

Privacy Policy for retirement provision and investment products from Zurich Invest

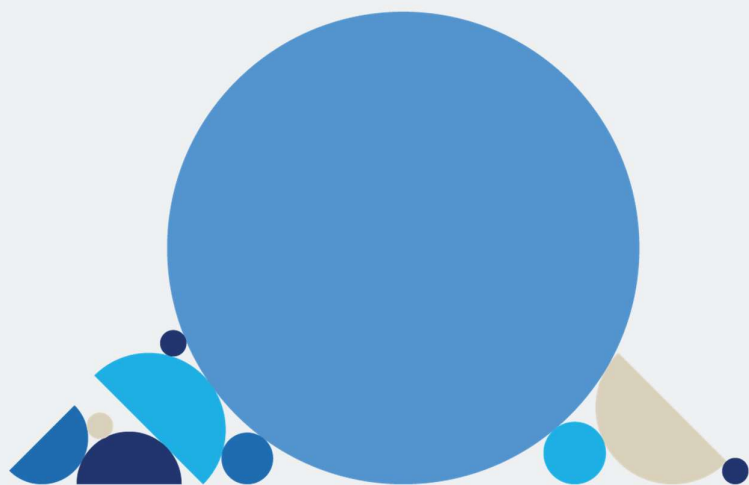


Table of content

Para.	Page
1. What does this Privacy Policy concern?.....	3
2. Who is responsible for processing your data?	3
3. Which data do we process?.....	4
4. For what purposes do we process your data?	6
5. What applies in the case of profiling and automated individual decisions?	9
6. To whom do we disclose your information?..	10
7. Do we disclose personal data abroad?.....	12
8. How long do we process your data for?.....	12
9. How do we protect your data?	12
10. What are your rights?.....	13
11. Can this privacy policy be changed?	14

1. What does this Privacy Policy concern?

Zurich Invest Ltd offers various products in the areas of retirement provision, investments and asset management. Depending on the products, it works together with other bodies, such as the Zurich Invest Bank Foundation or the Zurich Vesting Foundation (together the "**Foundations**") and with custodian and settlement banks, and processes personal data while doing so.

"Personal data" is data relating to an identified or identifiable person; in other words, the data or corresponding additional data can be used to make inferences about their identity. "Processing" refers to any handling of personal data, e.g. collection, storage, use disclosure and deletion. "Particularly sensitive personal data" includes, for example, data that reveals racial and ethnic origin, health data, and other data that finds particular protection under data protection law.

In this Privacy Policy, you will find information on how the Foundations and Zurich Invest Ltd (together also "**we**") handle data relating to you (we use the term "data" here synonymously with "personal data"). This data processing concerns, for example, the following individuals (each referred to as "**you**"):

- Pension account holders and customers (e.g. asset management clients and investors),
- depending on the product, dependents of pension account holders (e.g. current and former spouses and registered partnerships, life partners, parents, siblings and children) supported persons and other beneficiaries.
- past, present and future employers or their contacts,
- authorized representatives (e.g. legal representatives),
- persons involved in the sales organization of Zurich Insurance Company Ltd ("**ZIC**") such as contact persons and employees of ZIC and of sales partners members of our governing bodies,

- Contact persons from social and private insurers, other retirement provision and vested benefits institutions, reinsurers, suppliers and partners and from government authorities and offices.

This Privacy Policy applies to all our services and contracts, unless we provide you with separate privacy policies for these.

Contractual and other documents may contain further information about our handling of personal data. For some products and services you will also find information in additional privacy policies, which apply in addition to this Privacy Policy, e.g. in connection with your use of our websites.

In this Privacy Policy, we use the masculine form to make it easier to read, but this of course refers to people of all genders (in the English version, the neutral form is used where applicable).

We are available at any time should you have any questions (sub-paragraph 0).

