Privacy policy

Version: 24 November 2025

1. General

Reichmuth & Co (hereinafter referred to as the "**bank**") also treats data protection in an open, transparent and customer-friendly manner. The purpose of this privacy policy is to tell you how the bank handles personal data.

By "personal data" we mean all information that relates to a natural person. By "processing" we mean all handling of personal data, irrespective of the measures and procedures employed, especially the collection, storage, utilisation, modification, disclosure, archiving and destruction of personal data.

Additional provisions (e.g. the General Terms & Conditions and the terms of use) apply to certain types of data processing, e.g. when using applications such as e-Connect offered by the bank. These are available on our website or in paper form.

2. General Terms and Conditions

The provisions of the General Terms & Conditions (GTCs) contain general information about data protection, especially with regard to contractual performance.

3. Data security

The bank is bound by banking secrecy and data protection laws to protect your privacy in accordance with the applicable laws. To this end, the bank takes many measures, such as the implementation of technical and organisational security measures (e.g. the use of firewalls, personal passwords and encryption technology, access restriction, awareness training for staff and the appointment of a data protection adviser).

4. Processing framework

4.1 Personal data categories

The bank may process the following categories of personal data:

- Master and inventory data (e.g. name, address, date of birth, documents to establish the customer's identity, such as an identity card or passport, contract number and duration, information about the account, portfolio, completed transactions and about third parties such as spouses/partners, proxies and consultants who are also affected by data processing)
- Tax residence and other tax-relevant information and documents
- Transaction data or order and risk management data (e.g. information about the recipients of transfers, recipient banks, information about investment products, risk and investment profiles)
- Marketing data (e.g. needs, wishes and preferences)
- Technical data (e.g. internal and external identifiers, transaction numbers, IP addresses, logged access or changes)

The bank processes data on interested parties and visitors (i.e. visitors to web pages in particular). By this we mean the following:

- Master and inventory data (e.g. name and address)
- Technical data (e.g. internal and external identifiers, IP addresses, logged access or changes)
- Marketing data (e.g. needs, wishes and preferences)

No sensitive data is processed, unless you provide such data for processing yourself.

4.2 Sources

To fulfil the purposes described in section 4.3, the bank may collect personal data from the following sources:

- Personal data provided to us, e.g. within the framework of the initiation of business relations, consultancy meetings, for our products and services or on our website
- Personal data that is generated through the use of products and services and which is transferred to us via the technical infrastructure or shared processes, e.g. the website, Chatbot, e-Connect, payment transactions, securities trading or collaboration with other financial or IT service providers or marketplaces and stock exchanges
- Personal data from third-party sources, e.g. authorities, other group companies or EU/UN sanction lists

We may use cookies, tracking technology and other methods to collect and process personal data from various channels and devices. This includes devices you use to access our websites and mobile device applications in order to obtain information about Reichmuth & Co products or services.

For information about our use of cookies and other tracking technologies in relation to our website, please also read the website and cookie notice here.

4.3 Purposes

The bank may process the data described in section 4.1 for the provision of its own services as well as for its own or legally required purposes. By this we mean the following in particular:

- Customer onboarding process, verification, conclusion, termination, processing and administration of customer relationships and providing, handling and administering the products and services of a private bank (e.g. communication, payments, billing, accounts, financing, financial planning, loan decisions, investment, shares, pensions, foundation, succession and insurance and e-Connect)
- Monitoring and managing risks, auditing, opening a business, timely conclusion of business transactions (e.g. fraud prevention, investment profiles, limits, market risk and credit and operational risks)
- Statutory or regulatory information or reporting obligations towards courts or authorities, fulfilling official directives (e.g. automatic exchange of information with foreign tax authorities, directives issued by FINMA, cantonal public prosecutors, in relation to money laundering and the funding of terrorism)
- Defending the interests and securing the entitlements of the bank in the event of claims against the bank and/or its clients
- To make the online services, their content and functions available.
- To respond to contact enquiries and communicate with users of the online content.
- Chatbot communication: Answering inquiries and providing support with general information about our offerings via the interactive chatbot.
- For marketing, advertising and conducting market research.
- Security measures

4.4 Categories of intended recipients and foreign disclosure (see GTCs section 1.12 a-b)

The bank only discloses client data to third parties in the following cases:

