

Data Protection at Viseca Card Services SA (General Privacy Statement of Viseca)

Contents

I. General Provisions	2
II. Who are we and who is this Privacy Statement addressed to?	2
1. Who are we?	2
2. For whom and for what is this Privacy Statement intended?	2
III. How do we process your data?	2
1. What do we mean by “data processing”?	2
2. For what purposes and on what legal bases do we process your data?	2
3. Which specific data processing operations do we carry out?	3
4. Data retention	5
5. How do we protect your data?	5
IV. Who processes and receives your data?	5
1. Within the Aduno Group	5
2. Outside the Aduno Group	6
3. Customer and card data, aggregate turnover figures and transaction data	6
4. Credit information	6
V. Data transmission abroad	7
VI. Your rights in connection with the processing of your personal data	7
VII. Final provisions	8
1. Changes to this Privacy Statement	8
2. Where else can you find information about data processing by Viseca?	8

I. General Provisions

Viseca Card Services SA (hereinafter “**Viseca**” or “**we**”) respects your privacy. We take the necessary precautions at all times to protect your personal data and to merit the trust you have placed in us.

This Privacy Statement is intended to provide you with information in particular about which data we collect and process, why we do this, how we protect your data and how you can contact us and exercise your rights.

II. Who are we and who is this Privacy Statement addressed to?

In this section, you will learn who we are and whom this Privacy Statement is intended for, i.e. whose personal data we collect and process.

1. Who are we?

With over 1.5 million credit cards in circulation, Viseca is one of the largest Swiss issuers of payment cards. Working in close cooperation with Swiss banks, Viseca markets credit and prepaid cards, as well as other payment card products, such as the Mastercard Flex.

As the Controller with respect to the processing of personal data described in this Privacy Statement

Viseca Card Services SA
Hagenholzstrasse 56
8050 Zurich

is available for any questions or communications you may have regarding data protection and data processing.

You can obtain information by telephone (+41 58 958 84 00), email (privacy@viseca.ch) or post (Viseca Card Services SA, Data Protection, Hagenholzstrasse 56, 8050 Zurich).

2. For whom and for what is this Privacy Statement intended?

This Privacy Statement is addressed to our customers and to persons interested in our products and services. It is also addressed to persons whose data we are required to process in the context of business relationships (e.g. beneficial owners within the meaning of the anti-money laundering legislation).

III. How do we process your data?

In this section, you will learn which data we collect from you either directly or indirectly and how we use this data.

1. What do we mean by “data processing”?

Personal data (also referred to as “data” in the following) is all information relating to an identified or identifiable (natural or legal) person. If we process data, this means, for instance, that we collect, store, use, transmit or erase the data.

2. For what purposes and on what legal bases do we process your data?

We process your data mainly for the following purposes:

- **For concluding, performing and enforcing our agreements:** We process your data in particular to review card applications, conclude agreements and in the context of performing our agreements (you will find additional information about these data processing operations in the applicable General Terms and Conditions (“GTC”), (see Section VII/2). This also includes performing a credit risk and behaviour analysis (including fraud risk analysis and scoring), administering and developing customer relationships (including customer service, support and holding customer events) and customer communications.
- **For safeguarding our interests:** We also process your data to safeguard our legitimate interests. These vary widely and include in particular the following:
 - Continuous improvement and development, e.g. of the products and services we offer;
 - Gaining an understanding of customer behaviour, concerns and needs and conducting market studies, as well as creating corresponding customer profiles (e.g. based on card usage with certain categories of dealers or on the frequency with which the card is used for Internet purchases);
 - Conducting advertising and marketing activities, including creating marketing profiles. Direct marketing, e.g. by sending out a newsletter (including analysing its acknowledgement) and/or promotional materials. Channeling online advertising;
 - Providing efficient and effective customer service, maintaining contacts and otherwise communicating with cardholders outside the process of performing the agreement;

