Privacy Statement for Credit Cards of Swisscard AECS GmbH for Private Customers

November 2024

1. What is this Privacy Statement about?

Swisscard AECS GmbH, Neugasse 18, 8810 Horgen ("Swisscard" or "we") processes data relating to you or other persons. This Privacy Statement explains our processing of such data (hereinafter "data" or "personal data") insofar as it relates to cashless means of payment ("cards") issued by us. **For further details on our data processing,** please refer to the following documents:

- in Swisscard's General Terms and Conditions, which provide additional information on the establishment and processing of the card relationship, and
- in other product and service terms and conditions (e.g. for bonus programs, online services and social media presences).

Our further Privacy Policies are provided on our website (www.swisscard.ch/datenschutz). If you have any questions, please do not hesitate to contact us (Section 2).

All references to persons in this document are meant to cover all genders.

2. Who is responsible for processing your data?

For the data processing under this Privacy Policy, the Data Controller is Swisscard, which means that it is primarily in charge of such processing under data protection law. If you wish to contact us in this regard, please use the following address:

Swisscard AECS GmbH
Data Protection Office
Neugasse 18
P.O. Box
8810 Horgen
E-mail: datenschutz@swisscard.ch

3. What data do we process?

We process various data from multiple sources for the purposes explained in Section 4. This includes the following data:

- **Basic customer data**: Basic customer data is what we call data relating to your person, e.g. name, address and other contact details, date and place of birth, nationality, additional information from identification documents, information about your contractual relationship with us (e.g. date of contract conclusion or type of card products, etc.), information about your banking relationship and information about relationships with third parties included in the data processing, e.g. authorized representatives or beneficial owners of the assets contributed in connection with the card agreement. We receive this data directly from you, e.g. in the card application, but also use third-party data. Such third-parties include, for example, financial institutions named in the card application, including UBS Group companies (as the legal successors of companies belonging to the Credit Suisse Group), your employer, address dealers and publicly available sources such as the Commercial Register, the media, the internet and online telephone directories;
- **Financial and risk data**: This is data relating to your asset and income situation, your financial situation, as well as other data used to prevent misuse and fraud, to comply with the Anti-Money Laundering Act and the Consumer Credit Act or other legal provisions. This includes, for example, information to determine your credit rating (e.g. information that allows conclusions to be drawn about the probability that claims will be settled) and information about the origin of assets. We receive this data from you, e.g. in the card application, but also from financial institutions, including UBS Group companies, from credit reference agencies, from the Central Office for Credit information (ZEK), from the Consumer Credit Information Office (IKO), and from publicly available sources such as the Commercial Register, the media, the internet and online telephone directories;
- **Transaction data**: Transaction data is data arising in connection with individual transactions, particularly when using cards or in the course of investigations at acceptance points (i.e. the merchants and service providers with whom you use the card) in the event of a complaint or fraudulent use of the card. Such data may include: information about acceptance points, amount, currency, time and date of individual transactions, further details on the type of transaction (e.g. “contactless”) or incorrect PIN entries, etc. For certain transactions such as the purchase of airline tickets, hotel invoices and vehicle rental invoices, such information may be more detailed. We receive this data from the acceptance point (i.e. the merchant) and from the American Express, VISA and Mastercard card networks; for more information on these networks, see Sections 6 and 7. In the case of mobile payment transactions (Apple Pay, Google Pay, Samsung Pay, Swatch Pay, etc.), we receive additional information from the corresponding provider (Apple, Google, Samsung, Swatch, etc.; “eWallet operator”), e.g. regarding the device used;
- Additional **information about the contractual relationship**, e.g. about insurance benefits (including insurance claims and related communication with you and with third parties) and in connection with bonus and loyalty programs and the use of online services. We also receive this data from you, but also from partners with whom we work (e.g. insurers, bonus and loyalty program providers or mobile payment providers);
- **Preferences**: This is data about the statistical probability that you will have an affinity to certain products and services or that you will behave in a particular way. We obtain this information from analysis of existing data that we can link to other data, e.g. anonymous data from statistical offices;
- **Communication data**: This is data related to our communication with you and, where applicable, with third parties that relates to you, e.g. information in e-mails or letters or records of telephone conversations;

- **Other data**: We may process additional data that we collect or receive in connection with the card relationship, e.g. information from authorities when we are involved in official investigations.