2. Who is responsible for processing your data?

With regard to the processing of personal data according to this Privacy Policy, the following companies are "data controllers", i.e. are the primary competent authority according to data protection law unless communicated in the further details of this Privacy Policy and otherwise in individual cases (e.g. in further privacy policies, on forms or in contractual provisions):

- for the **retirement provision account 3a**: the **Zurich Invest Bank Foundation** and **Zurich Invest Ltd**, both Hagenholzstrasse 60, 8050 Zurich as managing directors of the Foundation;
- for the **vested benefits account**: the **Zurich Vesting Foundation**, Hagenholzstrasse 60, 8050 Zurich, and **Zurich Invest Ltd** as managing directors of the Foundation;
- for **asset management mandates** and **investment products**: Zurich Invest Ltd.

We may disclose data to third parties who are separate data controllers, e.g. to intermediary partners, companies of the Zurich Group,

authorities and other bodies. Settlement and custodian banks, other banks and other involved entities are also responsible for their processing of data.

For each data processing operation, there are one or more bodies who bear primary responsibility for ensuring that the data processing complies with the requirements of data protection law. This body is referred to as the "data controller" or "controller". It is responsible, among other things, for responding to requests for information (sub-paragraph 10) or for ensuring that personal data is secure and not used in a way that deviates from what we tell you or from what is permitted by law. Details of third parties with whom we cooperate and who are responsible for their own processing can be found in sub-paragraph 0, sub-paragraph 4 and in sub-paragraph 6.

If you wish to contact us in this regard, you can contact any of the data controllers. However, your request will be processed faster if you contact us at the following address:

Zurich Insurance Company Ltd
Data Protection
P.O. Box
CH 8085 Zurich
datenschutz@zurich.ch

We may disclose data to third parties who are separate data controllers, e.g. to certain sales partners, companies of the Zurich Group, authorities and other bodies. You will find details of this in this Privacy Policy under sub-paragraph 4 and sub-paragraph 6.

3. Which data do we process?

We process different data from different sources. Information regarding this data can be found here in sub-paragraph 3, and information regarding the purpose of the processing in sub-paragraph 4. We collect this data primarily directly from the pension account holder or customer, such as when submitting an application, during communication and when processing the retirement provision or other contractual relationship, as well as from other sources such as sales partners or advisers. You will find further details in this sub-paragraph 3.

We primarily process the categories of data described below, although this list is not exhaustive. If data changes over time, we may

retain earlier versions of information in addition to the current one.

Master data: We use the term "master data" to refer to the basic data that we require, in addition to the contractual data (see below), to process our contractual and other business relationships or for marketing and advertising purposes. We process master data, for example from pension account holders, relatives or beneficiaries of a pension account holder, from our customers, from contact persons (e.g. of banks, retirement provision or vested benefits institutions, suppliers and authorities) and from addressees of messages (e.g. messages sent in the context of marketing and advertising, invitations to events, vouchers, newsletters, etc.).

Master data primarily includes name, address and contact details, date and -place of birth, age, gender, nationality and hometown, marital status, details from identification data (e.g. from your passport, ID or other identification documents), with the scope of the statutory provisions the AHV number, your contract and insured number, language details, further details from application documents etc. and, where applicable, data in connection with risk assessments.

Details regarding relationships to **third persons** who are also affected by the data processing also fall under this data, e.g., authorized representatives or, in the case of a retirement provision or vested benefits account, e.g. about dependents and beneficiaries.

We generally receive master data from the pension account holder or customer (directly or via sales partners) but may also consult **third-party** data. These may include other Zurich Group companies and credit reporting agencies, media monitoring companies, participating financial service suppliers and banks, address dealers, internet analysis services, private insurers, social insurers, public authorities, parties to proceedings and publicly available sources such as the commercial register, media and sources on the Internet, public registers, media, etc.

Contract and benefits data: This is information that accrues in connection with the preparation, conclusion, processing and dissolution of a contractual relationship, e.g. details in connection with a payment of retirement provision or vested benefit assets, other payments and court orders. This may include health information and

information about third parties. We may also collect data from other bodies in this relation. **When you send us an application for a retirement provision or investment product, you release these bodies from any professional secrecy obligations.**

This data includes information related to the **initiation** and **conclusion** of the contractual relationship and to its processing and administration (e.g. information in connection with advice and customer service). Contract data also includes information relating to complaints about and adjustments to a contract, as well as information about customer satisfaction which we may collect, for example, by means of surveys.