- Maintaining data security, in particular to protect against the loss of, destruction of and authorised access to your data and secrets, as well as our assets;
 - Administration, management, accounting and archiving;
 - Compliance with the statutory and regulatory requirements applicable to us, as well as our internal regulations;
 - Within the framework of risk management and to prevent and investigate fraudulent transactions, further criminal offences and other misconduct;
 - As with all companies, your personal data may also be used in connection with other operations. This includes e.g. executing the sale or acquisition of business segments, companies or parts thereof and other corporate transactions and the transfer of associated personal data.
- **For complying with legal obligations and safeguarding rights:** We also carry out data processing operations in connection with our statutory obligations, particularly to combat money laundering and terrorist financing, to verify your creditworthiness, to retain certain data as well as to comply with our internal regulations. Further, we may process your data to enforce and exploit rights and claims, to defend against legal claims, lawsuits or complaints and to combat abusive behaviour, to initiate investigations and proceedings and to answer official enquiries.
 - **Based on your consent:** We also process your data based on your consent which we request from you, e.g. when you visit one of our websites, apply for and conclude a card agreement or in connection with your use of the applicable services. Related consents can be found in particular in the applicable GTC (see Section VII/2). In these instances, the data are only processed for the purposes indicated in the consent.

3. Which specific data processing operations do we carry out?

3.1. When processing card applications

If you apply for a card with us, we process the data you provide us during the application process, such as your name and address.

Before concluding the agreement and in order to fulfil the contractual relationship, we are then required by law to collect and process your contact data, language, sex, date of birth and creditworthiness, as well as data relating to a verification conducted for purposes of combating money laundering (e.g. occupation). Where the provisions of the Consumer Credit Act apply, we are required to conduct a creditworthiness check pursuant to the statutory rules.

Your data may also be processed and associated with data that we obtain from other sources or collect ourselves.

In particular, we receive or obtain data from governmental authorities, databases/credit agencies (World Check, Teledata/CRIF, CreditReform, Zefix, tel.search.ch etc.), credit information services such as the Centre for Credit Information (ZEK) and the Centre for Consumer Credit Information (IKO), intermediary banks, employers, other member companies of the Aduno Group, registries such as local.ch, commercial registers, the media, as well as from the Internet in general.

3.2. When using the card

3.2.1 In general

When you or third parties use your card, we process the following data in particular:

- Data that are provided to us during the card relationship or that we collect ourselves (e.g. name changes, changes regarding the beneficial owner, proof of assets, data from other persons in case of an insured event etc.);
- Transaction data (data concerning service and cash-withdrawal details). This relates to the following information in particular:
 - Card acceptance point (*where was the purchase made?*);
 - Transaction amount (*how much did the purchase cost or how high was the debit amount?*);
 - Time of the transaction (*when was the purchase made or when did the debit occur?*);
 - Additional data such as the type of card usage (e.g. online, contactless), the number of wrong PIN entries or the currency selected.
- Only for certain transactions is the information more detailed, e.g. when purchasing airline tickets, renting a car or booking a (hotel) stay, as well as – if you participate in the surprize bonus programme – when redeeming rewards on the surprize website, as well as for payments between private individuals. Only in these few exceptional cases do we have access to your shopping basket (*what was purchased?*).

- Viseca may potentially draw substantial conclusions about the cardholder's behaviour from the transaction data (e.g. place of residence and employment, state of health, financial situation, leisure habits, social behaviour and further details);
- Data associated with using the card for online payments such as Internet access details (IP address), the devices used or the performance of an additional authentication by the cardholder, although such data often do not constitute personal data;
- Data from other sources (e.g. intermediary banks, the Centre for Credit Information (ZEK) and the Centre for Consumer Credit Information (IKO), governmental authorities, credit agencies, employers, other member companies of the Aduno Group, publicly available databases or registries such as local.ch or the commercial register) in connection with the respective purpose.

3.2.2 Contactless payment

Our products enable you to make contactless payments. This works via an antenna-equipped chip that is integrated into the card. The antenna uses Near Field Communication (NFC) technology to exchange information between the payment terminal and the card.

The chip stores the 16-digit card number, the expiry date and other details (card data) that are necessary in order to process a transaction. The chip of Mastercard cards also currently stores the dates and amounts of the last 10 transactions made with the card. In contrast, the cardholder's surname and first name are not stored on the chip itself (except for Visa cards issued before 28 April 2014), but rather on the card (magnetic strip).

To customers who, despite the advantages of contactless payment, wish not to use this feature, we offer an **alternative**. You can apply for a credit card without the contactless payment option. You can download the corresponding **application form** [here](#).

3.2.3 Transaction monitoring

If you or third parties use your card, the transaction data is transmitted to us from the card acceptance points (i.e. from the business where your card is used, the "merchant" or a cash machine). We then review, authorise and invoice the cardholder for the transactions.

In the event of the withdrawal of cash from Swiss cash machines using a card with a debit feature or a credit card that is authorised for use at cash machines with direct debit to the bank account, the transmission takes place via direct debit (authorisation request and direct debit of the corresponding bank account of the cardholder).

