

Your trust is important to us. PostFinance is fully committed to handling your personal data responsibly. Our Privacy Policy contains information about the personal data that we collect from our customers and other data subjects, what we do with this data and what your rights are in this respect.

1. What is this Privacy Policy about?

PostFinance Ltd, which has registered offices at Mingerstrasse 20, CH-3030 Bern (hereafter referred to as "PostFinance" or "we"), processes personal data that relates to you or to individuals with whom we have no direct contact. We use the terms "data" and "personal data" synonymously throughout this Privacy Policy.

"Personal data" refers to information that relates directly to you or to other people with whom we are not in direct contact, or which we can attribute to you. You can find details on the data we process in accordance with the information provided in this Privacy Policy in section 4 ("What data do we process?"). "Process" refers to any activity that involves, for example, the handling, collection, storage, use, disclosure or deletion of personal data.

In this Privacy Policy, we describe how we process your data when you use our products or services, stay in touch with us as part of a contractual relationship or communicate or interact with us in other ways.

We process data that relates to the following individuals in particular:

- Our current and former private customers, business customers and their associates, such as business partners, additional card or account holders, authorized representatives (e.g. authorized persons or individuals authorized to receive information), beneficial owners, controlling persons, key contact persons or heirs
- Interested parties and potential customers
- Individuals who we provide with products
- Participants in competitions, prize draws, surveys, user tests, customer events and similar organized gatherings
- Visitors to our premises and Postomat users
- Contact persons and employees at suppliers and partners
- Contact persons, company owners and management bodies of businesses in which PostFinance has a stake
- Persons who make payments to our customers
- Representatives of authorities, agencies, auditors and other bodies
- Media employees

This Privacy Policy applies to the processing of data that we have already collected or which we will collect in future. We will inform you about certain types of data processing separately, e.g. in specific privacy policies, general terms and conditions, subscriber conditions for products and services, product and service descriptions, on our website and in declarations of consent, contracts, forms and notes. A separate privacy policy containing information concerning data processing in relation to our websites can be found at postfinance.ch/dps-web.

2. What do you have to do when sending us personal data about other people?

When you share data with us about other individuals (e.g. authorized representatives, controlling persons or heirs), you confirm that you are authorized to do so and that the data you are providing is correct. Please ensure prior to this that all third parties have been informed that we will process their data and forward them a copy of either this Privacy Policy or the document entitled "Information on data protection", which can be found at postfinance.ch/dps.

3. Who is responsible for processing your data?

PostFinance Ltd is generally responsible for processing data within the scope of this Privacy Policy, which means that it bears primary responsibility for this data processing under data protection law, unless otherwise specified in individual cases.

Every activity that involves data processing is monitored by at least one corporate body which is (or are) tasked with ensuring that said processing is performed in compliance with the statutory provisions on data protection. This entity is known as the "data controller". Other parties may be jointly responsible for processing within the context of this Privacy Policy if they are involved in determining how, and to what end, the relevant data is processed. On request, we will be happy to provide information about the individual data controllers that are responsible for specific processing activities (see section 12, "Your rights"). Please contact these third parties directly if you have any questions or wish to assert your rights against them.

It may be the case that, in app stores, the app developer is listed as the data controller. We, however, are responsible for the data we process ourselves under data protection law.

Please contact us using the following details if you have any concerns about data protection or wish to assert your rights in accordance with section 12 ("Your rights"):

PostFinance Ltd
Data Protection Officer, Legal
Mingerstrasse 20
CH-3030 Bern
mydata@postfinance.ch

4. What data do we process?

We process different data from a range of sources, depending on the situation and purpose. We generally collect this data from you directly, i.e. when you submit information to us, communicate with us or use our products and services. However, we can also collect it from other sources, such as public registers or other publicly accessible sources, as well as from authorities or other third parties. We process data about you from different categories, the most important of which are the following:

Master data: we use the term "master data" to refer to any information that relates to your identity, personal characteristics and circumstances, including your name, address, date of birth and factual data (e.g. market value of your property). This data can also relate to third parties (e.g. authorized agents) and can include authorizations to sign, powers of attorney and declarations of consent.