In connection with the **retirement provision relationship** we may also process data on claim entitlement, e.g. its amount, on payments into the retirement provision or vested benefits account and on our investment activities). We receive this information primarily from the pension account holder. When processing a retirement provision or vested benefits statement or corresponding applications, we also process data in connection with the regulatory grounds for an ordinary or early payment, including information about retirement provision and vested benefits institutions, other insurance companies and insurers, information about third parties such as involved individuals and beneficiaries, and particularly sensitive personal data such as health data. We receive this information primarily from the pension account holder, but may also receive it from third parties, e.g. other insurers, such as disability insurers, from whom we may also receive data – including health data, for example an annuity decision – possibly with a separate release declaration, or from spouses and registered partners. In other benefit cases, such as in the event of a divorce or the dissolution of a registered partnership, we process the associated data (information relating to the matrimonial property dispute, such as the date of divorce or dissolution of registered partnership and judicial order in this context). We obtain this information from pension account holders, asset management customers, their spouses or registered partners and from public authorities and courts.

In connection with **asset management, custody accounts and investments** we may, in particular, process information relating to the acquisition and management of assets.

In addition to the sources mentioned above and in addition to the pension account holder, asset management customer or investor, we also receive data **from other third parties**, such as sales partners, public authorities and offices, courts and lawyers, employers, other insurers, the settlement bank or custodian bank and from external bodies from which we obtain financial information.

Financial data: This is data relating to financial circumstances, payments and the securing of claims.

Financial data is information relating to the financial circumstances of the customer and, where applicable, third parties. We receive this data from the policy account holder or customer, such as in the course of processing the application, but also from government offices (such as tax offices), banks and credit agencies, and from publicly accessible sources.

Behavioral and preference data: Despite our large number of customers, we strive to get to know you better and to tailor our advice and offers to you in the best possible way. We therefore process certain data about you and your behavior. By 'behavioral data', we mean data about your behavior in the context of your interactions with us. We may combine this information with other information – also from third parties – and derive from it, for example, the statistical probability that you have an affinity for certain products and services or will behave in a certain way (preference data).

Behavioral data is information about certain actions, for example, payments, your use of electronic communications (such as whether and when you opened an email), your location (such as when you use a website of ours; please see the relevant separate privacy policies for our processing of data in connection with our website), your purchases of products and services from us, your interaction with our social media profiles, contacts with contractual partners and your participation in events, competitions contests and similar events.

Preference data tells us, for example, what your needs are, what products or services might be of interest to you, or when and how you respond to messages from us. We obtain this information from analyzing existing data, such as behavioral data, so that we can get to know you better, tailor our

advice and offers more precisely to you and generally improve our offers. In order to improve the quality of our analyses, we may combine this data with other data that we also obtain from third parties such as address dealers, websites and government offices; this may include information on your household size, income class and purchasing power, shopping behavior, contact details of relatives and anonymous information from statistical offices.

Communication Data: This is data relating to our communication with you and information regarding your use of our website. If you contact us via the contact form, email, telephone, by letter or by any other means of communication, we record the data that is exchanged between you and us, including your contact details and other marginal data. We may also record phone conversations. If we want or need to establish your identity, for example, in the context of a request for information, application for media access, etc., we collect data to identify you (such as a copy of an identity document).

Communication data includes your name and contact details, the manner, place and time of the communication and normally its content, such as details in emails or letters from you or to you or from third parties or to third parties, if the latter also relate to you. This also includes direct and indirect contacts with us, e.g. customer service and your customer consultant (e.g. via a website or an app, in a chatbot on the internet or an app).

Other data: We also collect data from you in other situations, which we cannot exhaustively list in this Privacy Policy. For example, data (such as files or evidence) accrues in connection with official or judicial proceedings, and some of this may also relate to you. We may also collect data for health protection reasons (for example, in the context of protection concepts). We may obtain or produce photographs, videos and audio recordings in which you may be identifiable (for example, at events, via security cameras etc.). We may also collect data about who enters certain buildings and when (including in the case of access controls, on the basis of registration data or visitor lists, etc.), who participates in events or campaigns (such as competitions) and when or who uses our infrastructure and systems.

