General privacy policy of St.Galler Kantonalbank AG

1. What is this privacy policy about?

St.Galler Kantonalbank AG (hereinafter "SGKB" or "we") obtains and processes personal data relating to you or other persons (referred to as "third parties").

Personal data" refers to information that relates to a specific or identifiable person, i.e. conclusions about their identity are possible on the basis of the data itself or with corresponding additional data. "**Particularly sensitive personal data**" is a category of personal data that is specially protected by the applicable data protection law. Personal data requiring special protection includes e.g. health data, data revealing racial or ethnic origin, data concerning religious or philosophical beliefs, biometric data for identification purposes and data concerning trade union membership. In Section 3, you will find details of the data that we process within the scope of this data protection declaration. "**Processing**" means any handling of personal data, e.g. obtaining, storing, using, adapting, disclosing and deleting.

We use the term "data" in our General Privacy Policy synonymously with "personal data" or "personal information".

In this Privacy Policy, we describe how we process your data when you visit our **website** (www.sgkb.ch), subscribe to a **newsletter**, obtain our **services or products**, otherwise interact with us under a contract, **communicate** with us (including through Microsoft Teams) or otherwise deal with us. We also inform you separately about specific data processing, e.g. in specific data protection statements, terms of use, declarations of consent, forms and notices.

For the following groups of persons and data processing, you will find a summary of the most important information at www.sgkb.ch/datenschutz:

- Clients and persons associated with them
- Interested parties and potential clients
- Shareholders
- Users of our website and our newsletter
- Suppliers and partners
- Video surveillance

Our data processing operations concern the following **persons** in particular:

- Current and former clients and persons associated with them, such as additional account and cardholders, authorised representatives (e.g. authorised persons, authorised signatories, provident representatives), beneficial owners, control holders or heirs
- Interested parties and potential clients
- Persons to whom we provide products and services or whom we advise
- Shareholders and investors
- Participants in competitions, surveys, customer events and other events
- Users of our website and our newsletter
- Visitors to our premises
- Users of our ATMs
- Suppliers and partners and their contacts
- Representatives of authorities, agencies and other bodies

If you provide us with data about other people (e.g. family members, authorised representatives), we assume that you are authorised to do so and that these data are correct. By submitting data via third parties, you confirm this. Please ensure that these third parties have been informed of this privacy policy.

This Privacy Policy is designed to comply with the requirements of the EU General Data Protection Regulation ("GDPR"), the Swiss Data Protection Act ("DPA") and the revised Swiss Data Protection Act ("revDPA"). However, whether and to what extent these laws are applicable depends on the individual case.

2. Who is responsible for processing your data?

St.Galler Kantonalbank AG (CHE-105.845.146) is responsible for the data processing described in this data protection declaration, unless otherwise communicated in individual cases.

In particular, SGKB is jointly responsible with other bodies for data processing in the following case:

- SGKB is jointly responsible with the St. Galler Kantonalbank (CHE-109.509.434) for the processing of personal data in connection with services and products of the Pension Savings "Sparen 3".

You can contact us for your data protection concerns and to exercise your rights under section 14 as follows:

St.Galler Kantonalbank AG, Data Protection Office, St. Leonhardstrasse 25, 9001 St. Gallen
E-mail: datenschutz@sgkb.ch

We have established the following additional posts:

▪ **Data Protection Officer** pursuant to Art. 37 et seq. GDPR:	St.Galler Kantonalbank AG Data protection office St. Leonhardstrasse 25 9001 St. Gallen E-mail: datenschutz@sgkb.ch
▪ **Data protection representative in the EU** pursuant to Art. 27 GDPR:	Swiss Infosec (Deutschland) GmbH Unter den Linden 24 10117 Berlin / Germany E-mail: sgkb.dataprivacy@swissinfosec.de

3. What data do we process?

We process different categories of data about you depending on the situation and purpose and based on the products and services you use. The main categories are as follows:

- **Master data**: We define master data as the basic data that we need, along with other data, for the processing of our contractual and other business relationships or for marketing and advertising purposes, such as name, contact details and information about your role and function, for example. We process your master data if you are a client or other business contact or work for one (e.g. as a contact person of the business partner), or because we want to address you for our own purposes or the purposes of a contractual partner (e.g. as part of marketing and advertising, with invitations to events, with newsletters, etc.). We receive master data from you yourself (e.g. as part of the business relationship), from bodies for which you work or from third parties such as our contractual partners, associations and address dealers and from publicly accessible sources such as public registers or the Internet (websites, social media, etc.). We may also process health data and information about third parties as part of master data. We can also collect master data from our shareholders and investors. We generally keep these data for 10 years from the last exchange with you, but at least from the end of the contract. This period may be longer insofar as this is necessary for reasons of proof or to comply with legal or contractual requirements or for technical reasons. For pure marketing and advertising contacts, the period is usually much shorter, usually no more than 2 years since the last contact.

  Master data includes **identification data** such as name, date of birth, gender, social security number, tax number, nationality, photographs, specimen signatures, copies of identification documents; **contact data** such as address, email address, telephone number; information about your relationship with us (client, supplier, etc.); **tax data** such as tax number, tax domicile and information in connection with the Automatic Exchange of Information (AEOI), Foreign Account Tax Compliance Act (FATCA) and Qualified Intermediary Agreement (QI Agreement); information on your **personal circumstances** such as marital status, family relationships, occupation, employer, qualifications, interests and hobbies; information on

your **financial circumstances** such as income, assets and debts; furthermore, reports or official documents (e.g. extracts from the commercial register).