When we deal with companies, we process data about their designated contact persons and occupational data. We may also process information about a company's relationship with third parties (e.g. controlling persons or beneficial owners). Depending on its area of activity, we may also need to examine the company in question and its employees in more detail, e.g. by performing a security check (for example using a criminal records extract).

Financial and risk data: this involves processing data that relates to your income and assets, your financial situation and financial behaviour, as well as other information that we use to combat fraud and misuse and comply with legislation on money laundering, consumer credit or other statutory provisions.

This includes data such as information about your risk and investment profile, your risk capacity and your knowledge of and experience in dealing with financial products. It also includes data for determining creditworthiness (i.e. information that allows conclusions to be drawn about the probability of accounts receivable being settled). This also includes, for example, data on any technically identifiable behaviour when accessing e-finance and the PostFinance App (behavioural biometrics to tackle abuse and fraud).

Order and transaction data: this refers to the data that accumulates prior to the conclusion of a contract or in relation to individual orders and transactions, such as incoming and outgoing payments (including card payments). This also includes data pertaining to brokered products and services.

Tax data: this includes information about compliance with fiscal regulatory requirements.

Fiscal data includes information about your tax domicile and corresponding certificates and documentation, your Tax Identification Number (TIN), declarations to certify compliance with tax obligations, and tax assessment notices, as well as data associated with the automatic exchange of information (AEOI), the Foreign Account Tax Compliance Act (FATCA) and the Qualified Intermediary Agreement (QI Agreement).

Additional data relating to the contractual relationship: if you have concluded a contract with us, we will process additional data, including information on the products and services you buy and use, how contracts are performed and executed and information on feedback about our services (e.g. information on satisfaction).

Behavioural and preference data: this is information that relates to particular actions and interactions with us. We can use this information, along with other types of data, to calculate the statistical probability of you being interested in certain products and services or to predict that you will behave in a certain way (preference data). We generate this type of data based on existing information, but can also combine it with other data to improve the quality of our analyses.

Behavioural data also gives us an insight into your specific actions, such as how and when you log into e-finance, which payment methods you use, which transactions and payments you are involved in, which products and services provided by us or third parties you buy and use, the contact you have with the Customer Center, your visits in-branch, and which prize draws, competitions and events you participate in.

Preference data helps us to gauge what your needs are, which products and services might appeal to you, or how and when you respond to messages from us, for example. We use this information, which we obtain by analysing existing data, to get to know you better, tailor our services so that they are more relevant to you and optimize them in general, for example.

Behavioural and preference data can be analysed either at an individual level (e.g. to allow us to share bespoke offers created for you or to show you specific adverts) or on a general basis (e.g. to assist with product development). We can combine behavioural and preference data with other types of data.

Visitor and communication data: this includes information that relates to how and when we communicate with you, whether in written form, by telephone or via electronic channels (such as e-finance, chat, e-mail, SMS, push notifications or the PostFinance App). It can also include data concerning our communications with third parties, authentication data (as well as biometric data where applicable) and video and audio recordings or data related to building access. We also collect data to help identify you (such as a copy of your passport) if we want to confirm your identity or are required to do so, e.g. as part of a request for information.

We also process data (such as the speed, frequency and volume of your voice) when we use voice recognition to authenticate you, provided that you have given your consent to the use of such a method. We collect this data during your call and compare it to the corresponding information that we have on record about you (your "voiceprint"). More information on this topic can be found in separate privacy policy notices, which can be accessed at

→ Authentication with voice recognition – Adjust settings | PostFinance. We may also record video footage in designated areas of our sites and around Postomats. Please do not hesitate to contact us if you have any questions (see section 3, "Who is responsible for processing your data?").

Technical data: this refers to the information that we collect when you use e-finance, the PostFinance App or other digital services offered by PostFinance or take part in an online survey, for example. This includes your device's IP address, as well as the log files that we use to record information on how our systems are used. To ensure that our services function correctly, we may also assign an individual code to you, your device or your system (in the form of cookies, for example; see section 11, "Which online tracking and analysis techniques do we use?"). It is not

possible to identify you or deduce anything about your identity based solely on technical data. However, we can link this data, as well as information collected from user accounts, registrations or access controls (or even with information about the performance of a contract) to other information and consequently to you, given the right circumstances (see section 11, "Which online tracking and analysis techniques do we use?").

