) und dem österreichischen Datenschutzgesetz („DSG“).

## ZIELGRUPPEN

### FÜR WEN GILT DIESE DATENSCHUTZERKLÄRUNG?

**Diese Datenschutzerklärung gilt für folgende Personen bzw. Personengruppen:**

- Interessent:innen und Kund:innen (Privat- und Firmenkarteninhaber)
- Akzeptanzpartner
- Partnerbanken und Vertriebspartner
- Service-Dienstleister und Auftragsverarbeiter
- Besucher unserer Websites und Personen, die sich bspw. für unser Portal oder unsere Apps registrieren
- Alle anderen natürlichen Personen, die in Kontakt mit der card complete stehen

Die Datenschutzerklärung der DC elektronische Zahlungssysteme GmbH finden Sie auf <https://www.cardcomplete.com/datenschutz/dcez/>. Sie gilt für die Verarbeitung von personenbezogenen Daten im Rahmen der Servicetätigkeit mit card complete Terminals (POS Terminals).

## VERANTWORTLICHKEIT DATENVERARBEITUNG, KONTAKT DATENSCHUTZBEAUFTRAGTER

**WER IST FÜR DIE DATENVERARBEITUNG VERANTWORTLICH UND AN WEN KÖNNEN SIE SICH WENDEN, WENN SIE FRAGEN ZUM DATENSCHUTZ BEI CARD COMPLETE HABEN?**

**Für die Datenverarbeitung verantwortlich ist:**

card complete Service Bank AG (card complete)  
Lassallestraße 3  
1020 Wien

### **WIE KÖNNEN SIE KONTAKT IN BEZUG AUF DATENSCHUTZ ODER MIT UNSEREM DATENSCHUTZBEAUFTRAGTEN AUFNEHMEN?**

Bei Fragen im Zusammenhang mit der Verarbeitung Ihrer personenbezogenen Daten und mit der Wahrnehmung Ihrer Rechte gemäß der DSGVO und des DSG wenden Sie sich bitte über nachfolgendes Kontaktformular an den Datenschutzbeauftragten der card complete (dieser ist ausschließlich für die card complete Service Bank AG zum Datenschutzbeauftragten bestellt).

**Bitte verwenden Sie das Kontaktformular auf <https://www.cardcomplete.com/datenschutz/kontakt>.**

Beachten Sie, dass wir dem Bankwesengesetz und somit dem strengen Bankgeheimnis unterliegen. Aus diesem Grund fordern wir bei jeder Kontaktaufnahme in Bezug auf Ihre personenbezogenen Daten zur eindeutigen Identifikation eine Ausweiskopie an.

# DATENARTEN UND -QUELLEN

## WELCHE PERSONENBEZOGENEN DATEN VERARBEITEN WIR VON IHNEN UND AUS WELCHEN QUELLEN STAMMEN DIESE DATEN?

Wir verarbeiten jene personenbezogenen Daten, die wir im Rahmen einer Geschäftsbeziehung von Ihnen, im Zuge der Transaktionsabwicklung von teilnehmenden Parteien im Zahlungsverkehr (z. B. Online-Händler bzw. Akzeptanzpartner) oder von einem von Ihnen beauftragten Vertriebspartner (z. B. Ihrer Bank) erhalten. Hierzu gehören auch Daten, die wir von Auskunftfeien, Schuldnerverzeichnissen, Business-Analyse-Anbietern (z. B. CRIF GmbH, KSV 1870 Holding AG, Bureau Van Dijk Electronic Publishing GmbH, Dow Jones News GmbH, Creditreform Wirtschaftsauskunftei Kubicki KG), von Partnerunternehmen die uns z. B. im Zuge der Reklamationsabwicklung unterstützen (z. B. Verifi, Visa oder Mastercard) oder aus öffentlich zugänglichen Quellen (z. B. Firmenbuch, Vereinsregister, Grundbuch, Medien, Sanktionslisten) zulässigerweise erhalten haben.

### Zu den personenbezogenen Daten gehören:

- Ihre Personalien (z. B. Anrede, Name, Adresse, Kontaktdaten, einschließlich E-Mailadresse und Telefonnummer, Geburtsdatum, Staatsangehörigkeit, Familienstand)
- Legitimations- und Authentifikationsdaten (z. B. Ausweisdaten, Unterschriftenprobe)

### Darüber hinaus können auch folgende Daten verarbeitet werden:

- Beim Kartenauftrag/Akzeptanzvertrag oder im Anschluss daran bekanntgegebene Angaben (z. B. Kartenprodukt, Bankverbindung)
- Angaben im Zusammenhang mit dem Finanzmarkt-Geldwäschegesetz (FM-GwG) (z. B. Informationen zu politisch exponierten Personen (PEP), überwiegende Verwendung der Karte, Online-Einkäufe von Waren und Dienstleistungen, Rechnungsadresse, Berufliche Angaben und Einkommensdaten)
- Produktspezifische Daten bei Firmenkunden (z. B. Firmenname, Rechtsform, wirtschaftliche Eigentümer, Firmenbuchnummer, Bankverbindung)
- Nutzungsdaten auf der card complete Website, im complete Control Portal und in der mobilen App (einschließlich complete Shop) oder Akzeptanzpartnerportal CAP (z. B. Zugangsdaten wie Benutzername und Passwort), Nutzungsverhalten oder Informationen aus dem elektronischen Datenverkehr, Häufigkeit, Zeitpunkt, Orte, verwendete Funktionen, Bestelldaten (Produkt, Menge, Preis) Anmeldung zu unseren Newslettern, etc.
- Daten über die Nutzung unseres digitalen Sprachassistenten (= Voicebot) bei telefonischen Anfragen auf der card complete Facebook/Instagram Fanpage (z. B. Besucheranzahl, Häufigkeit, Zeitpunkt, Orte, Zielgruppen) über Facebook Insights
- Transaktionsdaten (z. B. Zeitpunkt & Höhe des Umsatzes, Informationen zur Akzeptanzstelle)
- Datenfelder von Partnerunternehmen (z. B.: ÖAMTC Mitglieds-Nr., Miles & More Nr., Kartenschutz-Nr.)
- Daten zur Erfüllung gesetzlicher oder regulatorischer Anforderungen. (z. B. Bankkontoinformationen)

# ZWECK UND RECHTSGRUNDLAGE

## FÜR WELCHE ZWECKE VERARBEITEN WIR IHRE PERSONENBEZOGENEN DATEN UND AUF WELCHER RECHTSGRUNDLAGE BERUHEN DIESE VERARBEITUNGEN?