With respect to contact persons and representatives of our clients, suppliers and partners, we process as master data, e.g. name, address and date of birth, details of role, function in the company, qualifications and, where applicable, details of supervisors, employees and subordinates and details of interactions with these persons.

Master data is not comprehensively collected for all contacts. Which data we collect specifically will depend in particular on the purpose of the processing.

- **Contract data**: This is data that arises in connection with the conclusion or processing of a contract, e.g. information about contracts and the services to be provided or provided, as well as data from the run-up to the conclusion of a contract, the information required or used for processing, and information about reactions (e.g. complaints or information on satisfaction, etc.). This also includes health data and information about third parties. We generally collect these data from you, from contractual partners and from third parties involved in the processing of the contract, but also from third party sources (e.g. credit agencies) and from publicly accessible sources (e.g. a commercial register). We generally keep these data for 10 years from the last contract activity, or from the end of the contract. This period may be longer insofar as this is necessary for reasons of proof or to comply with legal or contractual requirements or for technical reasons.

  Contractual data include **general data on the business relationship**, such as information on the conclusion of the contract, on your contracts, e.g. the nature and date of the contract, information from the application process (such as an application for our products or services) and information about the contract in question (e.g. its duration) and the processing and administration of the contracts (e.g. information related to invoicing and the enforcement of contractual claims), information on allocations and classifications (e.g. customer segment) as well as information on complaints and customer satisfaction. Contractual data also include **product and service-related data** such as account and deposit numbers, information on individual orders and transactions (e.g. incoming and outgoing payments, card payments, securities information), card details (e.g. limits), information on your risk and investment profile as well as your knowledge and experience in connection with financial products, information on loans (e.g. amount, term, collateral).

- **Behavioural and preference data**: Depending on the relationship we have with you, we try to get to know you and better tailor our products, services and offers to your needs. To do this, we collect and use data about your behaviour and preferences. We do this by analysing information about your behaviour in our area, and we may also supplement this information with information from third parties, including publicly available sources. Based on this, we can calculate, for example, the probability that you will use certain services or behave in a certain way. The data processed for this purpose is partly already known to us (e.g. when you use our services) or we obtain these data by recording your behaviour (e.g. how you navigate our website or use our apps). We anonymise or delete these data when they are no longer meaningful for the purposes pursued, which may be after four years (for product and service preferences) depending on the nature of the data. This period may be longer insofar as this is necessary for reasons of proof or to comply with legal or contractual requirements or for technical reasons. We describe how tracking works on our website in Section 12.

  Behavioural data is information about certain actions, such as your response to electronic communications (e.g. whether and when you opened an email) or your location, as well as your interaction with our social media profiles and your participation in prize draws, competitions and similar events. For example, we may collect your location data wirelessly through unique codes sent by your mobile phone or when you use our website.

  Preference data tell us what your needs are, what products or services might be of interest to you, or when and how you are likely to respond to messages from us. We obtain this information from the analysis of existing data, such as behavioural data so that we can get to know you better, tailor our advice and offers more precisely to you and generally improve our offers. To improve the quality of our analyses, we may combine these data with other data that we also obtain from third parties such as address dealers, public offices and publicly accessible sources such as the Internet, e.g. with information on your household size, income class and purchasing power, shopping behaviour and contact details of relatives and anonymous information from statistical offices.

Behavioural and preference data can be evaluated on a personal basis (e.g. to show you personalised advertising), but also on a non-personal basis (e.g. for market research or product development). Behavioural and preference data can also be combined with other data.

- **Communication data**: If you are in contact with us using the contact form, by email, telephone or chat, by letter or by any other means of communication, we collect the data exchanged between you and us, including your contact details and the metadata of the communication. If we record or listen in on telephone conversations or video conferences, e.g. for training and quality assurance purposes, we will specifically draw your attention to this unless the recording is required to comply with legal requirements. Such records may only be made and used in accordance with our internal guidelines. If we want or need to establish your identity, e.g. in the case of a request for information submitted by you, a request for media access, etc., we collect data to identify you (e.g. a copy of an ID). We usually keep these data for 24 months from the last communication with you. This period may be longer insofar as this is necessary for reasons of proof or to comply with legal or contractual requirements or for technical reasons. E-mails in personal mailboxes and written correspondence are generally kept for at least 10 years. Records of chats are usually kept for 24 months.

  Communication data comprise your name and contact details, the place, time and methods of communication and usually also its content (i.e. the content of emails, letters, chats, telephone conversations etc.). These data may also contain information about third parties. For identification purposes, we may also process your ID number or a password you have set or your ID card. Information about the use of an electronic infrastructure is known as metadata. Metadata provide information about who was in contact with whom, when, how and from where.

- **Technical data**: When you use our electronic offers (e.g. e-banking, mobile banking) or our website, we collect the IP address of your terminal device and other technical data to ensure the functionality and security of these offers. These data also include logs recording the use of our systems. We usually keep technical data for 24 to 48 months. To ensure the functionality of these offers, we may also assign an individual code to you or your end device (e.g. in the form of a cookie, see section 12). Technical data as such do not allow any conclusions to be drawn about your identity. However, in the context of user accounts, registrations, access controls or the processing of contracts, they may be linked to other categories of data (and thus possibly to your person).