This data relates not only to you, but also, in some cases, to third parties (e.g. authorised agents, beneficial owners or additional cardholders). We primarily receive information about third parties directly from you, but in some cases also from third-party sources. Whenever you transmit data about third parties to us (e.g. information in the card application), we assume that you are authorised to do and that such data is correct. Therefore, please inform these third parties about the processing of their data by us and notify them of this Privacy Statement.

4. For what purposes do we process your data?

We process the data specified in Section 3 for various purposes related to the card relationship:

- To comply with laws, directives and recommendations issued by government agencies, and internal regulations ("**compliance**"), e.g. to combat money laundering and terrorist financing ("know your customer"), and to comply with tax control and reporting obligations as well as record-keeping obligations. To this end, we process your basic customer data and financial information in particular, as well as transaction data. This includes computer-based analysis of transaction data and payment transactions to identify unusual transactions.
- For purposes of our **risk management, fraud prevention** and **credit rating checks and credit assessments**, we especially process financial and risk data, as well as basic customer data and transaction data that allow the relevant conclusions to be drawn. For example, like all companies that advance funds, we must be able to assess and cover our credit risks (e.g. by setting an appropriate card limit). Under the Consumer Credit Act, we are also legally obliged to carry out a credit assessment when granting a partial payment option and must process the corresponding data for this purpose.
- To process the **card application** and the **contractual relationship**, particularly for **card transactions**, we process basic customer data, transaction data and other information, e.g. in connection with loyalty programs and insurance products. Such processing includes checking and authorising transactions, dealing with objections to transactions (e.g. under the charge-back procedure), managing points for loyalty and bonus programs, and settling insurance claims.
- We process data for **market research**, **marketing** and **customer care**. For example, we will provide you with information, advertising and product offerings from Swisscard and from third parties (e.g. insurance companies), as printed matter, electronically or by telephone. Like most companies, we also personalize marketing and other communications to provide you with information and offers that are relevant to you. We therefore collect data on preferences as the basis for these personalisations (see Section 3).
- We also process your data to **improve our services** and for product **development**. For example, we analyse which products are used by which groups of people and how.
- We may also process your data to ensure adequate **IT security**. Such processing includes, for example, analyses, tests, error checks and backup copies.
- We may process your data to the extent necessary **for other purposes**. These include training and education purposes, administrative purposes (e.g. management of basic customer data, accounting and record-keeping), enforcement of our rights and defence against claims (e.g. by securing evidence, legal assessments and participating in court or administrative proceedings), and preparing and processing purchases and sales of companies and assets (including the realization of existing or future credit card claims) and safeguarding other legitimate interests.
- To the extent that we ask for your **consent** for certain types of processing, we will inform you separately of the relevant purposes of the processing. You may revoke your consent at any time by giving us written notice thereof.

We base the processing of your personal data on the fact that processing is necessary to process your card application or to fulfil the card relationship (e.g. processing of basic, transaction, and financial and risk data for application verification, fraud prevention, credit rating checks and credit assessment, processing of transactions, etc.), that such processing is required or permitted by law, that it is necessary for our legitimate interest or the legitimate interest of third parties (e.g. processing for administrative and security purposes, for credit rating checks and purposes of marketing, market research, improving our services, and product development) or that you consented separately to the processing.

You may object to the processing for marketing purposes at any time by notifying us, including for individual communication channels (e.g. only advertising via e-mail) or for individual advertising campaigns or newsletters. This does not apply to automatically generated messages that cannot be individually adjusted, e.g. billing texts. Further information about your rights can be found in Section 9.

5. What applies to profiling and automated decision-making?

We can process and evaluate your data automatically in accordance with Section 3 for the purposes mentioned in Section 4 and thereby collect data on preferences. This includes what is known as profiling, i.e. automated analyses of data for analysis and forecasting purposes. The most important examples are profiling to combat money laundering and terrorist financing, to prevent fraud, to check credit ratings, and to manage risk, for customer care and for marketing purposes.

To ensure the efficiency and consistency of our decision-making processes, we make certain decisions on an automated basis, i.e. according to certain computer-based rules and without review by an employee. For example, we may:

- reject credit card applications or requests to increase limits in connection with credit rating and creditworthiness checks,
- block transactions if there are irregularities or, in case of products without fixed spending limits, if the relevant credit line has been exhausted,
- block or cancel the card in case of returned direct debits or in case of default on payment.