Sämtliche Verarbeitungen erfolgen gemäß der DSGVO und dem DSG. Wir verarbeiten Ihre personenbezogenen Daten auf Grundlage mindestens einer der im Folgenden angeführten Rechtsgrundlagen.

### ERFÜLLUNG VON VERTRAGLICHEN PFLICHTEN (ART. 6 ABS. 1 LIT B DSGVO):

Die Verarbeitung Ihrer personenbezogenen Daten ist zur Erbringung von Bankgeschäften bzw. Finanzdienstleistungen erforderlich und umfasst sämtliche im Zusammenhang mit dem Betrieb und der Verwaltung eines Finanzdienstleistungsinstituts stehende Tätigkeiten. Diese Notwendigkeit der Verarbeitung ergibt sich insbesondere für die Abwicklung von Verträgen, vorvertragliche Maßnahmen, sowie Ausführung von Aufträgen.

### Beispiele für solche Fälle sind:

- Allgemeine Abwicklung von Bankdienstleistungen, die Herausgabe und Verwaltung von Kreditkarten sowie Karten- und Akzeptanzgeschäften
- Betrieb von Zahlungsdiensten, Kundendienstleistungen, Kundenservice (z. B. Notfallmeldungen bzgl. Kartenverlusten, Eilüberweisungen, Bearbeitung von Umsatzreklamationen)
- Bearbeitung von Kundenanfragen
- Provisionsberechnung
- Laufende Aktualisierung der Kundenstammdaten
- Konsultation von Auskunftfeien zur Ermittlung von Bonitäts- bzw. Ausfallrisiken (z. B. KSV 1980, CRIF GmbH)
- Betreuung, Beratung und Servicierung durch das Akzeptanzpartner Service Back Office
- Betreuung, Beratung und Servicierung am Geschäftsstandort durch berechnigte Repräsentanten
- Schriftverkehr, Rechnungsstellung & Entgeltberechnung im Akzeptanzbereich

## **ERFÜLLUNG RECHTLICHER VERPFLICHTUNGEN (ART. 6 ABS. 1 LIT C DSGVO):**

Die Verarbeitung Ihrer personenbezogenen Daten kann ebenso zum Zweck der Erfüllung unterschiedlicher gesetzlicher Verpflichtungen, denen die card complete als Finanzdienstleistungsunternehmen unterliegt, erforderlich sein. Verpflichtungen können sich etwa aus dem Bankwesengesetz oder dem Finanzmarkt-Geldwäschegesetz ergeben, aber auch aus aufsichtsrechtlichen Vorgaben.

### **Beispiele für solche Fälle sind:**

- Kontrolle zur Einhaltung der rechtlichen Rahmenbedingungen
- Rechtliche Verpflichtungen bei der Abwicklung von sicheren Online-Zahlungen (Starke Kundenauthentifizierung)
- Monitoring von Kartentransaktionen zur Identifikation potenzieller Geldwäschetätigkeiten und Erfüllung gesetzlicher Auflagen (z. B. FM-GwG oder EU-Zahlungsdiensterichtlinie (PSD II))
- Meldung an die Geldwäschemeldestelle in bestimmten Verdachtsfällen
- Auskunftserteilung an die FMA
- Auskunftserteilung an Finanzstrafbehörden im Rahmen eines Finanzstrafverfahrens
- Datenübermittlung an die Staatsanwaltschaft gem. behördlicher Anforderungen
- Aktenverwaltung und Verfahrensführung aufgrund datenschutzrechtlicher Verpflichtungen

## **WAHRUNG BERECHTIGTER INTERESSEN (ART. 6 ABS. 1 LIT F DSGVO):**

Sollte es zur Wahrung berechtigter Interessen der card complete oder eines Dritten notwendig sein, dass Ihre Daten über die Erfüllung des Vertrages hinaus bearbeitet werden, so erfolgt in folgenden Fällen eine Datenverarbeitung:

### **Beispiele für solche Fälle sind:**

- Betrugsprävention (Risikominimierung von Kartenmissbrauchs- und Schadensfällen durch Monitoring von (Prepaid)Karten-Limit-Überschreitungen und Veranlassung entsprechender Kartensperren oder Identifikation und Prüfung potenziell schadhafter bzw. verdächtiger Umsätze)
- Marktforschung, davon umfasst sind Maßnahmen zur Geschäftssteuerung und Weiterentwicklung von Dienstleistungen und Produkten (Nutzung bestehender Daten zur Entwicklung und zum Testen neuer Services)
- Gewährleistung der Netz- und Informationssicherheit (z. B. technische Maßnahmen, wie Google reCaptcha in complete Control, als auch Maßnahmen zum Schutz von Mitarbeitern, Kunden und des Eigentums durch Videoüberwachung innerhalb der card complete Räumlichkeiten und externer Rechenzentren zum Zweck des Eigentumsschutzes)
- Bearbeitung etwaiger Anfragen von Behörden, Rechtsanwälten, Inkassobüros o. Ä. im Zuge der Rechtsverfolgung und Durchsetzung von Rechtsansprüchen
- Abwicklung von allgemeinen telefonischen, schriftlichen oder elektronischen Kundenanfragen (inklusive digitaler Sprachassistent = Voicebot) sowie aktive Kontaktaufnahme über die hinterlegten Kontaktdaten zur Abwicklung von Geschäftsfällen
- Überprüfung qualifizierter elektronischer Signaturen via Signaturprüfungsdienst
- Statistische Erhebungen und Marktforschung über die Facebook/Instagram Fanpage und andere ähnliche Plattformen
- Direktwerbung (zielgerichtete Versendung von Gutscheinen sowie Versand des complete Magazins inklusive werblicher Beilagen per Post durch die card complete und ihre Partnerunternehmen)

## **IM RAHMEN IHRER EINWILLIGUNG (ART. 6 ABS. 1 LIT A DSGVO):**

Wenn Sie uns eine Einwilligung zur Verarbeitung Ihrer personenbezogenen Daten erteilt haben, erfolgt eine Verarbeitung nur gemäß der in der Einwilligungserklärung festgelegten Zwecke und im darin vereinbarten Umfang. Sie besitzen jederzeit das Recht eine erteilte Einwilligung ohne Angabe von Gründen und mit Wirkung für die Zukunft gänzlich zu widerrufen, wenn Sie mit einer Verarbeitung nicht mehr einverstanden sind.

