PRIVACY NOTICE

Introduction

We are pleased about your interest in data protection at card complete Service Bank AG (card complete). For us, it is a priority that you feel secure while visiting our website as well as when doing business with us.

As soon as you use the products and/or services of card complete, you entrust us with your personal information, which we process as a data controller. In this role, we take protection of your data very seriously and would therefore like to inform you about what data we require, how we process it and to whom we transfer it.

We also want you to know about how we protect your data, what rights you have in this context and to whom you can address any data protection concerns. With regard to the terms we use (“processing”, “personal data”, etc.), we refer to the definitions provided in the General Data Protection Regulations (“GDPR”) and Austrian Data Protection Act (“DPA”).

Target group

Who is affected by this privacy notice?

The privacy notice applies to the following individuals or groups:

- interested parties and customers (private and company cardholders);
- merchants;
- partner banks and distribution partners;
- visitors to our websites and individuals who sign up for our portals or apps;
- all other individuals who are in contact with card complete.

This privacy notice is also valid for KSG Karten-Versicherungs- und Servicegesellschaft m.b.H, a subsidiary of card complete, insofar as it acts as a data controller toward data subjects.

The privacy policy of DC elektronische Zahlungssysteme GmbH is available at https://www.cardcomplete.com/datenschutz/dcez/. It applies for the processing of personal data in the context of services to card complete terminals (POS terminals).

Data Controller and Data Protection Officer Contacts

Who is responsible for data processing?
Whom can you contact at card complete if you have questions about privacy?

The data controller is:
card complete Service Bank AG (card complete)
Lassallestraße 3
1020 Wien

How to contact our data protection officer

For queries on the processing of your personal data and your rights under the GDPR and DPA, you can contact card complete’s data protection officer **through the following contact form https://www.cardcomplete.com/datenschutz/kontakt**. (card complete’s data protection officer is only authorised to handle queries related to card complete.)

Please note that we are subject to the Austrian Banking Act (“BWG”) and its strict banking secrecy rules. Therefore, to process any query regarding personal data, we need to carry out an identification check by requesting a copy of a valid identity document.

Types of data and data sources

Which personal data do we process and what are the sources of the data?

We process the personal data that we receive from you in the context of a business relationship, in the course of payment transactions with other participating parties (e.g. online merchants or acceptance partners) or in the course of transactions with distribution partners instructed by you (e.g. your bank).

This also includes data which we receive from credit agencies, debtor agencies, business analysts (e.g. CRIF GmbH, KSV 1870 Holding AG, Bureau Van Dijk Electronic Publishing GmbH, Dow Jones News GmbH, Creditreform Wirtschaftsauskunftei Kubicki KG), from other companies that help us, for example, to process complaints (e.g. Verify, Visa, Mastercard, etc.), or which we obtain from publicly accessible sources (e.g. company registers, register of associations, land registry, media, sanctions lists).

The personal data includes:

– your personal details (e.g. title or form of address, name, residential address, contact information including e-mail and telephone number, date of birth, nationality, marital status);
– identification and authentication data (e.g. ID card data, specimen signature).

In addition, we may process the following data:

– information that you provide in the course of ordering a card/accepting a service contract (e.g. card product, banking details);
– information required under the Austrian Financial Market Anti-Money Laundering Act (“FM-GwG”) (e.g. information concerning politically exposed persons (PEP), main usage of the card, online purchases of goods and services, billing address, professional details, income details);
– product-specific data for corporate customers (e.g. company name, legal form, beneficial owners, commercial register number, banking details);
– data on usage of the card complete website, complete Control portal and mobile app (including the complete Shop) and merchant portal CAP (access data such as username and password), usage patterns from electronic data traffic, such as frequency, times, locations, functions used, order data (product, quantity, price), subscription to our newsletters;
– data on the usage of the card complete Facebook/Instagram Fan Page (e.g. number of visitors, frequency, times, locations, target groups) via the Facebook insights tool;
– transaction data (e.g. time, amount, point of acceptance);
– data relating to partner companies (e.g. ÖAMTC membership number, Miles & More number, Card Protection Program number);
– data for fulfilment of legal or regulatory requirements (e.g. bank account information).