Technical data includes information such as your device's IP address and information about its operating system, as well as the date, time, geographical region and the type of browser or device that you use to access our digital services. One of the ways this information helps us is that it allows us to display content correctly in your browser or on your device. Knowing your IP address allows us to identify your provider and thus your region, but we cannot usually use it to identify you unless you are logged in to a user account (see section 11, "Which online tracking and analysis techniques do we use?"). The log files that are generated in our system are another example of technical data. If you open one of our apps, we collect technical data about how the app is installed, when it is opened, and identifiers associated with the device that you are using.

Registration data: this refers to the data that you submit when you create a user account or register in order to use or participate in certain offers and services (e.g. newsletters and competitions). This also includes the data that we collect when you use that offer or service. Registration data, including biometric data, may also be required for access control.

Other data: we collect other data about you in various contexts. This includes information that relates to official or legal proceedings (e.g. case files, evidence, etc.). We can also collect data to help with fraud prevention or for reasons associated with occupational health and safety, and may obtain or produce photographs, videos and sound recordings in which you may be identifiable (e.g. in video recordings). We may also collect data when you enter or exit our premises, as well as information regarding your access rights (including access controls etc.). Finally, we may also collect data in connection with events or promotions (e.g. competitions) and the use of our systems and infrastructure. Sometimes we also carry out user tests and surveys, which also involve collecting data.

5. Why do we process your data?

We process your data for the purposes outlined below.

Establishing, registering, processing, managing and terminating business relationships

We process your data to establish, register, process, manage and terminate business relationships, or to process the contract that has been entered into with you (e.g. if you are our supplier). The data that we process to this end varies depending on the type and scope of the relationship and may include master, financial, risk-related, order, transaction, registration and communication data in particular.

When it comes to processing business relationships, we process data if you make use of our products and services, for instance concerning account management, during account and payment transactions, regarding card usage, during the acquisition and purchase of investment products and when you use e-trading, e-finance or the PostFinance App for the purposes of preparing and providing information and processing orders, etc.

We also process private customers' order and transaction data in order to automatically categorize transactions and display them graphically within e-finance and the PostFinance App, provided that the private customer has not opted out of receiving them.

Compliance with laws, directives and recommendations from public authorities and internal regulations

We also process data to comply with laws, directives and recommendations from public authorities and our own internal regulations (Compliance). The data that we process for this purpose includes your master, financial, risk-related, communication, order, transaction and behavioural data in particular.

This includes fulfilling our legal obligation towards combating money laundering and terrorist financing, for example. To this end, we have a duty to make certain enquiries or, under certain conditions, to submit reports (e.g. to authorities).

Data processing in this context also requires or entails the following:

- The fulfilment of obligations regarding the disclosure, provision and reporting of information, for example in the context of supervisory obligations and requirements under tax law, such as the automatic exchange of information
- The fulfilment of obligations concerning data retention, as well as the prevention, detection and investigation of criminal offences and other violations

This includes receiving and processing complaints and other messages, monitoring communications, conducting internal investigations or disclosing documents to a public authority if we are obliged or have a legitimate interest in doing so. Personal data about you may also be processed in the context of external investigations (i.e. those conducted by regulatory authorities and prosecution services or appointed private bodies) and internal investigations. This may also include the computer-assisted analysis of order and transaction data and payment processes, as well as risk data, in order to identify unusual transactions. Data is always processed either under Swiss law, in accordance with non-domestic regulations to which we are subject, or in keeping with self-regulation, industry standards, our own corporate governance or instructions and requests from public authorities.

Risk management, prevention of fraud and other illegal activities, and prudent corporate management

We also process data – in particular, master, order and transaction, financial, risk-related and behavioural data – for the purposes of risk management, to assist in preventing fraud and other illegal activities, and to ensure prudent corporate management, including business organization and corporate development.