### **Dies gilt beispielsweise für:**

- Verarbeitung personenbezogener Daten für Marketing- und Werbezwecke (z. B. Profiling)
- Durchführung von personenbezogenen Kundenzufriedenheitserhebungen & Marktforschung
- Versand des Newsletters und werbliche Mitteilungen
- Durchführung von Gewinnspielen und ggfs. Datenübermittlung an Gewinnspielpartner
- Video Identifikation (im Zuge der Eröffnung einer Kreditkarte, sofern diese Bestellstrecke ausgewählt wurde. Nähere Informationen im Punkt „Video ID“)
- Zum Betrieb des complete Shops (unser Auftragsverarbeiter Connex Marketing GmbH, Dr. Schauer-Str.26, 4600 Wels, Österreich, wird einige personenbezogene Daten verarbeiten).

## **VERARBEITUNG IM ÖFFENTLICHEN INTERESSE (ART 6 ABS 1 LIT E DSGVO):**

Die Verarbeitung Ihrer personenbezogenen Daten kann ebenso eine Angelegenheit des öffentlichen Interesses sein. Beispielsweise handelt es sich bei der Verarbeitung Ihrer personenbezogenen Daten nach dem FM-GwG zu Zwecken der Verhinderung von Geldwäsche und Terrorismusfinanzierung auch um eine Angelegenheit des öffentlichen Interesses (§ 21 Abs 6 FM-GwG).

## **DATENWEITERGABE**

### **WER ERHÄLT IHRE PERSONENBEZOGENEN DATEN?**

Innerhalb der card complete erhalten jene Stellen bzw. Mitarbeiter Ihre Daten, die diese zur Erfüllung der Aufgaben benötigen. Darüber hinaus erhalten von uns beauftragte Auftragsverarbeiter (z. B. Versand-Unternehmen, IT- sowie Backoffice-Dienstleister), Partnerunternehmen (wie z. B. Ihre zuständige Bank, Versicherungen oder Beratungsfirmen) und Parteien im Zahlungsverkehr (z. B. Akzeptanzpartner oder Payment Service Provider) Ihre Daten, zweckgebunden in eingeschränktem Umfang. Sämtliche Empfänger sind vertraglich und/oder gesetzlich dazu verpflichtet Ihre Daten vertraulich zu behandeln, diese nur im Rahmen der Leistungserbringung zu verarbeiten und für Datensicherheit zu sorgen.

Liegt eine gesetzliche Verpflichtung vor, können öffentliche Stellen und Institutionen (z. B. Österreichische Finanzmarktaufsicht, Finanzbehörden, etc.) sowie unsere Eigentümer personenbezogene Daten einsehen. Auf die Grundsätze der Datenminimierung und Zweckbindung wird stets besonderer Wert gelegt.

### **HINWEIS AUF DAS BANKGEHEIMNIS**

card complete ist als österreichisches Kreditinstitut zur Einhaltung des Bankgeheimnisses gemäß § 38 BWG und somit zur Verschwiegenheit bezüglich sämtlicher kundenbezogener Informationen und Tatsachen verpflichtet, die im Zuge der Geschäftsbeziehung anvertraut oder zugänglich gemacht wurden. card complete darf Ihre personenbezogenen Daten nur dann an Dritte weitergeben, wenn Ihrerseits vorab eine schriftliche und ausdrückliche Entbindungserklärung vom Bankgeheimnis erfolgte oder eine gesetzliche Verpflichtung bzw. Ermächtigung zur Weitergabe vorliegt.

Karteninhaber erteilen diese Erlaubnis im Zuge der Karteneröffnung über den Kartenauftrag, Akzeptanzpartner über den Akzeptanzvertrag. In diesem Zusammenhang können andere Kredit- und Finanzinstitute, internationale Kreditkartenorganisationen oder vergleichbare Einrichtungen (je nach Vertrag z. B. Tochterunternehmen der card complete, Partnerunternehmen (Partnerbanken, Vertriebspartner, Kooperationspartner oder Versicherungen) Empfänger Ihrer personenbezogenen Daten sein. Hinsichtlich Partnerbanken weisen wir darauf hin, dass diese für den Zweck des Vertriebs der card complete Zahlungskarten als datenschutzrechtlicher Auftragsverarbeiter agieren.

## **INTERNATIONALER DATENVERKEHR**

### **WIE FUNKTIONIERT DAS INTERNATIONALE KREDITKARTENGESCHÄFT?**

Das Kreditkartengeschäft der internationalen Kreditkartenorganisation beruht auf einem Mehrparteiensystem. Je nach Umfang der Lizenz ist der Lizenznehmer der Kartenorganisation (z. B. Visa oder Mastercard) einerseits berechtigt Kreditkarten an Kartenantragsteller auszugeben („Issuing“) und andererseits Unternehmen, die Kreditkarten als Zahlungsart akzeptieren, anzuwerben und zu betreuen („Acquiring“). Soweit es für die Abwicklung der Geschäftsverbindung erforderlich ist, findet ein entsprechender Datenfluss mit den Beteiligten statt.

Im Zusammenhang mit der Benutzung einer Karte können z. B. spezielle Reklamationsfälle bei einem Akzeptanzpartner auftreten (Vor-Ort oder im E-Commerce). In solchen Spezialfällen werden dafür benötigte Informationen mit den internationalen Kreditkartenorganisationen ausgetauscht und somit außerhalb der EU bzw. des EWR von den dahinterstehenden Lizenznehmern sowie den betroffenen Akzeptanzstellen verarbeitet. Die vertraglich vereinbarte Leistung setzt je nach in Anspruch genommenem Produkt, auch die Übermittlung personenbezogener Daten in diese Länder voraus.