  Technical data include, among other things, the IP address and information about the operating system and language of your terminal device, the date, region and time of use as well as the type of browser with which you access our electronic offers. This can help us to submit the correct formatting of the website or show you a website adapted for your region, for example. Based on the IP address, we know which provider you use to access our offers (and thus also the region), but we cannot usually deduce who you are from this. This changes when you create a user account, for example, because personal data can then be linked to technical data (e.g. we can see which browser you use to access an account via our website). Examples of technical data include logs generated by our systems (e.g. the log of user logins to our website).

- **Registration data:** Certain offers, e.g. of competitions and services (e.g. login areas of our website, newsletter dispatch etc.) can only be used with a user account or registration, which can be completed directly with us or using our external login service providers. In doing so, you must provide us with certain data and we collect data about the use of the offer or service. Access controls to certain facilities may generate registration data; depending on the control system, biometric data may also be generated. We generally retain registration data for 12 months after the end of the use of the service or the termination of the user account.

  Registration data include, but are not limited to, the information you provide when you create an account on our website (e.g. Username, password, name, email). However, the registration data also include the data that we may require from you before you can make use of certain free services. You also need to register if you want to subscribe to our newsletter. In the context of access controls, we may have to register you with your data (access codes in badges, biometric data for identification) (cf. the category "other data").

- **Other data**: We also collect data from you in other situations. In connection with official or judicial proceedings, for example, data are generated (such as files, evidence, etc.) that may also relate to you. We may also collect data for health protection

reasons (e.g. within the framework of protection concepts). We may receive or produce photographs, videos and audio recordings in which you may be identifiable (e.g. at events, by security cameras etc.). We may also collect data on who enters certain buildings and when, or has access rights to certain buildings (including access control, registration data, visitor lists, etc.), who participates in events or activities (e.g., events in the city), and who participates in events or activities (e.g. competitions) or who uses our infrastructure and systems and when. Finally, we collect and process data on our shareholders and other investors; in addition to master data, these include information for the relevant registers, regarding the exercise of their rights and the holding of events (e.g. general meetings). The retention period for these data depends on the purpose and is limited to what is necessary. This ranges from a few weeks for security cameras to reports on occasions with images that can be kept for a few years or longer. Data about you as a shareholder or other investor will be kept in accordance with company law, but in any case for as long as you are invested.

4. Where do your data come from?

You provide us with much of the data mentioned in section 3 yourself (e.g. via forms, in the course of communication with us, in connection with contracts, when using the website, etc.). You are not obliged to do so, except in individual cases, e.g. within the framework of binding protection concepts (legal obligations). If you wish to conclude contracts with us or claim services, you must also provide us with data, in particular, master data, contract data and registration data, as part of your contractual obligation under the relevant contract or on the basis of statutory provisions which the Bank must observe. When using our website, the processing of technical data is unavoidable. If you wish to gain access to certain systems or buildings, you will need to provide us with registration details. However, in the case of behavioural and preference data, you generally have the option of objecting or not giving consent.

We only provide certain services to you if you provide us with registration data because we or our contractual partners want to know who is using our services or who has accepted an invitation to an event, because it is technically necessary, or because we want to communicate with you. If you or a person you represent (e.g. your employer), wants to enter into or implement a contract with us, we need to collect relevant master, contract and communication data from you, and we process technical data if you want to use our website or other electronic offers for this purpose. If you do not provide us with the data required for the conclusion and performance of the contract, we may refuse to conclude the contract, you may be in breach of contract, or we may not be able to honour the contract. Similarly, we can only send you a response to a request from you if we process the relevant communication data and where applicable, technical data, if you communicate with us online. The use of our website is also not possible without us receiving technical data.

Insofar as this is not inadmissible, we also extract data from publicly accessible sources (e.g. enforced payment collection registers, land registry, commercial registers, sanctions and embargo lists, the media or the internet including social media) or receive data from other companies within our group, from authorities and from other third parties (e.g. credit agencies, address dealers, associations, contractual partners, internet analysis services, etc.).

We receive data provided to us by third parties for the purpose of executing orders, fulfilling contracts or with your consent, such as third-party banks, operators of settlement systems, pension schemes, pension and vested benefits foundations, insurance companies, land registry offices, debt enforcement and bankruptcy offices, the Central Office for Credit Information (ZEK), the Consumer Credit Information Office (IKO), power of attorney providers, representatives of heirs, card issuers, pension foundations, Swiss Post, cashgate. We also receive data from official bodies and authorities which are communicated to us on the basis of their activities, e.g. from courts, child and adult protection authorities and public prosecutors' offices.

The categories of personal data that we receive about you from third parties include, in particular, information from public registers, information that we obtain in connection with official and legal proceedings, information in connection with your professional functions and activities (so that we can, for example, conclude and process transactions with your employer with your help), information about you in correspondence and meetings with third parties, creditworthiness information (insofar as we conduct business with you personally), information about you arising from correspondence and meetings with third parties, creditworthiness information (insofar as we process transactions with you personally), information about you provided by people close to you (family, advisors, legal representatives, etc.) allowing us to conclude or process contracts with you or with the involvement of you (e.g. references, your address for deliveries, powers of attorney, details of compliance with legal requirements such as anti-fraud, anti-money laundering, anti-terrorism and export restrictions, details of banks, insurance companies and distributors and other contractual partners of ours for the use or provision of services by you (e.g. payments, purchases, etc.), personal data from the media and Internet (if this

is appropriate in a specific case, e.g. in the context of an application, marketing/sales, press review, etc.), your address and, if applicable, interests and other socio-demographic data (especially for marketing and research) and data in connection with the use of third-party websites and online offers where this use can be attributed to you.