The data we process in accordance with this Privacy Policy relates not only to our pension account holders and customers, but often also to

third parties (you will find information on this in sub-paragraph 1 and in this sub-paragraph 3). We receive information about third parties primarily from the pension account holder. If you provide us with information about third parties, we shall assume that you are authorized to do so and that the information is accurate. By transmitting data about third parties, you confirm this fact. **Therefore, please inform these third parties about our processing of their data and provide them with a copy of this Privacy Policy.** If we refer you to a new version of these documents, please also hand over these new versions in each case.

With the exception of certain individual cases, such as in the context of binding protection concepts (legal obligations), you are not obliged to disclose data to us. However, in the case of voluntary processes, such as contributions or early drawing of retirement provision or vested benefits, we must process data for legal and operational reasons. If you do not wish to make this data available to us, we would therefore be unable to complete the applicable processes. When using our website, it is not possible to avoid technical data processing. If you wish to gain access to certain systems or buildings, you will need to provide us with registration details.

There are certain services which we can only make available to you if you provide us with certain registration data because we or our contractual partners wish to know who, for example, has responded to an invitation to an event, because it is either technically necessary or because we wish to communicate with you. If you or someone you represent (such as your employer) wish to enter into or perform a contract with us, we need to collect relevant master, contract- and communication data from you, and we process technical data when you wish to use our website or other electronic offers. Likewise, we can only send you a response to a request you have made if we process the relevant communication data and – if you communicate with us online – any applicable technical data. It is not possible to use our website without us receiving technical data.

4. For what purposes do we process your data?

In particular, we process your personal data for the following purposes, which must be agreed upon:

We process personal data to **fulfill legal and regulatory requirements** and to comply with laws, directives and recommendations imposed by authorities, as well as internal regulations ("compliance").

This includes, among other things, the legally regulated combating of money laundering and the terrorism financing. As a result, we may be obliged to make certain inquiries about legal and reputational risks such as political connections (Know Your Customer), such as via corresponding third-party directories such as World-Check, or to file reports under certain circumstances. Also the fulfillment of disclosure, information or reporting obligations, e.g. in connection with obligations to supervisory bodies, the fulfillment of archival obligations and support in preventing, exposing and clarifying criminal acts and other infringements. This includes the receipt and processing of complaints and other reports, the surveillance of communication, internal or external checks or the disclosure of documents to a public authority if we have a material reason for so doing or are required to by legal obligations. For these purposes, we process, in particular, master data, contract and financial data, communication data and, under certain circumstances, pension account holders' behavioral data. Legal obligations can arise from statutory provisions (in particular occupational retirement provision legislation), but also from self-regulation, industry standards, the company's own "corporate governance" and official instructions and requests.

We process data **for the initiation and conclusion of contracts, and for the administration and execution of contracts**, e.g. pension agreements, asset management and other contracts. This purpose also includes the provision of advice, customer care, compensation for distribution partners and, in the case of pension relationships, the review and settlement of payout cases, including coordination with other insurers such as disability insurance and the enforcement of recourse claims. We can also carry out profiling in this context (see sub-paragraph 5).

To conclude **retirement provision agreements**, we process in particular the pension account holder's master data, contract data, financial data and communication data and of sales partners or their contact persons. We then maintain a pension account for each pension account holder, for which

we process information on payments, the amount of the retirement provision or vested benefits credit balance and withdrawals. The assessment and processing of **claims** also falls under the provision of occupational pension arrangements. In this case, we primarily process contract, case and benefits data pertaining to the pension account holder and from beneficiaries for examining legitimation (you can find further information about this in the following sections) and, where required, for the provision of benefits. To this end, we may also process health data and other information that arises in the context of these purposes or is necessary for them.

If you entrust us with **asset management**, we process data for the preparation, including a standard risk assessment, the conclusion and the execution of the asset management agreement. For this purpose we process your personal data – especially master data, contract data, financial data and communication data – and data from contact persons at the custodian bank. We process comparable data for **investments and deposits**.