Auch Auftragsverarbeiter, die IT-Leistungen für die card complete erbringen, können sich in Drittländern befinden.

# DATENÜBERMITTLUNG IN DRITTLÄNDER DURCH CARD COMPLETE:

INT. ORGANISATION	DRITTLAND RECHTSGRUNDLAGE	WEITERE DATENSCHUTZ-INFORMATIONEN
<b>Visa International</b> Visa Europe (UK) Visa Austria (AT)	<b>USA</b> Standardvertragsklauseln Art. 46 Abs. 2 lit c DSGVO	<a href="#"><u>Visa International Privacy Policy</u></a> <a href="#"><u>Visa Europe Privacy Policy</u></a>
<b>Mastercard International Incorporated</b> Mastercard Europe SA (BE) Mastercard Österreich (AT)	<b>USA</b> Bindung Corporate Rules Art. 47 DSGVO	<a href="#"><u>Mastercard Global Privacy Policy</u></a>
<b>JCB International Co. Ltd</b> JCB International (Europe) Ltd (UK)	<b>Japan</b> Angemessenheitsbeschluss Art. 45 Abs. 1 DSGVO	<a href="#"><u>JCB Global Privacy Policy</u></a> <a href="#"><u>JCB Europe Privacy Policy</u></a> <a href="#"><u>Angemessenheitsbeschluss</u></a>
<b>China Union Pay Co. Ltd</b> betrifft ausschließlich teilnehmende Akzeptanzpartner (Akzeptanzpartner im Acquiring)	<b>China</b> Standardvertragsklauseln Art. 46 Abs. 2 lit c DSGVO	<a href="#"><u>Unionpay Privacy Statement</u></a>
<b>Alipay.com Co., Ltd.</b> betrifft ausschließlich teilnehmende Akzeptanzpartner (Akzeptanzpartner im Acquiring)	<b>China</b> Standardvertragsklauseln Art. 46 Abs. 2 lit c DSGVO	<a href="#"><u>Alipay Privacy Statement</u></a>
<b>Netcetera AG</b> Abwicklung von complete Secure (sicheres Bezahlen im Internet)	<b>Schweiz</b> Angemessenheitsbeschluss Art. 45 Abs. 1 DSGVO	<a href="#"><u>Angemessenheitsbeschluss</u></a>
<b>Opentech Payment Services AG</b> Betreuung von complete Control (Portal und App)	<b>Schweiz</b> Angemessenheitsbeschluss Art. 45 Abs. 1 DSGVO	<a href="#"><u>Angemessenheitsbeschluss</u></a>
<b>Facebook Inc.</b> Facebook Ireland Limited (IE)	<b>USA</b> Standardvertragsklauseln Art. 46 Abs. 2 lit c DSGVO	<a href="#"><u>Facebook Privacy Statement</u></a>
<b>DFS Services LLC</b> Nur für Diners Club Produkte	<b>USA</b> Vertragserfüllung gemäß Art. 49 Abs. 1 lit b DSGVO	<a href="#"><u>Discover Privacy Policy</u></a>
<b>Diners Club International LTD</b> Nur für Diners Club Produkte	<b>USA</b> Vertragserfüllung gemäß Art. 49 Abs. 1 lit b DSGVO	<a href="#"><u>Diners Club Privacy Policy</u></a>
<b>Pulse Network LLC</b> Nur für Diners Club Produkte	<b>USA</b> Vertragserfüllung gemäß Art. 49 Abs. 1 lit b DSGVO	<a href="#"><u>Pulse Privacy Policy</u></a>

## DAUER DER DATENSPEICHERUNG UND DER DATENVERARBEITUNG

### WIE LANGE WERDEN IHRE PERSONENBEZOGENEN DATEN GESPEICHERT UND VERARBEITET?

Wir speichern Ihre personenbezogenen Daten, soweit erforderlich, für die Dauer der gesamten Geschäftsbeziehung, von der Anbahnung und Abwicklung bis zur Beendigung eines einzelnen oder mehrerer Verträge sowie darüber hinaus, gemäß den gesetzlichen Aufbewahrungs- und Dokumentationspflichten bzw. zur Verteidigung von Rechtsansprüchen. Die Aufbewahrungsdauer ergibt sich somit aus den unterschiedlichen gesetzlichen Aufbewahrungsfristen bzw. aus Verjährungsfristen, z. B. gem. FM-GwG 10 Jahre, gem. Unternehmensgesetzbuch (UGB) und Bundesabgabenordnung (BAO) 7 Jahre, gem. Gleichbehandlungsgesetz (GIBG) 7 Monate und in bestimmten Fällen zwischen 3 und 30 Jahre nach dem Allgemeinen Bürgerlichen Gesetzbuch (ABGB), etc.



# VERPFLICHTUNG ZUR BEREITSTELLUNG VON PERSONENBEZOGENEN DATEN

## **SIND SIE ZUR BEREITSTELLUNG VON PERSONENBEZOGENEN DATEN VERPFLICHTET?**

Es ist erforderlich, dass Sie uns jene personenbezogenen Daten zur Verfügung stellen, die für die Aufnahme und Durchführung unserer Geschäftsbeziehung notwendig sind und zu deren Erhebung wir gesetzlich verpflichtet sind. Möchten Sie diese Daten nicht bereitstellen, sind wir in der Regel gezwungen den Abschluss des Vertrages oder die Ausführung des Auftrags abzulehnen. Einen bestehenden Vertrag können wir in diesem Fall nicht mehr aufrechterhalten und müssten diesen folglich beenden. Es besteht allerdings keine Verpflichtung eine Einwilligung zu einer Datenverarbeitung zu erteilen, welche für die Vertragserfüllung nicht relevant ist.

# AUTOMATISIERTE ENTSCHEIDUNGSFINDUNG INKL. PROFILING

## **GIBT ES EINE AUTOMATISIERTE ENTSCHEIDUNGSFINDUNG INKL. PROFILING?**

card complete nutzt keine ausschließlich automatisierten Entscheidungsfindungen nach Art. 22 Abs. 1 DSGVO. Weder zur Herbeiführung einer Entscheidung noch für die Begründung und Durchführung einer Geschäftsbeziehung kommen ausschließlich automatisierte Entscheidungen zum Einsatz. Nachfolgend werden Verfahren aufgelistet, bei denen Algorithmen eine zentrale Rolle spielen.