As part of our corporate development, we may acquire or sell businesses, sections of a company or companies, or enter into partnerships, which can all entail the exchange and processing of data. We may also process data for the purpose of auditing and optimizing our internal processes (e.g. as part of an audit review). In order to prevent fraud and other illegal activities, we may also conduct internal investigations and process data to detect irregularities (e.g. in card money).

Brokering of third-party products and services

We also process personal data – in particular master, order and transaction data – to broker third-party products and services, e.g. insurance, vested benefits accounts, retirement savings accounts, personal loans and mortgages.

The products and services that we broker are offered through our infrastructure, but are operated and performed, either in full or in part, by third parties. For example, we are responsible for making mortgages available on the market and for generating sales, performing credit checks, loan processing, servicing and, in some cases, issuing payment reminders. Our cooperation partner deals with refinancing, and ultimately acquires the receivables from mortgage loans. In the case of pension products, insurance policies and other services (e.g. when using PostFinance Pay, digital services such as issuing iTunes or Netflix gift cards, Paysafe vouchers and travel payment methods, including banknote delivery), the respective provider is generally responsible for data processing. However, we may also process this data for our own purposes, primarily for marketing purposes.

Marketing and customer care purposes

We process data for marketing and customer care purposes to allow us to send you, for example, personalized information, recommendations and offers regarding the products and services provided by us and third parties (e.g. cooperation partners). This information may be sent in a letter, via e-finance or as part of a newsletter, for example, or it may also come in the form of a personal consultation over the phone. We may also process your personal data in order to tailor the marketing material on our PostFinance website, so that it corresponds more closely to your interests (see section 11, “Which online tracking and analysis techniques

do we use?”). The data that we process for the purpose of marketing and customer care includes your master, financial, risk-related, order and transaction, and behavioural and preference data, as well as other information regarding the contractual relationship.

You can object to the analysis of certain personal aspects of yourself (*profiling*) for marketing purposes at any time.

We also process data in relation to competitions, prize draws and events. Our customer care service includes personalized communications, such as invitations to sporting and cultural events, which we send to existing customers as part of our customer loyalty programme. We also have a customer relationship management (CRM) system in which we store data that is essential to maintaining our relationship with customers, suppliers and other business partners. This includes data about contact persons, historical data about the relationship (e.g. details on which products and services have been purchased or supplied, interactions), interests, preferences and marketing measures, in addition to other information. We process personal data to be able to organize customer events, provide participants with information and share marketing materials before, during and after the event has taken place.

Market research, optimization of services and operations as well as product development and development of self-learning programmes

We also process your data for the purpose of market research, to optimize our services and operations, for product development as well as for developing self-learning programmes. This involves processing your master, transaction, behavioural and preference data, as well as information from surveys and user tests.

It is our goal to continually adapt our products and services to the needs of our (potential) customers and determine how satisfied they are with what we offer. To achieve this, we analyse data such as which groups of people use what products in what way, how new products and services and any other measures could be designed, and how our e-finance and the PostFinance App are used. This gives us an insight into the public response to existing products and services and the market potential of new ones. We are also constantly committed to improving our internal processes and systems, and may also use your data for this very purpose. The further development of self-learning programmes is intended to optimize these programmes, which serve to support internal processes and manage business relationships.

Security and access control purposes

We may also process your data – in particular your master, technical, behavioural and other data – for security reasons and access control purposes.

We continuously review and optimize the security of our IT and physical infrastructure (e.g. buildings). That is why we process data that is gathered via surveillance systems in our buildings or publicly accessible spaces. Maintaining security is also essential when it comes to our digitized products. Nonetheless, it should be noted that the threat posed by data security breaches can never be fully mitigated. PostFinance combats these risks by adopting appropriate technical and organizational measures in line with the state of the art. Access controls involve managing access to electronic systems (e.g. log-ins to user accounts) on the one hand and physical access control (e.g. access to rooms) on the other. We are also introducing access controls in the form of visitor lists and video surveillance (e.g. security cameras) for security purposes (these are preventive in nature but also assist in investigating incidents when they occur). We have installed the appropriate signage to draw your attention to the security cameras in the areas in which they are used.