Purpose and legal basis

For what purposes do we process your personal data and on what legal basis?

All data processing is carried out in accordance with the GDPR and DPA, and for one or more of the following legally defined purposes.

Fulfilment of a contractual obligation (Art. 6, Section 1 (b) GDPR):

The processing of your personal data is necessary for providing banking and financial services, and this also includes the fulfilment of various legal obligations to which the company is subject as a financial services provider. This data processing is particularly required for fulfilling contracts, implementing pre-contractual measures and executing instructions.

Examples of such activities are:

– general provision of banking services, issuing and management of credit cards as well as payment card and acceptance business;
– operation of payment services, customer services, customer support (emergency reporting of lost and stolen cards, express transfers, processing transaction complaints, etc.);
– handling of customer enquiries;
– calculation of commissions;
– continuous updating of customer data;

– consulting credit agencies (KSV 1870, CRIF GmbH, etc.) to determine credit and default risks;
– providing support to acceptance partners (merchant service back office);
– merchant service on site (POS) through authorised representatives;
– correspondence, invoicing, calculating payments and charges relating to merchant business.

Fulfilment of legal obligations (Art. 6 Section 1 (c) GDPR):

The processing of your personal data may also be necessary to fulfil various legal obligations to which card complete is subject in its role as a financial services provider. Obligations can arise from the BWG or from the FM-GwG, but also from other regulatory instruments.

Examples of such obligations are:
– verifying compliance with all applicable terms and conditions;
– complying with legal obligations for the settlement of secure online payments (strong customer authentication);
– monitoring card transactions to identify potential money laundering and to fulfil requirements under FM-GwG, Payment Service Directive II (“PSD II”), etc.;
– reporting suspicious activity to the anti-money laundering authorities;
– reporting to the Austrian Financial Market Authority (“FMA”);
– providing information in the context of investigations by the tax fraud authorities;
– providing data to the state prosecution office when legally required;
– managing files and procedures in compliance with data protection obligations.

Protection of legitimate interests (Art. 6 Section 1 (f) GDPR):

In some cases, it may be necessary to process personal data even beyond the fulfilment of a contract in order to protect the legitimate interests of the company or a third party.

Examples of such cases are:
– fraud prevention (minimising risk of loss by monitoring card limit overruns, identifying suspicious transactions and blocking cards as necessary);
– market research, which includes measures for business management and development (using existing data to develop and test new services);
– ensuring network and information security (measures to protect our employees, customers and property through video surveillance within the premises of card complete and external data centres);
– processing enquiries from authorities, lawyers, debt collection agencies or similar in the context of prosecution and enforcement of legal claims;
– handling general telephone, written or electronic customer enquiries as well as contacting customers through their details stored for the purpose of processing business transactions;
– verifying qualified electronic signatures via signature verification service providers;
– statistical surveys and market research through the Facebook/Instagram Fan Pages and similar platforms;
– direct advertising (targeted distribution of vouchers, postal delivery of the complete magazine including promotional supplements, by card complete and its partner companies).

On the basis of your consent (Art. 6 Section 1 (a) GDPR):

Any processing of your data that takes take place in accordance with your declaration of consent is done only within its defined purposes and to the agreed extent. If you decide that you no longer agree to such processing, you have the right to revoke your consent for the future at any time without giving reasons.

Your consent applies, for example, to:
– processing of personal data for certain marketing and advertising purposes (profiling);
– implementation of personal customer satisfaction surveys and market research;
– delivery of newsletters and advertising messages;
– participation in sweepstakes (prize draws, competitions, etc.) and any transfer of data to the sweepstakes sponsors;
– ideo identification in the course of making a credit card application, if you choose this type of processing. Further information is provided in the section “Video ID”.
– in order to operate the complete Shop (our processor Connex Marketing GmbH, Dr. Schauer-Str. 26, 4600 Wels, Austria, shall processes some data).

Data transfer

Who receives your personal data?

Within card complete, your data is shared with departments or employees who need it in order to perform the financial services that we provide. In addition, contractors engaged by us (e.g. delivery companies, IT and back-office system providers), partner companies (e.g. your bank, insurance companies or consultancy firms) and other parties in the payment transactions (e.g. merchant or payment service providers) receive your data to a limited extent and for specific purposes. All recipients are obligated by law and/or contract to treat your data confidentially, to process it only in the context of providing their services and to ensure due data protection.