## **MISSBRAUCHSPRÄVENTION**

Aufgrund rechtlicher Anforderungen, unter anderem aus der PSD II ist card complete zur Missbrauchsprävention („Fraud Prevention“) verpflichtet. Dazu wird jede Kartentransaktion am Point-of-Sale (Einzelhandel) oder im E-Commerce (Onlineshop) überprüft. In diesem „Transaktionsüberwachungssystem“ werden spezifische personenbezogene Daten herangezogen um anhand von vordefinierten Regeln zu bestimmen, ob eine Transaktion zulässig ist, ob potenzielle betrügerische Handlungen versucht werden und ob Transaktionen deshalb abgelehnt werden müssen und Kreditkarten präventiv gesperrt werden müssen.

## **BONITÄTSPRÜFUNG & RATINGKLASSE**

Eine Bonitätsprüfung muss durchgeführt werden, um unsere vertragliche Verpflichtung Ihnen gegenüber, z. B. bei der Abwicklung von neuen Kartenaufträgen, erfüllen zu können und um unsere rechtlichen Anforderungen aus dem Bankwesengesetz (BWG) sowie Finanzmarkt-Geldwäschegesetz (FM-GwG) einhalten zu können. Im Rahmen dieser Bonitätseinschätzungen werden interne und externe Informationen herangezogen, um jeweils einen individuellen Bonitätsscore als Grundlage zur Einschätzung des Zahlungsausfallsrisikos zu ermitteln. Während die internen Daten Informationen zur Geschäftsbeziehung betreffen, wie das Umsatz- und Zahlungsverhalten (sofern vorhanden), werden als externe Informationsquellen die von Kunden zur Verfügung gestellten Einkommensnachweise sowie Abfragen von der KSV 1870 „Konsumentenkreditevidenz“ oder der Wirtschaftsauskunftei CRIF GmbH im „Credit Check Consumer“ herangezogen. Wir weisen an dieser Stelle darauf hin, dass keine Meldung der card complete an diese Auskunftsteien erfolgt, sondern lediglich Abfragen durchgeführt werden. Um den Ursprung der Daten bei den genannten Auskunftsteien zu erfragen, wenden Sie sich bitte direkt an diese da jede dieser Parteien als eigenständiger Verantwortlicher im Sinne der DSGVO auftritt.

Es wird darauf hingewiesen, dass keine ausschließlich automatische Auswertung von persönlichem Nutzerverhalten (Profiling) stattfindet. Weiter wird keine automatisierte Entscheidung getroffen, da jede individuelle Berechnung final durch einen Mitarbeiter geprüft und behandelt wird. Da der Grad der Berücksichtigung der einzelnen Informationen auf einem internen Algorithmus basiert, welcher als Geschäftsgeheimnis einzustufen ist, kann über die Auswirkung einzelner Informationen auf den ermittelten Bonitätsscore selbst dann keine Auskunft gegeben werden, wenn Sie Ihr Recht auf Auskunft gemäß Artikel 15 DSGVO in Anspruch nehmen. Dieses Vorgehen entspricht dem österreichischen Datenschutzgesetz (§ 4 Abs. 6).

## **IDENTIFIKATION POTENZIELLER GELDWÄSCHETÄTIGKEITEN**

Aufgrund von Sorgfaltspflichten aus dem Finanzmarkt-Geldwäschegesetz (FM-GwG) ist card complete gesetzlich zur Geldwäsche- und Terrorismusbekämpfung verpflichtet.

# DER CARD COMPLETE SOCIAL MEDIA AUFTRITT

## SOCIAL MEDIA SEITEN-INSIGHTS

Bei unserem Social Media Auftritt auf Facebook (<https://www.facebook.com/cardcomplete>) und Instagram (<https://www.instagram.com/card.complete>) sind card complete und Facebook Inc. gemeinsame Verantwortliche für die Verarbeitung personenbezogener Daten, wie z. B. für statistische Auswertungen („Seiten-Insights“) und bei Inhalten von Nutzerkommentaren und Privatnachrichten (z. B. zur Abwicklung von Kundenanfragen). Eine Vereinbarung nach Art. 26 Abs. 1 DSGVO ist hier abrufbar [https://www.facebook.com/legal/terms/page\\_controller\\_addendum](https://www.facebook.com/legal/terms/page_controller_addendum). Betroffenenanfragen können direkt bei Facebook oder mittels Kontaktaufnahme mit card complete z. B. über die Kontaktkanäle von Facebook oder über das card complete Kontaktformular gestellt werden. card complete betreibt in erster Linie die so genannten „Fanpages“ in sozialen Medien, daher haben wir nur einen begrenzten Einfluss auf deren Datenschutzaspekte.

## SOCIAL MEDIA GEWINNSPIELE

Alle Informationen zu Gewinnspielen in Social Media Auftritten finden Sie hier:  
<https://www.cardcomplete.com/social-media/>

# DATENSICHERHEIT

## WIE ERFOLGT DIE SICHERUNG IHRER DATEN?

Während im Mittelpunkt der Betrachtung des Datenschutzes personenbezogene Daten liegen, umfasst die Datensicherheit alle Daten, unabhängig davon ob sie einen Personenbezug aufweisen oder nicht.

Datensicherheit verfolgt einen praktischen Ansatz, weg von der Beschränkung im Hinblick auf die Art der Daten, hin zur Definition und Umsetzung von Maßnahmen welche zum Schutz der Daten und Erfüllung der datenschutzrechtlichen Schutzziele Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit umgesetzt werden müssen.

Kernpunkt der Datensicherheit sind so genannte technische und organisatorische Maßnahmen, die den Schutz der Daten vor Missbrauch, Verlust, Verfälschung und unberechtigtem Zugriff gewährleisten. card complete trifft umfangreiche technische und organisatorische Sicherheitsvorkehrungen, die den höchsten internationalen Sicherheitsstandards entsprechen, um Ihren Daten den bestmöglichen Schutz zu bieten.