Communication

We also process the data that we collect in connection with communications with you and third parties so that we can send you information or messages, respond to your enquiries and communicate with you. We use your master and communication data in particular for this. We normally store this data on our system in order to document our communication with you, perform quality assurance and refer to it in the event of future enquiries.

If you get in touch with us by telephone, e-mail or using a contact form, or if communication via a mobile phone number is required to use specific products, namely SMS, push notification etc., such as to send a confirmation, authentication or activation code, these messages will not be transmitted in encrypted form. For this reason, it cannot be ruled out that they may, for example, be read by unauthorized individuals or intercepted, and that third parties such as Internet or mobile network providers might infer the existence of the banking relationship or gain access to bank customer information.

Other purposes

We may process your data for other purposes as well, e.g. to aid our internal processes and administration.

Other purposes include the following:

- Administrative purposes, e.g. in order to manage master data, for accounting and data storage, to manage real estate or to test and manage IT infrastructure
- To safeguard our rights, e.g. to settle claims before, in or out of court, as well as claims brought before public authorities in Switzerland and abroad, or to defend ourselves against claims i.e. by securing evidence, for legal clarifications and participation in court or official proceedings, including proceedings brought before the Swiss Banking Ombudsman
- To evaluate and improve internal processes, including internal support in the event of enquiries
- To prepare and execute the acquisition and/or sale of companies and assets
- For analytical and statistical purposes (particularly in connection with our online services), including, for example, internal analyses for evaluating Key Performance Indicators (KPIs) and for testing purposes
- Training and educational purposes

Furthermore, we may also process your data in order to safeguard further legitimate interests which cannot be named exhaustively.

If we ask for your consent to process certain data, we will notify you separately about the reasons for doing so.

6. What rules apply to profiling and automated decision-making?

We may use an automated, i.e. computer-assisted, system when processing and analyzing (including what is known as profiling) your data (see section 4, “What data do we process?”) for the purposes outlined in section 5 (“Why do we process your data?”) in order to obtain preference data, detect misuse and security risks, perform statistical analyses or plan our future operations, for example. We may also create profiles for these same purposes. To achieve this, we combine behavioural and preference, master, order and transaction data, as well as, amongst other things, additional information about the contractual relationship and the technical data that is attributed to you, in a way that helps us develop a better understanding of you, your individual interests and your personality. This also allows us to learn more about you, the products and services you already use, as well as those that you may wish to use in future. PostFinance may use automated decision-making processes for reasons of efficiency and uniformity. We will always contact you if any of these decisions have legal implications or significantly affect you in any other way, and will take any and all measures as required by law.

In each case, we will inform you if an automated decision has legal repercussions or otherwise significantly detrimental consequences. In such instances, you may choose to invoke any of the rights described in section 12 (“What are your rights?”) should you disagree with the outcome of the decision.

7. Who do we disclose your data to?

We are bound to confidentiality not only by data protection law, but also by bank client confidentiality and other regulations. More information on this topic can be found in our General Terms and Conditions, for example. Our products and services are often developed, prepared and handled by different teams, including in particular those within our Group. This means that your data is processed by various parties including PostFinance, as well as individuals to whom you transfer money, other banks, and contracted service providers, for example. There are a number of specific risks

associated with bank transfers and payment transactions (default, fraud, money laundering, etc.), which need to be investigated by third parties, which necessitates disclosing data to them. In this context, data may be disclosed to third parties as part of processing a transaction, as well as to other entities such as agencies, public authorities, other official bodies and banks. Data may likewise be disclosed in the context of legal provisions, i.e. when we are subject to obligations to clarify, report or provide information. The entities involved in these instances are legally permitted to process your data, but may only do so within the scope of legal and/or contractual provisions.

This section explains the main instances in which data is disclosed in connection with our products, services, contracts, and statutory obligations, for the purposes described in section 5 (“Why do we process your data?”) and to safeguard other legitimate interests. Your data will be disclosed to the following types of recipients:

Service providers: we work with service providers in Switzerland and abroad (see section 8, “Do we disclose personal data abroad?”).