If required by law, your data may be shared with governmental authorities and organisations (Austrian Financial Market Authority, tax authorities, etc.) as well as our owners. In such cases, the principles of data minimisation and purpose limitation are always given due consideration.

Information on banking secrecy

As an Austrian financial institution, card complete is obliged to ensure banking secrecy pursuant to Article 38 BWG and thus to treat all customer-related data and information that it acquires in the course of a business relationship as confidential. Card complete is only allowed to pass your data on to a third party if you provide in advance a written and express declaration of release from banking secrecy, or if there is a legal obligation or authorisation for disclosure.

A cardholder gives this consent in the course of completing a card application, and a merchant through the acceptance contract. In this context, other credit and financial institutions, international credit card organisations or similar institutions, e.g. card complete's subsidiaries or partner companies (partner banks, distribution partners, cooperation partners or insurance companies), depending on the contract, can be recipients of your data. With regard to partner banks, please note that they operate as data processors for the purpose of selling/distributing card complete payment cards.

International data transfers

How does the international credit card business work?

The credit card business of the international card organisations is based on a multilateral system. Depending on the scope of the licence, the licensee of a card organisation (e.g. Visa or MasterCard) may issue credit cards to card applicants ("issuing business") and, on the other hand, may recruit and service companies which accept the cards as a payment method ("acquiring business"). Insofar as it is necessary for conducting business, a flow of data takes place between the parties involved.

In connection with the use of cards, for example, special cases of complaints/disputes may arise with a merchant (either retail point of sale or e-commerce). In such cases, the information required to resolve the dispute is exchanged with the international credit card organisations and processed outside the EU/EEA by the relevant licensees and acceptance parties. Depending on the type of product involved, the contractual terms may also allow the transfer of personal data to those countries.

Moreover, data processors engaged to deliver IT services for card complete may be located in third countries.

Data transfer to third countries by card complete:

International Organisation	Third country legal basis	Further data protection Information
Visa International Visa Europe (UK) Visa Austria (AT)	**USA** Standard data protection clauses Art. 46 sect.. 2 (c) GDPR	Visa International Privacy Policy Visa Europe Privacy Policy
Mastercard International Incorporated Mastercard Europe SA (BE) Mastercard Österreich (AT)	**USA** Binding corporate rules Art. 47 GDPR	Mastercard Global Privacy Policy
JCB International Co. Ltd JCB International (Europe) Ltd (UK)	**Japan** Adequacy decision Art. 45 Section 1 GDPR	JCB Global Privacy Policy JCB Europe Privacy Policy
China Union Pay Co. Ltd only concerns participating merchants (acquiring business)	**China** Standard data protection clauses Art. 46 Section 2 (c) GDPR	UnionPay Privacy Policy
Alipay.com Co., Ltd. only concerns participating merchants (acquiring business)	**China** Standard data protection clauses Art. 46 Section 2 (c) GDPR	Alipay Privacy policy
Netcetera AG complete secure transactions (secure payment through the internet)	**Switzerland** Adequacy decision Art. 45 Section 1 GDPR	Adequacy decision
Opentech Payment Services AG support for complete Control (portal and app)	**Switzerland** Adequacy decision Art. 45 Section 1 GDPR	Adequacy decision
Facebook Inc. Facebook Ireland Limited (IE)	**USA** Standard data protection clauses Art. 46 Section 2 (c) GDPR	Facebook Privacy Statement

Duration of data retention and processing

How long is your personal data retained and processed?

We process your personal data, as necessary, for the entire duration of the business relationship, from the preparation, through the performance and up to the termination of the contract(s), and beyond, in accordance with statutory obligations for retention and documentation or for the defence of legal claims.

The retention periods thus result from the statutory obligations or from statutory limitation periods. According to the FM-GwG these terms are 10 years, according to the Austrian Companies Code (UGB) and Federal Fiscal Code (BAO) 7 years, according to the Equal Treatment Law (GlBG) 7 months, and in certain cases according to the General Civil Code (ABGB) between 3 and 30 years.