When authorising the transactions, we verify whether it was made by the authorised cardholder. As we want to limit the financial risk associated with fraudulent transactions, we take a variety of measures at our own discretion to prevent fraud/upon suspected fraud.

If a secure payment method (3-D Secure) is used for the card in an online shop, we collect and verify the data needed for this operation.

Your data are also processed in connection with the transaction complaint and chargeback process, e.g. for purposes of investigating unknown transactions or in connection with unjustified debits. Similarly, data are collected and processed for managing insurance cases in order to investigate the claims in cooperation with the insurance partner (see also the [General Terms and Conditions \(GTC of Insurance\)](#)).

3.3. In connection with the surprize bonus programme

If you participate in the surprize bonus programme, we process data that are communicated to us or that we obtain from third parties or collect ourselves when you register for the bonus programme, in the course of your participation in the bonus programme on the surprize website or when using the surprize app (see separate Privacy Statement at www.surprize.ch/datenschutz).

3.4. In connection with the use of one

If you use one, we process data that are communicated to us when you register, log in or manage your user account via one or that are communicated to us or that we obtain from third parties or collect ourselves when you use Mobile Pay, Wearable Payment or 3-D Secure (see separate [one Privacy Statement](#)).

3.5. In connection with the use of our websites and Internet services

When you visit our websites or use our Internet services, we process your data that are communicated to us or that we obtain from third parties or collect ourselves in connection with the use of the Viseca websites www.viseca.ch, www.one.viseca.ch, www.surprize.ch, www.mycard.ch, the one app, as well as other Viseca services in accordance with the terms and conditions of use of the respective websites or services;

3.6. Data processing for risk purposes (profiling)

We process your data for risk purposes in order to determine the risks associated with the issuance of cards (e.g. credit and market risks). This is particularly necessary because we bear the financial risk under the contractual relationship with the cardholder (credit risk).

3.7. Data processing for marketing purposes (profiling)

The collected credit or prepaid transaction data or debit transaction data in the case of a combined cards with a debit feature enable us, also in combination with publicly available data, to build customer, consumption and preference profiles for marketing purposes that allow us to develop and offer you products and services of interest to cardholders. We may send you such information about our own products and services or those of our partners via the available communication channels (e.g. post, email, push notifications) or channel online advertising accordingly.

For cards with only a debit feature, the collected debit transaction data enables us to build and analyse customer, consumption and preference profiles to develop and evaluate products and services exclusively associated with the debit feature and to offer you such products and services of Viseca or send you information about them via post, email or otherwise.

Every cardholder may opt out of receiving information (ad blocking) or by providing written notification (including via email) to Viseca generally withdraw its consent previously granted to the processing of data for marketing purposes (general withdrawal). The foregoing does not apply to non-marketing messages and automatically generated invoicing texts.

3.8. Mailing of information and advertising

We may send cardholders information (including advertising) and communicate with them by post or electronically (via email, push notification, SMS, one (website or app) or in any other appropriate manner. The electronic communication takes place through public communication networks. Data transmitted in this way is generally accessible to third parties and can be lost or intercepted or altered by unauthorised third parties during transmission. Therefore, despite the implementation of security measures, it cannot be ruled out that third parties will gain access to the communication with the cardholder.

We only initiate contact by email if we received the email address from the sender when the sender contacted us, such as by providing details in the card application, making the relevant entry in a contact form, registering for a service or newsletter or participating in competitions.

Detailed information regarding the initiation of contact by Viseca, phishing and online security in general can be found in the [FAQ](#) on the Viseca website.

4. Data retention

We store your data for as long as this is necessary for the purpose for which it was collected. Further, we store personal data if we have a legitimate interest in their retention, e.g. if we need the data in order to enforce or defend against claims, to guarantee IT security or if statutes of limitations are running. Finally, we store your data in order to comply with our statutory and regulatory obligations.

5. How do we protect your data?

We have implemented appropriate technical and organisational measures to ensure the security of your data and to protect them from unauthorised access, misuse, loss, falsification or destruction, etc. We review these measures on a regular basis.

IV. Who processes and receives your data?

In this section, you will learn who can access your data and to whom we may transmit your data.

1. Within the Aduno Group

Within Viseca, only those departments and persons are provided access to your data who need such access for purposes of performing our contracts or safeguarding our legitimate interests or complying with our contractual and statutory obligations (see Section III/2).