Die getroffenen technischen und organisatorischen Maßnahmen werden regelmäßig in Bezug auf deren Wirksamkeit und Eignung, die gewünschten Schutzziele zu erreichen, überprüft. Darüber hinaus stellt die card complete durch den Betrieb eines Datenschutz Managementsystems einen kontinuierlichen Verbesserungsprozess sicher.

### Beispiele für unsere technischen und organisatorischen Maßnahmen sind:

- Verschlüsselung
- Pseudonymisierung
- Zutritts-, Zugangs-, Zugriffs- und Weitergabekontrolle
- Verfügbarkeitskontrolle
- Rasche Wiederherstellbarkeit
- Datenschutzfreundliche Voreinstellungen
- Incident-Response-Management

## WIE SICHER IST DIE TRANSAKTIONSABWICKLUNG AN EINEM BEZAHL-TERMINAL?

card complete ermöglicht dem Kunden (Inhaber einer Zahlungskarte), bei einem Akzeptanzpartner durch das Vorweisen von Zahlungskarten am Geschäftsstandort mittels Bezahl-Terminal (vor Ort-Geschäft) (oder mittels Fernabsatz im Internet (E-Commerce/Online Handel)) bzw. mittels telefonischer oder schriftlicher Bestellung (MailOrder/TelefonOrder) auf sichere Weise bargeldlos zu bezahlen.

Die sichere Transaktionsabwicklung wird garantiert, indem Nachrichten innerhalb des Terminalnetzes netzwerktechnisch verschlüsselt und innerhalb eines sogenannten „Tunnels“ proprietär abgesichert werden. Fälschungen, Verfälschungen und das Wiedereinspielen von Nachrichten sind dadurch ausgeschlossen. Weiters ist der PIN-Block einer Zahlungskarte auf diesem Weg zusätzlich verschlüsselt.

## WIE SICHER IST DIE TRANSAKTIONSABWICKLUNG IM ONLINE HANDEL?

Für die Zahlungsabwicklung im E-Commerce bedienen sich die Online Shop Betreiber meistens externer Payment Service Provider, die geeignete technische Schutzmaßnahmen aufweisen, um die Datensicherheit zu gewährleisten. Für Anfragen bezüglich der Online Transaktionsabwicklung bitten wir Sie als primäre Kontaktstelle den Betreiber des genutzten Online Shops zu kontaktieren.

## COMPLETE SECURE FÜR INTERNETZAHLUNGEN

Alle Parteien im Online-Zahlungsverkehr unterliegen den gesetzlichen Auflagen aus der PSD II. Die Umsetzung der Neufassung der PSD II durch technische Maßnahmen, wie die „starke Kundenauthentifizierung“ oder die „risikobasierte Transaktionsabwicklung“, soll vorrangig in Ihrem eigenen Interesse garantieren, dass jede Online-Zahlung so sicher wie möglich durchgeführt wird.

Zur technischen Umsetzung der starken Kundenauthentifizierung, kommt das sogenannte „3D-Secure Verfahren“, auch „complete Secure“ genannt, zum Einsatz.

Internetzahlungen müssen sowohl mit Ihrem Secure Code (Ihr persönliches Passwort – das nicht mit dem vierstelligen Karten-PIN und auch nicht mit anderen Login-Daten verwechselt werden darf), als auch mit einem zusätzlichen „Faktor“ z. B. einer mobile TAN, die als SMS auf Ihre hinterlegte Mobilnummer geschickt wird, bestätigt werden. Bitte beachten Sie, dass die card complete Ihre für complete Secure registrierte Mobiltelefonnummer außerdem verwenden kann, um Sie in speziellen Anlässen im Zuge der Geschäftsabwicklung aktiv zu kontaktieren. Nähere Informationen zu complete Secure finden Sie auf <https://www.cardcomplete.com/sicherheit/complete-secure/>.

## RISIKOBASIERTE AUTHENTIFIZIERUNG

Aufgrund der PSD II müssen auch Authentifizierungsanfragen an ein sogenanntes „Risiko-Tool“ weitergeleitet werden. Dort findet, basierend auf einem vordefinierten Regelwerk, eine Risikoklassifizierung der durchgeführten Transaktion anhand verschiedener personenbezogener & anonymer Daten statt. Das Ergebnis dieser Klassifizierung hält fest, ob eine starke Kundenauthentifizierung gefordert ist oder nicht, bzw. ob eine Transaktion aus Sicherheitsgründen abgelehnt werden muss. card complete setzt für die Abwicklung dieser Prozesse einen gem. Art. 28 DSGVO vertraglich gebundenen Auftragsverarbeiter (Firma Netcetera AG) ein.

## WIE SICHER WERDEN PASSWÖRTER VERARBEITET?

In Portalen der card complete wie z. B. auf <https://customerportal.cardcomplete.com/> werden Ihre Daten sorgfältig nach den aktuellen Standards abgesichert. Alle Passwörter werden verschlüsselt abgespeichert.

# COMPLETE CONTROL BENUTZER-PORTAL / COMPLETE CONTROL IOS & ANDROID APP

## DATENSCHUTZ IM SELF-SERVICE PORTAL

Die personenbezogenen Daten im complete Control Benutzer-Portal <https://customerportal.cardcomplete.com/> bzw. in der complete Control iOS/Android App werden durch einen, gemäß Art. 28 DSGVO vertraglich gebundenen, Auftragsverarbeiter (Firma Opentech Payment Services AG) verarbeitet. In diesem Self-Service Portal können Sie unter anderem Ihre Kreditkarten hinzufügen, Ihre letzten Umsätze prüfen, Ihre Stammdaten bzw. Adressdaten ändern oder auch Geoblocking-Einstellungen vornehmen. Ihre bei card complete hinterlegte oder bekannt gegebene E-Mail-Adresse dient als Benutzername für den Login. Höchste Sicherheit wird durch die starke Kundenauthentifizierung gem. PSD II gewährleistet, die in Portal und App zur Anwendung kommt. Abgewickelt wird dies mittels Zusendung eines mobile TAN per SMS auf die Mobiltelefonnummer, welche Sie bei card complete bekannt gegeben haben. Verwenden Sie die complete Control iOS/Android App, kann der SMS Versand durch biometrische Funktionen (z. B. Face-ID oder Touch-ID) ersetzt werden, sofern Sie dies wünschen.