We procure services from third parties in a range of areas; this allows us to deliver our products and services cost-effectively, efficiently and safely, and to focus on our own core competencies. These services include IT services, information distribution, financial services, marketing, sales, communications, market research and/or printing services, as well as payment collection services, measures to counter fraud, and services provided by consultants, law firms and rating agencies.

We only disclose data that is essential in order for service providers to perform the requested services.

In conjunction with transfers abroad, we also transfer your data to the Society for Worldwide Interbank Financial Telecommunication, S.W.I.F.T. SC, Avenue Adèle 1, 1310 La Hulpe, Belgium (SWIFT). This organization processes your data as a joint controller alongside PostFinance. This allows PostFinance to send and receive financial news or files and to validate, track and manage financial transactions in advance. On SWIFT’s website, in their “Personal Data Protection Policy” (under “Data Protection Policies”), you will find the key points of the agreement upon which this joint responsibility is based. You will also find information there on how SWIFT processes your data. SWIFT may transfer your personal data outside the EEA under certain circumstances; in such cases, appropriate transfer precautions are taken to protect the data. This includes agreeing standard EU contractual clauses and taking additional technical and organizational security precautions.

Contractual partners, customers and involved parties: if you work for one of our contractual partners (e.g. a customer or supplier), we may transfer data about you to them. We also disclose personal data to creditors or individuals acting on your behalf (e.g. authorized persons) or who are otherwise involved in the performance of a contract.

If you work for a company with which we have concluded a contract or with which we have any other form of relationship, we may share any information with them that is collected as part of your work for that company. We may also share data with other entities that are involved in legal transactions, such as payment recipients, authorized persons, correspondent banks, other financial institutions, payment service providers, third-party depositories and other bodies.

Mobile payment: when you use a mobile payment-enabled card, data about the customer, device and mobile payment service provider is exchanged between ourselves, providers and card networks to facilitate card management, perform identity checks, prevent misuse and fraud, comply with legal requirements and process and display transactions. Furthermore, the provider’s terms and conditions may stipulate that they can acquire, process and disclose your data for other purposes.

Partners: if the contractual relationship includes bonus programmes or other third-party services, we may exchange data with these partners, provided this is necessary and you have given your consent for us to do so. If we provide you with products and services, we may pass your data on to a cooperation partner (see section 5, “Why do we process your data?”).

We may also share your personal data with third parties who may then process it in accordance with their own terms and conditions and also use it for marketing purposes, with your consent in each separate instance. By giving your consent, you also authorize these partners to share corresponding information with us.

Authorities and other official bodies: we may disclose personal data to agencies, courts and other public authorities or official bodies if we are legally obliged or entitled to do so or in order to protect our legitimate interests.

In certain circumstances, we share personal data with courts, public authorities, agencies and other official bodies (such as the Swiss Banking Ombudsman) in order to safeguard our rights, defend ourselves against claims and fulfil our legal obligations. We do this as part of official proceedings and those which take place either in or out of court, as well as in instances in which we are legally bound to share information and cooperate.

Other persons: data may also be disclosed to other recipients.

We may, for example, disclose data to:

- Individuals involved in legal or official proceedings
- Potential buyers of companies, receivables and other assets
- Public
- Auditors and other third parties, about whom we will inform you separately where possible (e.g. in declarations of consent or special privacy policy notices).

We are also legally obliged to disclose data to the Consumer Credit Information Office (IKO) (see also section 4, "What data do we process?"). For further information, please visit iko-info.ch. We also report to the Central Office for Credit Information (ZEK) in accordance with the relevant regulations, particularly in regard to specific cases involving instalment loans and card blocking. ZEK may make this data available to its members in the scope of loan agreements, leasing contracts and other contractual arrangements. For further information, please visit zek.ch. Your personal data may also be disclosed within the context of publishing our annual report. In this case, we will always ask for your consent.

We would also like to draw your attention to the fact that sending data via different networks involves multiple internet providers. It can therefore never be ruled out that third parties could gain access to data that is sent in this way and use it without permission. Sensitive data should consequently never be sent by e-mail, SMS or other unencrypted channels. Even when such information is transmitted via encrypted channels, data such as the sender and recipient names remain public, which means that, in some circumstances, third parties can still make deductions about existing or future business relationships.