5. For what purposes do we process your data?

We process your data for the purposes we explain below. Further instructions for the online area can be found in Sections 12 and 13.

- **Establishment, management and settlement of business or contractual relationships**: We process your data for the purpose of establishing, managing, processing and terminating business or contractual relationships. The type of data processed varies according to the type and scope of the relationship and the nature of the products and services used and may include, in particular, master data, contract data, communication data and registration data.

  We enter into a wide variety of contracts with our clients, suppliers, subcontractors or other contractual partners, e.g. partners in projects or with parties in legal disputes. In particular, we process master data, contract data and communication data and, depending on the circumstances, also registration data of the client or the persons to whom the client provides a service.
  In the course of initiating business, personal data, in particular master data, contract data and communication data, are collected from potential clients or other contractual partners (e.g. in an application form or contract) or result from a communication. In some cases, this information is checked for compliance with legal requirements.

  As part of the processing of contractual relationships, we process data for the administration of the customer relationship, for the provision and collection of contractual services (which also includes the involvement of third parties, such as logistics companies, security services, advertising service providers, banks, insurance companies or credit reference agencies, which may then in turn provide us with data), for advice and for customer care. The enforcement of legal claims arising from contracts (debt collection, court proceedings, etc.) is also part of the processing, as are accounting, termination of contracts and public communication.

  Furthermore, we also process data, in particular, master and contract data, when computers are used on our website (e.g. mortgage or pension calculator) as well as in connection with the brokerage of third-party products and services, e.g. insurance, retirement accounts, personal loans, credit cards and travel funds. Such products and services may be offered via our infrastructure or by our employees, but may be executed and processed in whole or in part by third parties. In this case, the respective third party, if applicable together with SGKB, is responsible for processing the data.

- **Adherence to laws, directives and recommendations of authorities as well as internal regulations ("Compliance")**: We further process your data to comply with laws, directives and recommendations from authorities and internal regulations ("Compliance"). Processed data include, in particular, your master data, contract data, communication data and behavioural data.

  These include, for example, the legally regulated fight against money laundering and the financing of terrorism. In certain cases, we may be obliged to make certain inquiries about clients ("Know Your Customer") or to report to the authorities. The fulfilment of obligations to provide information or to report, for example in connection with supervisory and tax obligations, also requires or entails data processing, e.g. the fulfilment of archiving obligations and the prevention, detection and clarification of criminal offences and other violations. This includes receiving and processing complaints and other reports, monitoring communications, conducting internal investigations or disclosing records to a government agency if we have reasonable cause or are legally required to do so. Your personal data may also be processed in the course of external investigations, e.g. by a law enforcement or supervisory authority or a mandated private body. We also process data in order to serve our shareholders and other investors and to fulfil our obligations in this regard. For all these purposes, we process in particular your master data, your contract data and communication data, but in some circumstances also behavioural data and data from the category of other data. The legal obligations may arise from Swiss law, but also foreign laws and regulations to which we are subject, as well as self-regulations, industry standards, our own "corporate governance" and official instructions and requests.

- **Risk management and prudent corporate governance**: We also process your data for the purposes of our risk management, fraud prevention and as part of prudent business management, including operational organisation and business development. The data processed include, in particular, master data, contract data, communication data, behavioural data and registration data, but also technical data.

  For example, we need to monitor our debtors and creditors as part of our financial management, and we need to avoid falling victim to crime and abuse, which may require us to analyse data for patterns. We may also carry out profiling and create and process profiles for these purposes and to protect you and us from tortious or abusive activities (see also section 7). In the context of planning our resources and organising our operations, we need to evaluate and process data on the use of our services and other offers or exchange information on this with others (e.g. outsourcing partners), which may include your data. The same applies to services rendered to us by third parties. As part of our business development, we may sell or acquire businesses, operations or companies to others or enter into partnerships, which may also result in the exchange and processing of data (including from you, e.g. as a client or supplier or as a supplier representative).

- **Marketing activities and relationship building**: We process data for marketing purposes and to maintain relationships, e.g. in order to provide our clients and other contractual partners with personalised recommendations and offers for products and services from us and from third parties (e.g. cooperation partners). This may be, for example, in the form of newsletters and other regular contacts (electronically, by post, by telephone), via other channels for which we have contact information from you, but also as part of individual marketing campaigns (e.g. events, competitions, etc.) and sponsoring. You can refuse such contacts at any time or refuse or revoke consent to be contacted for advertising purposes. The data processed include in particular master data, contract data, behavioural data and preference data.

  For example, with your consent, we may send you information, advertising and product offers from us and from third parties, in print, electronically or by telephone. Like most businesses, we personalise communications so that we can provide you with personalised information and offers that meet your needs and interests. For this purpose, we link data that we process about you and determine preference data and use these data as the basis for personalisation (see section 3). We also process data in connection with competitions, prize draws and similar events.