Obligation to provide personal data

Are you obliged to provide your personal data?

It is necessary that you provide us with the personal data we need in order to do business with you as well as to comply with legal requirements. As a rule, if you are not prepared to provide such data, we are not able to enter into a contract with you. Moreover, in such cases, we cannot maintain an existing contract and will consequently have to terminate it. However, you are not obliged to agree to any kind of data processing which is not relevant for the performance of the contract.

Automated decision-making, including profiling

Does card complete use automated decision-making (including profiling)?

Card complete does not rely solely on fully automated processing pursuant to Art. 22 Section 1 GDPR, neither for making decisions nor for establishing and conducting a business relationship. Below is a list of procedures, where algorithms do, however, play a central role.

Fraud prevention

According to legal requirements (including PSD II), card complete is obliged to protect its customers from fraud (“fraud prevention”). For this reason, every card transaction is verified at the point of sale (retail) or in E-Commerce (online shop). This transaction monitoring system processes specific personal data on the basis of pre-defined rules to determine whether a transaction is valid. If the system detects that a transaction is potentially fraudulent, it may be denied and the card blocked as a preventive measure.

Credit assessment and rating class

We must conduct a credit assessment in order to fulfil our contractual obligations toward you (for example, when issuing a new credit card) and to comply with our legal requirements under the BWG and the FM-GwG.

Within the framework of these credit assessments, internal and external information is used to determine an individual credit score as the basis for estimating the risk of payment default. While the internal information concerns the business relationship such as purchasing and payment behaviour (if available), external sources of information include the proof of income provided by the customer as well as queries sent to agencies such as KSV 1870 (“Consumer Credit Record”) or CRIF GmbH (“Credit Check Consumer”). Please note that card complete does not report information to these credit agencies, but only makes information requests. If you wish to know the origin of the data held by these agencies, please contact them directly, because they act as independent data controllers within the meaning of the GDPR.

Please note that no fully automated evaluation of personal user behaviour (profiling) occurs. Moreover, we do not take automated decisions; each individual calculation is ultimately examined and assessed by a (human) member of our staff. The weighting of the various factors within the credit score is based on an internal algorithm which is classified as a business secret. We therefore cannot provide information concerning the effect of particular factors for the determination of the credit score, even if you exercise your right to information under Art. 15 GDPR. This approach corresponds to the DPA (Art. 4 Section 6).

Identification of potential money laundering

Because of duties deriving from the FM-GwG, card complete is legally obliged to adopt appropriate measures to prevent money laundering and the financing of terrorism.

card complete on social media

Social media insights

For our social media presence on Facebook https://www.facebook.com/cardcomplete and Instagram https://www.instagram.com/cardcompleteservicebankag/, card complete and Facebook are joint controllers for the processing of personal data, such as statistical evaluation (Page Insights) and processing user comments and private messages (e.g. handling of customer enquiries). An agreement according to Art. 26 Section 1 GDPR is available at https://www.facebook.com/legal/terms/page_controller_addendum. Queries by persons affected can be sent directly through Facebook or through the card complete contact form. As card complete’s activities on social media consist mainly of operating Fan Pages, we have only limited influence on the data protection aspects of these media.

Social media sweepstakes, games and competitions

All information regarding sweepstakes, games, prize draws, etc. offered on social media is available at https://www.cardcomplete.com/social-media/.

Data security

How is your data secured?

While data protection rules focus mainly on personal data, data security involves all types of data, whether it contains personal references or not.

Data security takes a practical approach which is less concerned with limitations on certain types of data; it is more concerned with defining and implementing measures to safeguard all data and to fulfil the statutory data protection aims of confidentiality, availability, integrity and resilience.

The core of data security is technical and organisational measures which protect the data against misuse, loss, alteration and unauthorised access. Card complete takes extensive technical and organisational precautions, which correspond to the highest international security standards, to provide the best possible protection for your data.

These technical and organisational measures are regularly checked to ensure their effectiveness and suitability for the desired security goals. Furthermore, card complete ensures continuous improvement through the operation of a data protection management system.

Here are some examples of our technical and organisational measures:

– encryption
– pseudonymisation
– entry, access, and transmission control
– availability control
– rapid recovery
– privacy friendly default settings
– Incident response management.