8. Do we disclose personal data abroad?

As explained in section 7 ("Who do we disclose your data to?"), your data is processed not only by ourselves, but also by other parties where necessary. These parties are not based exclusively in Switzerland. Your data may therefore be processed worldwide, including in countries outside of the EU or the European Economic Area (third countries). We oblige our contractual partners in particular to maintain confidentiality when processing data to which we are bound by bank client confidentiality. Recipients in countries with insufficient legislation on data protection are contractually obliged to comply with data protection regulations, which is usually accomplished by inserting recognized standard contractual clauses (these can be found at <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32021D0914&qid=1687793527879>). We can choose to waive this requirement if the partner is already subject to regulations designed to ensure data protection and which are recognized in Europe, or if we can make use of an exemption clause. The latter option may particularly apply to legal proceedings outside of Switzerland, in cases of overriding public interest or where the disclosure of data in this way is required to perform the contract, if you have consented to us disclosing data or in instances involving publicly accessible data made available by you that you have not objected to being processed.

Please be aware that making transactions and performing services within Switzerland or internationally (e.g. payment transactions, trading and safekeeping of custody account assets, foreign exchange or precious

metal transactions, or derivative/OTC transactions) requires data about you and third parties to be disclosed to recipients located abroad. Data may also be disclosed to correspondent banks, particularly when processing payment orders. These recipients and their sub-processors might be located in different countries anywhere in the world. Under certain circumstances, they may not be subject to a legal duty of confidentiality and might be located outside our area of influence. We cannot rule out the possibility that authorities or third parties might access transferred data. Please also note that data exchanged via the Internet is often routed through third countries. As such, your data may be sent abroad even if the sender and recipient are located in the same country.

9. How long do we store your data for?

We store your data for as long as we are required to do so in accordance with the applicable legal provisions or to fulfil the purpose of its processing. We also take into account the need to protect our own interests (e.g. to enforce or defend against claims and to ensure IT security and for documentation and evidence purposes). We delete or anonymize your data as part of our normal processes once these purposes have been achieved and our obligation or right to retain it ceases to apply. This may take more than ten years.

It may even be necessary to retain some data from a technical standpoint as certain data elements cannot be isolated from others, meaning that we have to store them as a whole (as is the case with backup or document management systems).

10. How do we protect your data?

We take appropriate technical, organizational and legal security measures to maintain the security of your personal data, safeguard it against unauthorized or unlawful processing and protect it against the risk of loss, accidental modification, unintentional disclosure or unauthorized access. The security measures that we employ in this respect include precautions such as data encryption and pseudonymization, keeping logs, access restrictions, storing backup copies, issuing directives to our employees, confidentiality agreements and data monitoring. We use suitable encryption mechanisms to protect the information you submit via our websites, the PostFinance App and e-finance while said data is in transit. We also oblige our third parties to implement appropriate security measures in line with the state of the art. It is, however, generally impossible to fully mitigate security risks; residual risks are unavoidable.

11. Which online tracking and analysis techniques do we use?

Cookies and other technologies

Whenever you access a server online (e.g. when you use an app or website), your behaviour may be recorded using cookies and other technologies (such as software development kits, or SDKs for short, and marketing automation tools). We use technologies of this kind on our website, in e-finance and in the PostFinance App. Information on cookies and other technologies, how these are used and additional data processing in public areas on our website can be found in the privacy policy notices relating to our website, which can be accessed at postfinance.ch/dps-web. The following information relates to e-finance and the PostFinance App.

Software development kits (SDKs) are a type of technology supplied by third-party providers that enable you, for example, to gather user data within a mobile app and to transfer this data to the service provider. Whenever the PostFinance App is used, a unique code (e.g. a serial number) specific to every individual mobile device is sent to the service provider's server and is also stored on the user's mobile device. This means that you are classed as a unique visitor every time you access a site, and are identified when you log in. The marketing automation tool can record your responses to content in the publicly accessible section of our website, in e-finance and in the PostFinance App.

Use of technology for essential functions

These technologies enable us to distinguish your visits (or visits made using your system) from those made by other users, which is necessary in order for some functions within e-finance and the PostFinance App to work.