  Relationship management also includes addressing existing clients and their contacts, possibly personalised on the basis of behavioural and preference data. As part of our relationship management, we also operate a customer relationship management system ("CRM") in which we store the data on clients, suppliers and other business partners required for the relationship management, e.g. on contact persons, relationship history (e.g. on products and services purchased or supplied, interactions, etc.), interests, wishes, marketing measures (newsletters, invitations to events, etc.) and other information.

- **Market research, improvement of services and operations, and product development**: We continue to process your data for market research, to improve our services and operations and for product development. The data processed include in particular master data, contract data, behavioural data and preference data, as well as information from customer surveys, polls and studies.

  We strive to continuously improve our products and services (incl. our website and our newsletters) and to be able to react quickly to changing needs. We therefore analyse, for example, how you navigate through our website or electronic offers (e. g. e-banking, mobile banking), when you open our newsletter and what content you click on, or which products are used by which groups of people and in what way, and how new products and services can be designed (for further details see section 12). This gives us an indication of the market acceptance of existing products and services and the market potential of new ones. As far as possible, we use pseudonymised or anonymised data for these purposes.

- **Security purposes and access control**: We then also process your data for security and access control purposes. The data processed include master data, registration data, behavioural data, technical data and other data.

  We continuously review and improve the appropriate security of our IT and other infrastructure (e.g. buildings). We therefore process data, for example, for monitoring, controls, analyses and tests of our networks and IT infrastructures, for sys-

tem and error checks, for documentation purposes and as part of security copies. Access controls include not only the control of access to electronic systems (e.g. logging into user accounts), but also physical access control (e.g. building access). For security purposes (preventive and incident investigation), we also keep access logs or visitor lists and implement surveillance systems (e.g. security cameras). We draw your attention to surveillance systems at the relevant locations identified by appropriate signs.

- **Communication**: We also process your data in connection with communication with you, in particular to answer enquiries and assert your rights (section 14) and to contact you in the event of queries. For this purpose, we use in particular communication and master data and, in connection with offers and services used by you, also registration data. We retain these data to document our communication with you, for training purposes, quality assurance and for future reference.

  This can be for any purpose where you and we communicate, whether in customer service or consultation, authentication in the event of use of the website or for training and quality assurance (e.g. in the area of customer service). We further process communication data so that we can communicate with you by email and telephone, as well as messenger services, chat, social media, letter and fax. Communication with you is usually in connection with other processing purposes, e.g. so that we can provide services or respond to a request for information. Our data processing also serves as proof of the communication and its contents.

  For communication and collaboration (e.g. for meetings, counselling sessions, telephone and/or video conferences, online presentations and/or training), we also use **Microsoft Teams**, which is provided by the Microsoft Group. In doing so, Microsoft uses certain data, in particular technical data to optimise or improve its own services (e.g. for the technical optimisation of the conference system) and to combat cybercrime and attacks as an independent responsible party. Microsoft's privacy policy can be found at https://privacy.microsoft.com/de-de/privacystatement.

- **Other purposes**: We may process your data for other purposes, e.g. as part of our internal processes and administration or for training and quality assurance purposes.

  These other purposes include, e.g. training and educational purposes, administrative purposes (such as master data management, accounting and data archiving, and the testing, management and ongoing improvement of IT infrastructure), the protection of our rights (e.g. to enforce claims in or out of court and before authorities at home and abroad, or to defend ourselves against claims, for example, by preserving evidence, legal clarifications and participation in court or official proceedings) and the evaluation and improvement of internal processes. We may use recordings of (video) conferences for training and quality assurance purposes. The protection of other legitimate interests is also one of the other purposes that cannot be named exhaustively.

6. On what basis do we process your data?

If we ask you for your **consent** for certain processing, we will inform you separately about the corresponding purposes of the processing. You can revoke your consent at any time with future effect by notifying us in writing (by post) or, where not otherwise stated or agreed, by e-mail; you will find our contact details in section 2. Once we have received notification of the withdrawal of your consent, we will no longer process your data for the purposes to which you originally consented, unless we have another legal basis for doing so. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

Where we do not ask for your consent for processing, we base the processing of your personal data on the fact that the processing is necessary for the **initiation or execution of a contract** with you (or the entity you represent) or that we or third parties have a **legitimate interest in** doing so, so in particular to pursue the purposes and related objectives described above under section 5 and to be able to implement appropriate measures. Our legitimate interests also include compliance with **legal regulations**, insofar as these are not already recognised as a legal basis by the respective applicable data protection law (e.g. in the case of the GDPR, the law in the EEA and Switzerland). But this also includes the marketing of our products and services, the interest in better understanding our markets and in managing and developing our business, including operations, safely and efficiently.

As a bank, we are subject to various legal, professional and supervisory requirements, in particular the Banking Act (BankG), the Financial Market Supervision Act (FinfraG), the Financial Services Act (FIDLEG), the Collective Investment Schemes Act (KAG), the Anti-Money Laundering Act (AMLA), the Automatic Exchange of Information Act (AIAG), circulars of the Swiss Financial Market Supervisory Authority (FINMA), guidelines of the Swiss Bankers Association (SBVg) and requirements of the Swiss National Bank (SNB). The obligations include, for example, credit checks, identity checks, fraud and money laundering prevention, the fulfilment of reporting obligations under tax law and the assessment and management of risks.

When we receive sensitive data (e.g. health data, information on political, religious or ideological views or biometric data for identification purposes), we may also process your data on the basis of other legal grounds, e.g. in the event of disputes due to the necessity of processing for a possible lawsuit or the enforcement or defence of **legal claims**. In individual cases, other legal grounds may come into play, which we will communicate to you separately where necessary.