## NÄHERES ZU BIOMETRISCHEN DATEN AM BEISPIEL DER COMPLETE CONTROL IOS APP

card complete verarbeitet in der complete Control iOS App keine biometrischen Daten bei der technischen Abwicklung der Face-ID oder Touch-ID. Informationen zu Datenschutz & Sicherheit zu Touch-ID finden Sie auf <https://support.apple.com/de-de/HT204587> und zu Face-ID auf <https://support.apple.com/de-at/HT208108>.

## GOOGLE RECAPTCHA FÜR COMPLETE CONTROL

complete Control nutzt Funktionen des Dienstes „Google reCAPTCHA“. Anbieter ist die Google Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA.

reCAPTCHA ist ein freier Captcha-Dienst von Google, der Websites vor Spam-Software und den Missbrauch durch nicht-menschliche Besucher schützt. Mit reCAPTCHA soll überprüft werden, ob die Dateneingabe auf complete Control (z. B. in einem Kontaktformular) durch einen Menschen oder durch ein automatisiertes Programm (Roboter) erfolgt. Hierzu analysiert reCAPTCHA das Verhalten des Benutzers der Website anhand verschiedener Merkmale. Diese Analyse beginnt automatisch, sobald sich der Benutzer auf der Website befindet. Zur Analyse wertet reCAPTCHA verschiedene Informationen aus:



- Referrer URL (die Adresse der Seite von der der Besucher kommt)
- IP-Adresse (z. B. 256.123.123.1)
- Infos über das Betriebssystem (die Software, die den Betrieb Ihres Computers ermöglicht. Bekannte Betriebssysteme sind Windows, Mac OS X oder Linux)
- Cookies (kleine Textdateien, die Daten in Ihrem Browser speichern)
- Maus- und Keyboardverhalten (jede Aktion, die Sie mit der Maus oder der Tastatur ausführen wird gespeichert)
- Datum und Spracheinstellungen (welche Sprache bzw. welches Datum Sie auf Ihrem PC voreingestellt haben wird gespeichert)
- Alle JavaScript-Objekte (JavaScript ist eine Programmiersprache, die Webseiten ermöglicht, sich an den User anzupassen. JavaScript-Objekte können alle möglichen Daten unter einem Namen sammeln)
- Bildschirmauflösung (zeigt an aus wie vielen Pixeln die Bildarstellung besteht)

Die bei dieser Analyse erfassten Daten werden an Google weitergeleitet. Die reCAPTCHA-Analysen laufen vollständig im Hintergrund. Die Benutzer der Website werden nicht darauf hingewiesen, dass eine Analyse stattfindet. Die Datenverarbeitung erfolgt auf Grundlage von Art. 6 Abs. 1 lit. f DSGVO. card complete hat ein berechtigtes Interesse daran, seine Webangebote vor missbräuchlicher automatisierter Ausspähung und vor SPAM zu schützen.

Weitere Informationen zu Google reCAPTCHA sowie die Datenschutzerklärung von Google entnehmen Sie folgenden Links: <https://www.google.com/intl/de/policies/privacy/> und <https://www.google.com/recaptcha/intro/android.html>

## VIDEO-IDENT-VERFAHREN (VIDEO-ID) & ELEKTRONISCHER SIGNATUR

Bei der Beauftragung einer card complete Zahlungskarte haben Sie die Möglichkeit Ihre jederzeit widerrufbare Einwilligung in das Video-Ident-Verfahren („Video-ID“) abzugeben und den Kartenauftrag, anstelle einer klassischen Unterschrift, mit einer qualifizierten elektronischen Signatur („QES“) rechtskonform und medienbruchfrei zu unterzeichnen. Die dafür notwendigen Daten befüllen Sie in der Web-Anwendung, dem sogenannten „Bestell-assistenten“.

Es wird eine eindeutige Vorgangsnummer generiert mit der Sie, bei dem gem. Art. 28 DSGVO vertraglich gebundenen Auftragsverarbeiter der Firma CRIF GmbH, über die Anwendung „CRIF Video Identifikation“ per Video-Call, durch zertifizierte und geschulte Call-Center-Agents identifiziert werden. Die Anwendung basiert auf dem Produkt der WebID Solutions GmbH und WebID Austria GmbH als Softwarehersteller und Plattformbetreiber und wurde entsprechend den Anforderungen der Online-Identifikationsverordnung (Online-IDV) entwickelt.

Durch einen technischen „pre-check“ wird überprüft, ob die Netzwerkqualität und andere technische Leistungsdaten des verwendeten Endgerätes für den Video-ID Prozess genügen. Während des Identifikationsverfahrens werden Sie und Ihr Ausweisdokument fotografiert und in einem ausführlichen Prozessablauf auf Betrugsverdacht geprüft. Die Tonspur des gesamten Gesprächs wird nach Ihrer Einwilligung aufgezeichnet. Eine Videoaufzeichnung findet nicht statt. Bei erfolgreicher Identifikation wird Ihnen via SMS/E-Mail ein Bestätigungs-Code zugesandt.

Bei card complete sowie unseren Partnern kommen nur Produkte und Services zum Einsatz, die den höchsten technischen Sicherheitsanforderungen entsprechen. Der Video-Call erfolgt über ein regelmäßig überprüftes, hochsicheres Callcenter und durch speziell geschulte Servicemitarbeiter.

Sollten Sie eine qualifizierte elektronische Signatur statt einer klassischen Unterschrift auf dem Vertragsdokument abgeben wollen, werden Sie nach Ihrer Einwilligung zu einem eigenständigen Verantwortlichen im Sinne der DSGVO, einem qualifizierten Vertrauensdiensteanbieter, weitergeleitet. Dieses Verfahren entspricht den Anforderungen des Signatur- und Vertrauensdienstegesetzes (SVG).

Die aktuelle Liste der Vertrauensdiensteanbieter ist hier ersichtlich <https://www.signatur.rtr.at/de/vd/Anbieter.html>.