With your consent, e.g. by accepting the General Terms and Conditions, we transmit your personal data within the scope of your consent to other companies of the Aduno Group so that they can process the personal data for their own purposes.

2. Outside the Aduno Group

If you or third parties use your card, the transaction data is transmitted to us from the card acceptance points (merchant or cash machine). **This transmission generally occurs via the global networks of the international card organisations Mastercard and Visa** (see in this regard the global privacy notices of [Mastercard](#) and [Visa](#)).

Further, your data may be transmitted to governmental authorities in the event of a duty to provide data or a legitimate interest of Viseca.

2.1. Transmission in connection with Automatic Billing Updater (ABU)

For recurring services for which the cardholder has provided its card data ("card on file") we may, when the card is renewed or replaced, automatically transmit the card number and expiry date to Mastercard, which transmits the card data to authorized merchants (so-called Automatic Billing Updater, ABU). In order to initialize the ABU-service, we will transmit the card number and the expiry date of all active cards to Mastercard presumably in March 2019.

Exception: If the existing card is replaced due to a case of fraud, there is no automatic transmission of the new card data (card number and expiration date) to Mastercard.

Every cardholder has the option to prevent the transmission in connection with ABU by either (a) terminating the card relationship before obtaining a replacement card, (b) deleting or terminating the contractual relationship with the merchant with whom cards are on file or (c) by opting out of participating in ABU with Viseca.

The described process only works for merchants which are connected to the ABU-system.

2.2. Data processing by service providers

In order to perform the services we offer, we work with service providers in Switzerland and abroad. This mainly concerns services in the following areas:

- card personalisation, PIN generation etc.
- IT services, e.g. maintenance and operation of our systems, services related to data storage (hosting), distribution of email newsletters, data analytics, etc.;
- consulting services, e.g. services performed by tax advisors, attorneys, management consultants, etc. if data processing is involved;
- services related to order processing, shipping and logistics, e.g. for invoicing, mailing of ordered payment cards, as well as print services;
- business information and collections, e.g. if outstanding debts are not paid.

Through the selection, instruction and monitoring of those service providers who perform contracted data processing, we make sure that the protection of your personal data is ensured throughout the entire processing. Contracted data processors are subject to the same obligations in connection with data protection and data security as we are.

3. Customer and card data, aggregate turnover figures and transaction data

In connection with cards for which the Viseca Credit/Prepaid GTC or the Viseca Business GTC apply, we only provide data to third parties (e.g. the intermediary bank) for their internal purposes if permitted by law, e.g. in order to comply with a statutory obligation or based on the cardholder's consent. **You can withdraw your consent to the disclosure of credit or prepaid transaction data to the intermediary bank prospectively at any time without giving reasons.**

In connection with cards for which the Viseca Payment Card GTC apply, we provide intermediary banks with customer and card data as well as aggregate turnover figures and transaction data (credit or prepaid and/or debit transaction data, depending on the product type).

For cards with only a debit feature or combined cards with credit and debit features resp. prepaid and debit features, the disclosure of the debit transaction data to the bank is required for performing the services.

4. Credit information

In accordance with our obligations, we disclose credit information to the ZEK resp. the IKO. Particularly if a card is blocked or in the event of qualified payment default or fraudulent card use or similar circumstances, we are authorised to notify the ZEK and, as required by law, the relevant law enforcement agencies.

V. Data transmission abroad

The recipients of personal data mentioned in this Privacy Statement may be located abroad, including outside the EU or the European Economic Area (so-called "third countries"). These third countries may not have laws in place that protect your personal data to the same extent as in Switzerland or in the EU resp. EEA.

If we transmit your personal data to one of these third countries, the recipients of the personal data are required to ensure that your personal data receives appropriate protection. This occurs e.g. by concluding data transmission agreements. In this regard, it is important to us that these be agreements that are approved, issued or recognised by the European Commission and the Federal Data Protection and Information Commissioner (use of so-called standard contractual clauses). Further, transmission to U.S. recipients is permitted, if such recipients have subjected themselves to the U.S. Privacy Shield programme.

VI. Your rights in connection with the processing of your personal data

In this section, you will learn which decisions you can take concerning the data collected by us and how you can control these decisions.