7. What applies to profiling and automated individual decisions?

We may automatically evaluate ("profile") certain of your personal characteristics for the purposes mentioned in section 4 using your data (section 3), if we want to determine preference data, but also to determine risks of abuse and security, to carry out statistical evaluations or for operational planning purposes. For the same purposes, we may also create profiles, i.e. we may combine behavioural and preference data, but also master and contract data and technical data assigned to you, in order to better understand you as a person with your different interests and other characteristics.

If you are a client of ours, we can use "profiling", for example, to determine which other products and services are likely to interest you. An automated analysis of data can also check, for your protection, the likelihood of a particular transaction being fraudulent. This allows us to stop the transaction for clarification. When using the Financial Assistant (PFM), your transactions are allocated to specific expenditure and revenue categories automatically or according to criteria you specify. A distinction must be made between these and "profiles". The latter refer to the linking of different data in order to gain clues about essential aspects of your personality (e.g. what you like or how you behave in certain situations) from the totality of these data. Profiles can also be used for marketing, for example, but also for security purposes.

In certain situations, it may be necessary for reasons of efficiency and consistency of decision-making processes that we automate discretionary decisions affecting you with legal effects or possibly significant disadvantages ("automated individual decisions"). We will inform you accordingly in this case and provide for the measures required under applicable law.

We will inform you in each individual case if an automated decision leads to negative legal consequences or a comparable significant impairment for you. If you disagree with the outcome of such a decision, you will be able to communicate about it with someone who will review the decision.

8. Who do we disclose your data to?

In connection with our contracts, the website, our services and products, our legal obligations or otherwise to protect our legitimate interests and the other purposes listed in Section 5, we also transfer your personal data to third parties, in particular, to the following categories of recipients:

- **Service provider**: We work with service providers in Germany and abroad who process data about you on our behalf or in joint responsibility with us or who receive data about you from us in their own responsibility (e.g. IT providers, shipping companies, advertising service providers, security companies, banks, insurance companies, debt collection companies, credit agencies or address checkers).

  We procure services from third parties in various areas so that we can deliver our products and services efficiently and concentrate on our core competencies. These services concern, for example, IT services, the mailing of information, marketing, sales, communication or printing services, building security, debt collection, credit agencies, address checkers, real estate valuations, anti-fraud measures and services provided by consulting firms and law firms. We disclose to these service providers the data required for their services, which may also concern you. In addition, we conclude contracts with

these service providers that include provisions for the protection of data, insofar as such protection does not result from the law.

- **Contractual partners as well as bodies and persons involved**: We will also share your information with people acting on your behalf (e.g. agents, external asset managers) or who are otherwise involved in the settlement of a contract. If you work for one of our contractual partners (e.g. a client or supplier), we may also transfer data about you to them.

  If we have a contract or other relationship with a company you work for, we may transfer data about you to that company in connection with your work for that company. We may also transfer data to other entities involved in legal transactions, e.g. recipients of a payment, agents, correspondent banks, other financial institutions, payment service providers (including mobile payment service providers), third-party custodians, stock exchanges and trading platforms, brokers and counterparties, pension funds, insurance companies, share registers and other entities.

- **Partners**: We pass on your data to our partners if we provide you with products and services or if the contractual relationship includes bonus programmes or other third-party services. These third parties may process the transferred data jointly with us or as independent data controllers for their own legitimate interests or for the provision of services. The third parties provide information about their independent data processing in their own data protection statements.

  Such partners include, in particular, payment card issuers (Swiss Bankers, Viseca), TWINT, providers of personal loans (cashgate), vested benefits foundations (Swisscanto), pension foundations (Pension Foundation Sparen 3 of St. Galler Kantonalbank AG), pension schemes and insurance companies (e.g. Swisscanto, Mobiliar).

- **Authorities and other official bodies**: We may disclose personal data to offices, courts and other authorities, as well as other official bodies (e.g. the Swiss Banking Ombudsman) in Switzerland and abroad if we are legally obliged or entitled to do so, or if this appears necessary to protect our interests.

  Use cases include, for example, criminal investigations, police measures, supervisory requirements and investigations, judicial proceedings, reporting obligations and pre- and extra-judicial proceedings, as well as statutory obligations to provide information and to cooperate. Data may also be disclosed if we want to obtain information from public bodies, e.g. to justify an interest in information or because we need to say who we need information about (e.g. from a register). Such authorities and agencies include the Swiss Financial Market Supervisory Authority (FINMA), the Swiss National Bank (SNB), the Money Laundering Reporting Office Switzerland (MROS), courts, public prosecutors' offices, child and adult protection authorities, tax authorities, bankruptcy and debt collection offices.

  Clients domiciled in Germany are advised that SGKB will also forward suspicious activity reports regarding money laundering and terrorist financing from clients domiciled in Germany to the Money Laundering Reporting Office Switzerland (MROS), which only constitute a predicate offence to money laundering under German law.

- **Other persons**: We may also disclose personal data to other recipients if we are obliged or entitled to do so.

  Other recipients are, for example, persons involved in official or court proceedings, as well as auditing and review companies. When publishing content (e.g. photos, interviews, quotes, etc.), for example, on the website or in other publications by us, you may also be affected by this under certain circumstances. As part of our business development, we may sell or acquire businesses, operations, assets or companies, or enter into partnerships, which may also result in the disclosure of information (including information about you, for example, as a client or supplier or as a supplier's agent) to the persons involved in these transactions. The Central Office for Credit Information (ZEK) and the Consumer Credit Information Office (IKO) are also possible recipients of the data.