How secure is a transaction at a payment terminal?

Card complete enables its customers (cardholders) to make secure cashless payments to merchants by presenting payment cards at payment terminals (on-site or point-of-sale business), on the Internet (E-commerce/online business) or by telephone or written orders (mail order/phone order).

Secure transaction processing is guaranteed by a proprietary system of data encryption and transmission via a VPN tunnel within the terminal network. This measure rules out the possibility of forgeries, falsifications and the replay of messages.

How secure is a transaction online?

For payment processing in e-commerce, online merchants usually use external payment service providers which have suitable technical protection measures to ensure data security. For enquiries regarding online transaction processing, the online merchant should be your primary point of contact.

complete Secure for internet payments

In online payment transactions, all parties are subject to the legal requirements of the PSD II. The implementation of the new version of the PSD by means of technical measures such as “strong customer authentication” or “risk-based transaction processing” is primarily intended to guarantee, in your own interest, that every online payment is carried out as securely as possible.

For the technical implementation of strong customer authentication we use the so-called “3D-Secure procedure”, also known as “complete Secure”.

Internet payments must be confirmed with both your Secure Code (your personal password, not to be confused with the four-digit card PIN or any other login data) and “an additional factor”, e.g. a mobile TAN sent via SMS to the mobile number provided by you. Please note that card complete can also use the mobile phone number that you have registered for complete Secure to make contact with you in special circumstances in the course of business. You can find more information on complete Secure at https://www.cardcomplete.com/sicherheit/complete-secure/.

Risk-based authentication

According to PSD II rules, authentication requests must also be forwarded to a so-called “risk-tool”. This tool uses various personal and anonymous data to perform a risk classification on the basis of a predefined set of rules. The result of this classification determines whether strong customer authentication is required or not, or whether a transaction must be rejected for security reasons. Card complete contracts with an external processor (Netcetera AG) to handle these processes in accordance with Art. 28 GDPR.

How securely are passwords processed?

In card complete portals such as https://www.cardcompletecontrol.com, your data is carefully safeguarded according to the current market standards. All passwords are stored in encrypted form.

complete Control user portal/complete Control iOS & Android app

Data security in our self-service portal

Personal data in the complete Control user portal or the complete control iOS/Android app are processed by an external service provider (Opentech Payment Services AG) bound by contract according to Art. 28 GDPR. In the self-service portal, your can add your credit card(s), check your latest transactions, change your account and address data, choose geo-blocking settings and set other preferences. Your e-mail address on file at card complete serves as your user name for the login. The highest level of security in the portal and app is guaranteed by strong customer authentication in accordance with PSD II. This is achieved by requiring a mobile TAN that is sent via SMS to the mobile phone number you have registered with card complete. If you use the complete Control iOS/ Android app, you can choose to replace the mobile TAN transmission by biometric functions (e.g. Face ID or Touch ID) if you wish.

Details on biometric data using the example of the complete Control iOS app

card complete does not process any biometric data in the complete Control iOS app during the technical Face ID or Touch ID procedure. Information on data protection and security for Touch ID can be found at https://support.apple.com/de-de/HT204587 and for Face ID at https://support.apple.com/de-at/HT208108.

Google reCAPTCHA for complete Control

complete Control uses the functionality of the “Google reCAPTCHA” service, which is provided by Google Inc, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA.
reCAPTCHA is a service from Google that protects websites from spam software and abuse by non-human visitors. The purpose of reCAPTCHA is to detect whether the data provided to complete Control (e.g. in a contact form) is entered by a human or by an automated program (robot).
For this purpose, reCAPTCHA analyses the behaviour of the website user on the basis of various characteristics. This process starts automatically as soon as the user is on the website.

For the analysis, reCAPTCHA evaluates information such as:
- the referrer URL (the address of the webpage from which the visitor just came);
- the IP address (e.g. 256.123.123.1);
- operating system details (which software – such as Windows, Mac OS X or Linux – is being used to enable the user’s computer to operate):
- cookies (small text files that store data in the user’s browser);
- mouse and keyboard behaviour (every action performed with the mouse or keyboard is saved);
- date and language settings (which language or date has been preset on the computer);
- all JavaScript objects (JavaScript is a programming language that allows websites to adapt to the user. JavaScript objects can collect many kinds of data under one name.);
- screen resolution (how many pixels are used to display images).