Such automated decisions are made for your protection, as well. If such a decision has a negative impact on you, you have the right to explain your opinion and have one of our employees review the decision. If you wish to exercise that right, please get in touch using the contact information on the letter in which we informed you of the decision or call us at the telephone number on the back of your card.

6. Whom do we disclose your data to?

Credit card products and -services are provided and handled based on extensive collaboration. Your data is therefore processed by various entities; by us, but also for example by merchants at which you use your card, by the card networks, by banks or by the post office, and by the service providers involved. As a payment instrument with a credit function, credit cards are also associated with certain risks (default risks, fraud risks, money laundering risks, etc.) which require corresponding clarifications with third parties and thus also disclosure of data, e.g. from credit reference agencies, offices, banks and the Swiss post office (see Section 3). Disclosure of data also occurs due to legal requirements, e.g. when we are subject to duties to clarify, report or provide information. In such cases, the entities involved may process your data, but may do so only within the scope of legal and/or contractual requirements.

This Section 6 explains the most frequent cases of data disclosure, indicating in each case which data may be disclosed. Further information can be found in Sections 3 and 4.

- **Service providers**: We work with service providers in Switzerland and abroad (e.g. for IT services, mailing of information, card personalization or payment collection) and provide them with the data required for their services. These service providers are subject to contractual and/or statutory confidentiality and data protection obligations.
- **Acceptance points and card networks**: When processing card transactions, data is processed by the acceptance point (the merchant) and transmitted via the international card networks of American Express, Mastercard and VISA.
- **ZEK and IKO**: We report to the ZEK (see Section 3) in the event of card blocking, serious payment arrears or misuse of the card. The ZEK may make this data available to its members in relation to credit, leasing or other agreements. We also disclose data to the IKO (see Section 3) as part of our statutory duties.
- **Automatic update of card data**: In case of recurring services (e.g. for certain purchases in ticket apps and online shops and for subscribers to media or apps), you can store card data for payment. With the updating service provided by Mastercard ("Automatic Billing Updater") and VISA ("VISA Account Updater"), the card number and the expiration date will be forwarded to Mastercard or VISA when a new card is issued or a card is renewed (but not in case of card replacement in cases of fraud or card loss). They make the corresponding data available to the acceptance points (merchants) participating in the service worldwide. You may waive automatic updating of card data by contacting our customer service department by telephone or in writing. You also have the option of deleting card data stored at the merchant or terminating the contractual relationship with the merchant.
- **Tokenisation of card data:** For security reasons, the card networks provide a service in which card data (card number and expiration date) are replaced by an encrypted sign ("token"). If a merchant participates in the tokenisation service, transactions are executed based on this token. For this purpose, we transmit updated card data to the card networks (e.g. in case of card renewal, product change, card replacement, blocking or termination of the card). The merchant will not be updated in this case. If a lost or stolen card is replaced, transactions may therefore also be executed even if the cardholder has not yet received his replacement card.
- **Mobile payment**: In the case of cards with mobile payment enabled, customer and device data as well as eWallet operator data will be exchanged among Swisscard, eWallet operators and the card networks for card management, ID checks, preventing abuses and fraud, compliance with legal provisions, and processing and displaying transactions. The eWallet operator may also provide in its terms and conditions that it may collect, process and disclose the aforementioned data for other purposes.
- **Click to Pay:** The American Express, VISA and Mastercard card networks offer this service for online payments under their own responsibility. When you register for Click to Pay via the Swisscard App, we disclose your information (particularly your card data, name, address, email, telephone number and device data) to the relevant card network. The operating card network's conditions and information applicable to you may stipulate that the above-mentioned data may be procured, processed and shared for further purposes.
- **Partner**: If the card bears the name or logo of third parties or if the card relationship includes bonus programs or insurance or other third-party services, Swisscard may exchange data with these partners to the extent necessary. These partners process the data received according to their own terms and conditions and may also use it for marketing purposes. By signing the card agreement, you also **authorize** these partners to **provide us with corresponding information**, e.g. on points balances in bonus programs or on insurance claims.
- **UBS**: Swisscard is a joint venture of American Express and UBS Switzerland AG (legal successor of Credit Suisse (Switzerland) Ltd.). Swisscard may provide data to and/or exchange data with UBS Switzerland AG (including other affiliated companies domiciled in Switzerland, hereinafter collectively referred to as the "Bank") in order to comply with the statutory and regulatory provisions and internal rules. If cards bear Credit Suisse marks (co-branded products) or belong to a co-branded card package, we may provide the Bank with additional data, including but not limited to information about completion of the application process, data about the processing of the card relationship (including additional and secondary benefits. e.g. bonus programs), transaction data to be displayed on the Bank's online banking portal, data

for the Bank's internal information and reporting purposes and information for its marketing purposes (for this last purpose, we may also provide the Bank with information about the card type, cumulative revenue figures and the number of transactions);