All these categories of recipients may in turn involve third parties, so that your data may also become accessible to them. We can restrict processing by certain third parties (e.g. IT providers), but not by other third parties (e.g. authorities, banks, etc.).

9. Does your personal data also end up abroad?

As explained in Section 8, we also disclose data to other bodies. These data are not located solely in Switzerland. Your data may therefore be processed worldwide, including outside the European Union (EU) or the European Economic Area (EEA). If a recipient is located in a country without adequate data protection legislation, we contractually oblige the recipient to comply with the applicable data protection legislation, usually by entering into recognised standard contractual clauses. This may be waived if the recipient is already subject to a legally recognised set of rules to ensure data protection, or if we can rely on an exemption clause. An exception may apply in particular in the case of legal proceedings abroad, but also in cases of overriding public interests or if the execution of a contract requires such disclosure (e.g. for the processing of payments and securities transactions), if you have given your consent (e.g. requests for information from foreign financial market supervisory authorities and securities issuers) or if it is a matter of data that you have made generally accessible and you have not objected to its processing.

In connection with the transmission of data in international payment transactions and investments in foreign securities, we also refer you to the relevant circular from the Swiss Bankers Association (SBA) of February 2016.

Please also note that data exchanged via the internet is often routed through third countries. Your data can therefore end up abroad even if the sender and recipient are in the same country.

10. How long do we process your data for?

We process your data for as long as required for our processing purposes, to comply with statutory retention periods and our legitimate interests in processing for documentation and evidence purposes, or as long as storage is technically necessary. Further information on the respective storage and processing period can be found in the individual data categories in Section 3 or in the cookie categories in Section 12. In the absence of any legal or contractual obligations to the contrary, we will delete or anonymise your data after the storage or processing period has expired as part of our normal processes.

Documentation and evidence purposes include our interest in documenting processes, interactions and other facts in the event of legal claims, discrepancies, IT and infrastructure security purposes and evidence of good corporate governance and compliance. For technical reasons, storage may be necessary if certain data cannot be separated from other data, and we therefore have to store them together (e.g. in the case of backups or document management systems).

11. How do we protect your data?

We take reasonable security measures to maintain the confidentiality, integrity and availability of your personal data, to protect it against unauthorised or unlawful processing and to protect against the risks of loss, accidental alteration, unauthorised disclosure or access.

Technical and organisational measures may include, for example, measures such as the encryption and pseudonymisation of data, logging, access restrictions, the storage of backup copies, instructions to our employees, confidentiality agreements and controls. We protect your data transmitted via our website in transit using suitable encryption mechanisms. However, we can only secure areas that we control. We also oblige our processors to take appropriate technical and organisational measures. Security risks cannot be completely ruled out, however, and residual risks are unavoidable.

12. Do we use online tracking?

On our website, in e-banking and in the mobile app (mobile banking), we use various technologies that enable us to recognise you when you use them and, in some circumstances, to track you across multiple visits. In this section we inform you about it.

In essence, it is about us being able to differentiate access by you (via your system) from access by other users, so that we can ensure the functionality of the website, in e-banking and in the mobile app and can carry out evaluations and personalisation. The technologies used are designed in such a way that you are recognised as an individual visitor each time you access the site, for example by our server (or the servers of third parties) assigning you or your browser a specific recognition number (referred to collectively as "cookies").

Cookies are individual codes (e.g. a serial number) which our server or a server of our service providers or advertising contractors transmits to your system when you connect to our website and which your system (browser, mobile) accepts and stores until the programmed expiry time. With every further access, your system transmits these codes to our server or the server of the third party. Therefore you will be recognised even if your identity is unknown.

Other technologies may also be used to make you more or less likely to be recognised (i.e. distinguished from other users), e.g. "fingerprinting". Fingerprinting combines your IP address, the browser you use, screen resolution, language choice and other details your system tells each server), resulting in a more or less unique fingerprint. This means that cookies can be dispensed with.

Whenever you access a server (e.g. when using a website or an app or because an image is visibly or invisibly integrated in an email), your visits can therefore be "tracked" (traced). If we integrate offers from an advertising contractor or analytics tool provider on our website, they may track you in the same way, even if you cannot be identified in individual cases.

We use such techniques on our website, in e-banking and in the mobile app. However, depending on the purpose of these techniques, we ask for your consent before they are used. You can configure the settings of your browser to block or reject certain cookies or to delete existing cookies. You can also enhance your browser with software that blocks tracking by certain third parties. You will find further information on this on the help pages of your browser (usually under the keyword "Data protection").

A distinction is made between the following cookies (techniques with comparable functions such as fingerprinting are included here):

- **Necessary cookies**: Some cookies are necessary for the functioning of the website as such or certain functions. For example, they ensure that you can switch between pages without losing information entered in a form. They also make sure you stay logged in. These cookies only exist temporarily ("session cookies"). If you block them, the website may not work. Other cookies are necessary to allow the server to save decisions or entries you made in a session (i.e. a visit to the website) if you request this function (e.g. language selected, consent given, the automatic login feature, etc.). These cookies have different expiry dates.