If the applicable conditions are met, you have the following rights concerning your personal data and you may contact us in this regard at any time (Section II/1):

Right	Subject matter
Right to information	You have the right to be informed in a transparent, clear and comprehensive manner as to how we process your personal data and as to your rights in connection with the processing of your personal data.
Right of access	<p>You have the right to request access to your personal data stored by us at any time and free of charge if we process such data.</p> <p>The right of access may be restricted or excluded in individual cases, particularly:</p> <ul style="list-style-type: none"> • if you have not been able to adequately identify yourself; • to protect other persons (e.g. confidentiality obligations or data protection rights of third parties); • in case of misuse <p>As a rule, we will reply to your request within one month of receipt. However, if it will take longer to process your request, we will inform you of this.</p>
Right to rectification	You have the right to have incorrect or incomplete personal data rectified and to be notified of their rectification.
Right to erasure	<p>Under certain conditions, you have the right to have your personal data erased. You may request the erasure of your personal data if:</p> <ul style="list-style-type: none"> • the personal data are no longer necessary for the purposes pursued; • you have validly revoked your consent or validly objected to the processing (see below); or • the personal data are being processed unlawfully. <p>The right to erasure may be excluded in individual cases, particularly if the processing is required:</p> <ul style="list-style-type: none"> • for exercising the right of freedom of expression; • for complying with a legal obligation or for performing a task in the public interest; or • for enforcing legal claims.
Right to restriction of processing	Under certain conditions, you have the right to request that the processing of your personal data be restricted. This may mean, for instance, that the processing of personal data is (temporarily) discontinued or that published personal data are (temporarily) removed from a website.
Right to lodge a complaint	You have the right to lodge a complaint with the Federal Data Protection and Information Commissioner (FDPIC) against the manner in which your personal data is processed.

Right	Subject matter
Right to withdraw and object	<p>You have the right to withdraw at any time a consent previously given.</p> <p>In certain cases, you may also object to the processing of your personal data (for instance, where your data is processed in connection with advertising). However, past processing activities based on your consent are not rendered unlawful by your withdrawal of consent. You can deactivate the targeting of behaviour-based online advertising on the respective website.</p> <p>In cases where a data processing operation is required for performing the relevant service (e.g. forwarding of transaction data to your bank when you use the debit feature so that your bank account can be debited) or fulfilling the agreement (e.g. processing data for risk purposes), withdrawal of consent is not possible. In such cases, these data processing operations can only be waived by terminating the card agreement.</p>

The provision of information and processing of your requests are free of charge unless your request is obviously unwarranted or excessive (particularly in case of a repeated request). In this case, we may charge a reasonable fee or refuse to process your request.

VII. Final provisions

1. Changes to this Privacy Statement

This Privacy Statement may be modified over time if we change our data processing operations or if new legal requirements become applicable. We actively inform persons registered with us about such changes if this is possible without unreasonable effort. Our current Privacy Statement is available on our website (www.viseca.ch/en/data-protection/viseca) at all times.

2. Where else can you find information about data processing by Viseca?

Separate privacy statements may apply to individual processing operations. At present, this concerns the following processing operations:

- **one:** available at [one Privacy Statement](#);
- **surprise:** bonus programme: available at www.surprise.ch/datenschutz;
- **Website:** accessible at the respective Terms and Conditions of Use of the Viseca websites (see Terms and Conditions of Use at www.viseca.ch / www.one.viseca.ch / www.surprise.ch / www.mycard.ch), the [Terms and Conditions of Use of one](#) and the [Privacy Statement of one](#), as well as the [Terms and Conditions of Use of the "eXpense" Online Services](#) (for business cards) and the relevant [FAQ](#).
- **Smart Data OnLine:** The "Smart Data OnLine" service is provided for purposes of displaying transactions and invoices for holders of corporate cards. This is a service of Mastercard International. Registration for this service is completed directly on the "Smart Data OnLine website". The information provided by Viseca for this service is processed and stored by Mastercard abroad, particularly in the USA. The use of "Smart Data OnLine" is subject to the applicable legal provisions and the global [Mastercard SmartData Privacy Notice](#).
- **Other:** [Terms and Conditions for SMS Services](#), [Special Terms and Conditions for Electronic Invoices](#), [Terms and Conditions for 3D-Secure](#), [Special Terms and Conditions for the "e-banking connection"](#) (provided that consent to the integration of certain information into e-banking has been received by the bank), as well as the relevant [FAQ](#).
- **Mastercard and Visa:** Please also note the relevant terms and conditions of Mastercard and Visa, particularly the global privacy notice of Mastercard and your enforcement rights as a thirdparty beneficiary regarding the binding internal data protection regulations of Mastercard as well as the information from Visa.

Version of 12/2018