- **Additional cards**: The principal cardholder has access to all data in the principal and additional cards and may disclose it to third parties. The additional cardholder only has access to his/her own data, but may also disclose it to third parties.
- **Other disclosures**: In the larger context of the card relationship, data may also be disclosed to other recipients, e.g. to courts and government agencies in the context of proceedings and statutory duties of disclosure and cooperation, to purchasers of companies and assets, to financing companies in case of securitisations and to debt collection companies.

We also draw your attention to the following: when data is transmitted over networks, several Internet providers are involved in the transmission. It therefore cannot be ruled out that third parties may access and use transmitted data unlawfully. Sensitive data such as means of identification (especially card number, expiration date, card security code and PIN) should therefore never be transmitted by e-mail. In this regard, please note the due diligence obligations under the general terms and conditions applicable to the card product as well as any additional product and service conditions. Moreover, even in the case of encrypted transmission, the names of the sender and recipient remain identifiable. Third parties may therefore draw conclusions regarding existing or future business relationships.

The aforementioned disclosures in Switzerland and abroad (see Section 7) are necessary for legal or operational reasons. **By sending the card application, you therefore expressly release us from the statutory and contractual confidentiality obligations** that could prevent such disclosures.

7. When do we disclose personal data to foreign countries?

As explained in Section 6, your personal data is processed both by us and by other entities. These may be located outside of Switzerland. Your data may also be transferred abroad due to the fact that card services are based on international collaboration, that card networks have an international structure, that the cards may also be used abroad and that the eWallet providers may be located abroad. Your data may therefore be processed worldwide, including outside the EU or the European Economic Area (so-called third countries such as the USA). Many third countries currently do not have laws that ensure a level of data protection comparable to the level of protection under Swiss law. We therefore take contractual precautions to contractually compensate for the weaker statutory protection, unless disclosure is otherwise permitted by data protection law on a case-by-case basis (e.g. through express consent to disclosure, if the disclosure is directly connected with the formation or performance of a certain agreement, or if it is necessary for the determination, exercise or enforcement of legal claims). These precautions particularly include standard contractual clauses issued or recognised by the European Commission and the Swiss Data Protection and Information Commissioner (FDPIC). Additional information and a copy of these clauses can be found at https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/handel-und-wirtschaft/uebermittlung-ins-ausland.html.

Please also note that data exchanged over the Internet is often transmitted via third countries. Your data may therefore be transferred abroad even if the sender and recipient are located in the same country. The same applies to card transactions, even if the card is used at a domestic merchant.

8. How long do we store your data?

We store your data for as long as required by applicable statutory requirements or by the purpose of its processing. The duration of storage is therefore based on statutory retention obligations and the processing purposes (see Section 4), which also include safeguarding our legitimate interests.

9. What are your rights?

Data protection law gives you specific rights related to your personal data:

- You have the right to request certain information about our processing of your personal data (right to information).
- You may also require us to correct or supplement inaccurate or incomplete data, to cease processing for specific purposes (e.g. by objecting to marketing or by revoking a specific consent, which will not affect the legality of the processing performed pursuant to the consent up to the time of revocation) or to delete data that requires no further processing for the fulfilment of legal obligations or the protection of overriding interests. In the case of certain data, you also have the right to require us to make such data available in machine-readable format.

Please note that these rights are subject to statutory requirements and limitations and are therefore not available in their entirety in every case.

You are under no obligation to disclose data to us. However, we must process extensive data for legal or operational reasons for establishing and processing the card relationship. Therefore, if you do not wish to provide us with such data (particularly basic customer data or financial and risk data), we must refrain from entering into or continuing the card relationship. In such cases, a right to object can therefore only be asserted by terminating the card relationship.

If you wish to exercise any rights against us, please write a letter to us using regular mail (see Section 2) and attach a legible copy of your identification document.

10. How may we modify this Privacy Policy?

This Privacy Policy is not an integral part of the contractual relationship with you and we reserve the right to adapt this Privacy Policy at any time. At any given time, the version that is posted on our website shall be applicable.

Version of 11/2024