- **Analytics cookies**: To optimise our website and corresponding offers and to better adapt them to the needs of the users, we use cookies to record and analyse the use of our website, possibly also beyond the session. You can revoke this at any time by deleting the session cookie (_cfy_cc) in your browser.

Name	Cookie type	Portal	Storage period	Function
AL_SESS	Necessary	Website e-banking	Session	Cookie for storing the actions of a user. It helps to recognise a user and does not contain any personal data.
_pk_ (several)	Analytic	Website e-banking	6-13 months	Matomo cookies to distinguish users & optimise usability
CLX_EB_LOGIN (several)	Necessary	E-Banking	90 days	Saves default settings within the e-banking applications
EB_DESKTOP_LOGIN	Necessary	E-Banking	90 days	Enables a simplified login procedure within the e-banking applications
BRSINFO (several)	Necessary	E-Banking	Session	Anti-phishing cookie
_cfy_cc	Necessary	Website	Session	Memory cookie that has indicated the user's preferences.

13. What data do we process on our social media pages?

We may operate pages and other websites ("fan pages," "channels," "profiles," etc.) on social networks and other platforms operated by third parties and collect the data about you described in Section 3 and below. We receive these data from you and the platforms

when you come into contact with us through our website (e.g. when you communicate with us, comment on our content or visit our presence). At the same time, the platforms evaluate your use of our websites and link these data with other data about you known to the platforms (e.g. on your behaviour and preferences). They also process these data for their own purposes under their own responsibility, in particular for marketing and market research purposes (e.g. to personalise advertising) and to control their platforms (e.g. which content they show you).

We obtain information about you when you communicate with us through websites or view our content on the relevant platforms, visit or are active on our websites (e.g. publish content, post comments). These platforms also collect, among other things, technical data, registration data, communication data, behavioural data and preference data from you or about you (for the terms, see section 3). These platforms routinely analyse the way you interact with us, how you use our websites, our content or other parts of the platform (what you look at, comment on, "like," forward, etc.) and link these data to other information about you (e.g. information about age and gender and other demographic information). In this way, they also create profiles about you and statistics on the use of our websites. They use these data and profiles to show you our or other advertising and other content on the platform in a personalised way and to manage Platform behaviour, but also for market and user research and to provide us and other bodies with information about you and the use of our website. We can partially control the evaluations that these platforms create regarding the use of our websites.

We process these data for the purposes described in Section 5, in particular, for communication, marketing and market research purposes. Content you have published yourself (e.g. comments on an announcement) we may disseminate ourselves (e.g. in our advertising on the platform or elsewhere). We or the operators of the platforms may also delete or restrict content from or to you in accordance with the usage guidelines (e.g. inappropriate comments).

Further information on the processing by the operators of the platforms can be found in the privacy policies of the platforms There you will also find out in which countries they process your data, which rights of access, deletion and other data subjects you have and how you can exercise these or obtain further information.

14. What rights do you have?

To help you control the processing of your personal data, you have the following rights in connection with our data processing, depending on the applicable data protection law:

- The right to request information from us as to whether and which data we are processing;
- the right to have us rectify data if it is inaccurate;
- the right to request the erasure of data;
- the right to request that we provide certain personal data in a commonly used electronic format or transfer it to another controller;
- the right to withdraw consent insofar as our processing is based on your consent;
- the right to obtain, on request, further information necessary in order to exercise these rights;
- the right to express your point of view in the case of automated individual decisions (Section 6) and to request that the decision be reviewed by a natural person.

Applicable data protection law grants you the right to object to the processing of your data in certain circumstances, in particular for direct marketing, direct marketing profiling and other legitimate processing interests.

Please note that these rights are subject to conditions, exceptions or limitations under applicable data protection laws (e.g. to protect third parties or trade secrets). We will inform you accordingly if necessary.

In particular, we may need to process and store your personal data to perform a contract with you, to protect our own legitimate interests, such as the assertion, exercise or defence of legal claims, or to comply with legal obligations. To the extent permissible by law and in particular, to protect the rights and freedoms of other data subjects and to safeguard interests worthy of protection, we may therefore also reject a data subject request in whole or in part (e.g. by blacking out certain content relating to third parties or our trade secrets).

If you wish to exercise any of the above rights against us, please contact us in writing, at our premises or, unless otherwise stated or agreed, by email; you will find our contact details in Section 2. In order for us to be able to rule out misuse, we must identify you (e.g. with a copy of your ID card, if this is not possible in any other way).

You also have these rights in relation to other bodies who work with us under their own responsibility - please contact them directly if you wish to exercise rights in relation to their processing. You will find details of our important cooperation partners and service providers in Section 8.

If SGKB does not meet your expectations with regard to the processing of your personal data, please inform us or our data protection officers (Section 2) in a meaningful communication. This gives us the opportunity to consider your request.

If you believe that SGKB has not dealt with your enquiry or concern to your satisfaction, or if you believe that SGKB is not processing your personal data in accordance with data protection law, you can contact the data protection supervisory authority in your country. You can reach the Swiss supervisory authority here: https://www.edoeb.admin.ch/edoeb/de/home/der-edoeb/kontakt/adresse.html. You can find a list of authorities in the EEA here: https://edpb.europa.eu/about-edpb/board/members_de.

15. Can this privacy policy be changed?

We can change this privacy policy at any time. The version published on our website (www.sgkb.ch/datenschutz) is the current version.

Last updated: September 2023