- To execute orders, i.e. the use of products or services, e.g. to service providers, stock exchanges or marketplaces, notifications of certain stock exchange transactions to international trade repositories or upon receipt of a request for identification from an issuer (e.g. the EU's Shareholder Rights Directive) and this in any country in the world
- On the basis of statutory obligations, statutory justification or official directives, e.g. to courts or supervisory authorities in relation to money market or fiscal legislation or where required to safeguard the bank's legitimate interests both within Switzerland and abroad (abroad means any country in the world). The latter applies in particular in the event of threatened or initiated legal measures by clients against the bank or public statements, to safeguard the bank's claims against its clients or third parties, in the event of the collection of receivables of a client by the bank and to re-establish client contact following an interruption of contact with the competent Swiss authorities.
- On account of the outsourcing of business units or services (see section 5)

If a recipient is located in a country without adequate data protection, we contractually oblige the recipient to comply with an adequate level of data protection (for this purpose, we use the revised standard contractual clauses of the European Commission, which can be accessed here, including the necessary additions for Switzerland), unless the recipient is already subject to a legally recognised set of rules for safeguarding data protection. We may also disclose personal data to a country without adequate data protection, without concluding our own contract for this purpose, if we can rely on an exemption clause for this purpose. An exemption may apply in particular to legal proceedings abroad, but also where there is an overriding public interest or when the execution of a contract, which is in your interests, requires such a disclosure (e.g. in international transactions), if you have granted consent, or if it is not possible to obtain your consent within a reasonable period of time and the disclosure is necessary to protect your life or physical integrity, or that of a third party, or if it concerns data that you have made generally accessible and whose processing you have not objected to. We may also rely on the exemption for data from a legally prescribed register (e.g. the Commercial Register), to which we have legitimately gained access.

5. What happens to data in the event of an outsourcing of areas of business or services?

The bank may outsource areas of business and services to group companies and third parties within Switzerland and abroad. This relates in particular to payment transactions, the processing and custody of securities and other financial instruments, compliance, risk management, fund administration, auditing, investment/portfolio management services, research services, data management, the printing and sending of bank documents, IT and back- and middle-office services that may be outsourced either fully or in part. However, new services may also be added. Therefore,

your personal data may be processed both domestically and internationally. When client data needs to be disclosed in such cases, it is protected in Switzerland by Swiss law. If the data is outsourced to a service provider abroad and there is no adequate data protection there, the service provider is obliged to comply with appropriate data protection by concluding recognised standard contractual clauses for this purpose (see preceding paragraph). The bank's service providers abroad are mainly based in the EEA, but in exceptional cases they may be located in any country in the world.

6. Rights

To exercise your rights as set out below, please contact us in accordance with section 7. To avoid delays, please enclose a copy of your passport or identity card with your signed letter.

You can make use of your right to waive data processing for marketing purposes by sending a message to the contact address (see section 7).

6.1 Information

In accordance with legal requirements, you have the right to request confirmation as to whether the data in question is being processed, to access this data, and to obtain further information and a copy of the data.

6.2 Data issuing and transmission

In accordance with legal requirements, you have the right to request that your data be made available and transferred in a standard electronic format.

6.3 Erasure and rectification

In accordance with legal requirements, you have the right to request the erasure or alternatively, in accordance with legal requirements, to restrict the processing of the data, rectify it (insofar as the data is incorrect) or block the processing of your data, provided that there are no legal or contractual obligations to the contrary.

In accordance with legal requirements, you also have the right to lodge a complaint with the competent supervisory authority.

6.4 Withdrawal of consent and objection

In accordance with legal requirements, you have the right to withdraw consent granted with effect for the future.

In accordance with legal requirements, you may object at any time to the future processing of your data, provided that there are no legal or contractual obligations that prevent this. The objection can be made in particular with respect to processing of your data for the purpose of direct advertising, such as the newsletter.

6.5 Changes and updates

This privacy policy was last updated in November 2025. We reserve the right to change it from time to time. Any changes or updates will be made available here.

7. Contact

If we do not meet your expectations with regard to the processing of personal data or if you wish to complain about our data protection practices, please get in touch with us.

To assist us in responding to your enquiry, please notify us in writing. We will then assess and reply to your concern within an acceptable timeframe.

Reichmuth & Co Privatbankiers
Data Protection Officer
Ruetligasse 1
CH-6003 Lucerne
+41 41 249 49 49

datenschutz@reichmuthco.ch
www.reichmuthco.ch