The data collected during this analysis is forwarded to Google. A reCAPTCHA analysis runs completely in the background without the awareness of the website user.

This data processing is based on Art. 6 Section 1 (f) GDPR. card complete has a legitimate interest in protecting its web offers from abusive automated spying and from spam.

Further information on Google reCAPTCHA as well as the privacy notice of Google may be accessed at the following links: https://www.google.com/intl/de/policies/privacy/ and https://www.google.com/recaptcha/intro/android.html.

Video identification procedure (Video ID) & electronic signature

When applying for a card complete payment card, you have the option to consent to a video identification procedure ("Video ID"); you can revoke this consent at any time. Instead of providing a traditional signature, you can sign the card application with a qualified electronic signature ("QES") in a seamless procedure in compliance with applicable laws. You fill the necessary data directly into the application form on the website.

A unique transaction number will be generated for your case, and certified, trained call centre agents will use the "CRIF Video Identification" application to identify you in a video call. This is performed by the company CRIF GmbH, which is a contractually bound data processor in accordance with Art. 28 GDPR.

This application is based on the product of WebID Solutions GmbH and WebID Austria GmbH as software manufacturers and platform operators and was developed according to the requirements of the Austrian Online Identification Regulation (Online-IDV).

A technical "pre-check" is used to verify whether the network quality and other technical performance data of the device being used are sufficient for the Video ID procedure. During the identification process, you and your ID document will be photographed and carefully checked for potential fraud. With your consent, the audio track of the entire conversation will be recorded. There will be no video recording. If the identification is successful, a confirmation code will be sent to you via SMS/e-mail.

Card complete and its partners use only products and services that meet the highest technical security requirements. The video calls are carried out by a regularly checked, highly secure call centre and by specially trained service staff. If you wish to provide a qualified electronic signature on the contract, after giving your consent, you will be forwarded to a qualified and trusted service provider, which acts as an independent data controller in the sense of the GDPR. This procedure complies with the requirements of the Austrian Signature and Confidence Service Law (SVG). The current list of trusted service providers can be seen here https://www.signatur.rtr.at/de/vd/Anbieter.html.

The complete PCI-DSS portal for merchants

The Payment Card Industry Data Security Standard (PCI–DSS) regulates the handling of payment-relevant data in on-site (point of sale) business and remote selling (e-commerce) in order to prevent fraud. Merchants are required to provide proof of PCI-DSS compliance, as stipulated in the acceptance agreement, in order to fulfil their applicable service contracts (Art. 6 Section 1 (b) GDPR).

card complete has a contract with the company usd A.G. as a processor in accordance with Art. 28 GDPR to process personal data of merchants. On the website https://pci.cardcomplete.com, merchants can log in to a protected login area with their assigned merchant profile and specific user data. The data in the profile is processed to prove the merchant's PCI compliance to the card organisations.

Such a profile can contain the following information, which need not necessarily be personal:

– merchant master data (for example, company name);
– name and contact data (address, e-mail, telephone number) of the contact person;
– documents for proof of PCI Compliance and for merchant communication;
– anonymous information on the number of transactions carried out;
– technical information on terminals and/or the payment service provider partner.

Your rights

What are your data protection rights?

Under the data protection laws, you can exercise the following rights at any time in your capacity as a data subject:

– the right to information
– the right to rectification
– the right to erasure
– the right to restriction of processing
– the right to data portability
– the right to object.

If you don’t want your data to be used for promotional purposes

Visit us at https://www.cardcomplete.com/datenverwendung, to object to any promotional use of your data and to revoke any consent given. You will also find the option to unsubscribe from each electronic advertising channel.

How to contact us to exercise your rights

If you want to exercise your rights, please use the following contact form https://www.cardcomplete.com/datenschutz/kontakt.

If you think that the processing of your personal data is in violation of the GDPR or the DPA, please contact us to clarify your concerns.

You may address any complaints to the Austrian Data Protection Authority.

The German version of this privacy notice prevails.

Version of this privacy notice: 06/2021