# DAS COMPLETE PCI DSS PORTAL FÜR AKZEPTANZPARTNER

Der Payment Card Industry Data Security Standard (PCI-DSS) regelt den Umgang mit zahlungsrelevanten Daten im Präsenzgeschäft (Vor-Ort) und im Fernabsatz (E-Commerce), um etwaigen Missbrauch zu verhindern. Der Nachweis der PCI-DSS-Compliance durch den Akzeptanzpartner ist, wie im Akzeptanzvertrag festgehalten, zur Vertragserfüllung erforderlich (Art. 6 Abs. 1 lit b DSGVO).

Ein gemäß Art. 28 DSGVO vertraglich gebundener Auftragsverarbeiter (Firma und AG) ist durch card complete mit der Verarbeitung personenbezogener Daten von Akzeptanzpartnern beauftragt. Auf der Webseite <https://pci.cardcomplete.com> können Sie sich in einem geschützten Login-Bereich mit Ihrem zugewiesenen Akzeptanzpartnerprofil und Ihren spezifischen Benutzerdaten einloggen. Die Daten in Ihrem Profil werden zum Nachweis Ihrer PCI-Compliance gegenüber den Kartenorganisationen verarbeitet.

**In einem solchen Profil können folgende Angaben gespeichert oder abgerufen werden, die nicht zwingend personenbezogen sein müssen:**

- Akzeptanzpartnerstammdaten (Bspw. Firmenname)
- Name und Kontaktdaten (Adresse, E-Mail, Telefonnummer) des Ansprechpartners
- Dokumente zum Nachweis der PCI-Compliance und zur Akzeptanzpartnerkommunikation
- Anonymisierte Informationen über die Anzahl der durchgeführten Transaktionen
- Technische Informationen über Terminals und/oder den Payment-Service-Provider Partner

## DIGITALER SPRACHASSISTENT (= VOICEBOT)

Wenn Sie bei unserem Kundenservice anrufen, setzen wir gegebenenfalls einen digitalen Sprachassistenten (= Voicebot) ein, der als Computersystem in Echtzeit arbeitet und allgemeine Anfragen über die Telefonie entgegennimmt, analysiert und in natürlicher Sprache beantwortet, ähnlich wie mit einem Menschen. Die Angabe und Verarbeitung personenbezogener Daten ist für die Nutzung des Voicebot nicht notwendig und nicht erforderlich.

Der Betreiber des Voicebot (CallOne GmbH, Hugo-Vogel-Straße 23, 14109 Berlin, <https://www.callone.de>) speichert keine Daten außerhalb der EU, sondern in einem datenschutz-konformen Datenzentrum innerhalb der EU.

Dabei handelt es sich um folgende Angaben:

- Datum und Uhrzeit des Anrufs
- Vollständiger in Text umgewandelter Gesprächsverlauf, den Sie mit dem Voicebot geführt haben

Der Gesprächsverlauf sowie der Nutzungszeitpunkt (Datum und Uhrzeit des Anrufs) werden auf der Voicebot-Kommunikationsplattform in unregelmäßigen Abständen, spätestens jedoch nach drei Monaten, gelöscht, wobei bei der Nutzung keine personenbezogenen Daten abgefragt werden und diese für die Nutzung des Voicebot auch nicht erforderlich sind.

Die Speicherung erfolgt im Rahmen der gesetzlichen Aufbewahrungspflichten. Wir erheben nur Daten, die für die Bereitstellung des Voicebot-Dienstes erforderlich sind.

Die Telefonnummer wird von der weiterleitenden Telekommunikationsanlage maskiert an den Voicebot weitergegeben und nicht gespeichert.

Um der Erfassung und Speicherung eindeutig personenbezogener Daten, die Sie im Gesprächsverlauf angegeben haben, zu widersprechen oder zu löschen, ist eine Kontaktaufnahme zu uns erforderlich (<https://www.cardcomplete.com/datenschutz/kontakt/>). Bitte teilen Sie uns bei der Kontaktaufnahme Ihre angegebenen personenbezogenen Daten mit, um eine anschließende Löschung vorzunehmen. Da der Voicebot die Angaben automatisch verarbeitet und keine personenbezogenen Daten abfragt, kann nur der Anrufer wissen, ob und welche personenbezogenen Daten erfasst wurden, und muss diese bei einer Kontaktaufnahme als Merkmal für die Ermittlung beistellen.

Nähere Details entnehmen Sie bitte der Datenschutzerklärung des Voicebot-Betreibers (CallOne GmbH, Hugo-Vogel-Straße 23, 14109 Berlin, <https://www.callone.de/datenschutz>).

# BETROFFENENRECHTE

## WELCHE DATENSCHUTZRECHTE STEHEN IHNEN ZU?

Folgende Rechte können Sie jederzeit als betroffene Person im Sinne des Datenschutzgesetzes durchsetzen:

- Recht auf Auskunft
- Recht auf Berichtigung
- Recht auf Löschung
- Recht auf Einschränkung
- Recht auf Datenübertragbarkeit
- Recht auf Widerspruch

## SIE WÜNSCHEN KEINE WERBLICHE VERWENDUNG IHRER DATEN MEHR?

Besuchen Sie uns auf <https://www.cardcomplete.com/datenverwendung>, um jeglicher werblichen Verwendung Ihrer Daten zu widersprechen und gegebene Einwilligungen zur werblichen Datenverwendung zu widerrufen. Sie finden darüber hinaus in jedem elektronischen Werbemittel die Möglichkeit sich von diesem abzumelden.

## SO KÖNNEN SIE KONTAKT MIT UNS AUFNEHMEN, UM IHRE RECHTE IN ANSPRUCH ZU NEHMEN.

Wenn Sie von Ihren Rechten Gebrauch machen möchten, verwenden Sie bitte das Kontaktformular auf <https://www.cardcomplete.com/datenschutz/kontakt>.

Sind Sie der Meinung, dass wir bei der Verarbeitung Ihrer Daten gegen die DSGVO oder das österreichische Datenschutzgesetz verstoßen, so ersuchen wir Sie Kontakt mit uns aufzunehmen, um Ihre Bedenken zu klären.

Etwaiße Beschwerden richten Sie bitte an die österreichische Datenschutzbehörde.

Version der Datenschutzerklärung: 01/2024