Certain cookies are used to ensure that you can switch between pages without losing any text that you have entered in a form, or for saving preferences such as language selection for future sessions. Other cookies and tools are required to ensure functions such as managing and saving settings or logging into e-finance. Blocking them may therefore prevent e-finance from working. Certain functions in the PostFinance App are restricted, or may no longer work if certain access authorizations (e.g. camera access, push notifications, biometrics etc.) are not accepted. Information stored in log files is re-used to ensure that online services are secure and continue to function (e.g. by detecting faults or fraudulent intent).

Personal evaluations in relation to the use of e-finance and the PostFinance App

We can analyze customers' behaviour on a personal level by linking the device used to log into e-finance or the PostFinance App with our encrypted customer number (user ID), and thus track the behaviour of specific, identifiable users in e-finance or the PostFinance App. As a rule, therefore, it is possible to draw personal, cross-device conclusions about your behaviour, including your behaviour in the publicly accessible section of our website, after you have logged in once. This also applies to each individual third party that you allow to use your device.

The technologies outlined above allow us to conduct personal evaluations for analytical and statistical purposes, as well as for guidance regarding which content to display. One measure we take for this purpose is to employ a service provider; details about them can be found below. We also use the corresponding analytical and statistical data for our marketing measures. The information stored in our log files is also used as part of our personal evaluations of user behaviour.

Disabling data collection

For e-finance, you can configure your browser in such a way that it blocks certain cookies and other technologies or deletes existing cookies. You can likewise use browser-based software that blocks tracking. You can also opt out of data collection in the personal settings in e-finance or the PostFinance App at any time. Deactivation applies to both e-finance and the PostFinance App and takes effect from the next login.

Instructions

PostFinance App: More → My profile → Data protection settings – Edit → right arrow (menu opens) → Data usage (settings can be chosen here for web tracking, app tracking and categorization).

E-finance: Settings and profile → My data → Data protection settings – Edit → Data usage tab (settings can be chosen here for web tracking, app tracking and categorization).

The use of information stored in our log files as part of our personal evaluations of user behaviour cannot be deactivated.

Google Analytics

We use Google Analytics. We use Google Analytics to generate usage reports for e-finance and the PostFinance App, which we do by authorizing Google to track the behaviour (visit duration, frequency of pages accessed, geographical origin of access, etc.) of visitors to e-finance, the PostFinance App and the publicly accessible section of our website. To do this, Google utilizes cookies (for e-finance and the website) and the tracking functions in the Firebase SDK (for the PostFinance App). Google Analytics is provided by Google LLC, and Google Ireland Ltd is responsible for compliance with data protection law. We have configured Google Analytics so that the IP addresses of visitors to e-finance, the PostFinance App and our website are truncated by Google in Europe before being transferred to the United States, thus making them impossible to trace. Furthermore, we do not send any information to Google that it can link to our customers. Google provides us with reports and evaluations based on the collected user data, and is our order processor in this sense. Google also processes this data to optimize its products and services. Information on how Google Analytics protects your data can be found at <https://support.google.com/analytics/answer/6004245>.

12. What rights do you have?

Under specified preconditions, you have the right to information about your personal data and its processing by us, to rectify incorrect or incomplete data and to object to our processing of your data. In certain cases, you also have the right to receive certain data in a structured, established and machine-readable format. If the processing of personal data requires your consent, you may withdraw this consent at any time. Such a withdrawal applies only with regard to future processing.

If we make a decision that affects you by means of an automated process and this results in a legal impact on you or otherwise has a significant effect on you, you have the right to speak to a person responsible for these matters at our company and to request that they reconsider the decision. If such an event occurs, we will contact you separately.

Should you wish to exercise your rights concerning us, please send us a signed letter (see section 3, "Who is responsible for processing your data?") and a clearly legible copy of your identity document to allow us to identify you and to prevent misuse. You can revoke consent by other means, provided we give them as an option (e.g. under "Settings and profile" in e-finance).

13. Can this Privacy Policy be amended?

We reserve the right to amend this Privacy Policy at any time. The version published at postfinance.ch/dps is the currently valid version.

Last updated: February 2024