Our **customer service** and our **advisory service** also fall under this purpose, as does the assertion of legal claims from contracts (payment defaults, legal proceedings etc.), accounting, the termination of contracts and public communication. We also process data for the purpose of assessing and documenting compensation paid to sales partners (see also sub-paragraph 6).

We may draw upon **other bodies** e.g. IT and logistics companies, advertising service providers, banks or credit reporting agencies who can make data available to us for the purpose of initiating and concluding contracts and setting up contractual relationships. We also collect data via our sales organization. Our sales partners include independent general agencies, intermediaries and brokers.

When **cooperating with companies and business partners**, such as partners in projects or cooperating with parties in legal disputes, we also process data to process and initiate contracts, for planning, for accounting purposes and other purposes related to the contract.

We also process data to **prevent fraud** and for **legal processes**, for our **risk management** and in the context of prudent **company administration**,

including the business organization and development.

For this purpose we process, in particular, master data, contractual data, claims and benefits data and financial data, but also behavioral and communications data. For example, we must take measures against **fraudulent claims**. We may also carry out profiling and create and process a profile (see sub-paragraph 5) for the above purposes and in order to protect you and us from illicit or abusive activities.

We also process your data for **market research** purposes, to **improve our services and our operation** and for **product development**.

We strive to continuously improve our products and services and to be able to react quickly to changing needs. We therefore analyze how, for example, offers are used and how new products and services can be created. This gives us an indication of the market acceptance for existing products and services and the market potential of new ones. To this end, we process, in particular, your master data, behavioral data and preference data, as well as communication data and information from customer surveys, polls and studies and other information, such as from the media, from social media, from the Internet and from other public sources. As far as possible, however, we use pseudonymized or anonymized data for these purposes. We may also use media monitoring services or perform media monitoring ourselves, whereby we process personal data in order to carry out media work or to understand and respond to current developments and trends.

We also process data to the extent permitted by law for **marketing purposes**, such as for personalization and the transmission of information on products and services from us and from third parties and for **relationship management**. You can refuse such contacts at any time (see the end of this sub-paragraph 4).

We may send you information, advertising and product offers from us and from selected third parties, such as newsletters, via apps and messenger services, as printed matter or by telephone, on a regular basis or as part of individual promotions (such as for events, competitions, etc.). We may also personalize notifications so that our information and offers better meet your needs and

expectations. To do this, we link data that we process about you, determine preference data and use this data as the basis for personalization (see sub-paragraph 3). We may also carry out profiling for marketing purposes (see sub-paragraph 5). We also process data in connection with contests, competitions and similar events. Customer care also includes addressing existing customers – in a manner that may be personalized on the basis of behavioral and preference data or data from customer surveys – and organizing customer events (such as sponsoring-, sports and cultural events and promotional events). In the case of customer events, we process personal data to carry out the events, as well as to inform the participants and to provide them with information and advertising before, during and after the event.

All of this processing is not only important to enable us to promote our offers in the most effective way possible, but also to make relationships with customers and other third parties more personal and positive, to concentrate on our most important relationships and to use our resources as efficiently as possible.

You may object to processing for marketing purposes at any time by notifying us. Further information on your rights can be found in sub-paragraph 9.

We may also process your data for **security purposes** and for **access control** purposes.

We continuously review and improve the appropriate security of facilities and buildings and our IT. In doing so, we process data, among other reasons, in connection with the surveillance of buildings and publicly accessible premises. We are not able to rule out data breaches with absolute certainty but we do use our very best endeavors to reduce the risk. We therefore process data, for purposes such as monitoring, control, analysis and testing of our networks and IT infrastructures, to carry out system and error checks, for documentation purposes and in the context of security copies.

We may process your data **for other purposes**, such as our internal processes and administration.

These other purposes may include training and educational purposes, administrative purposes (such as the administration of master data,

accounting and data archiving or the administration of real estate and the testing, administration and ongoing improvement of IT infrastructure), the protection of our rights (for example, to enforce claims in or out of court and before authorities in Switzerland and abroad or to defend ourselves against claims, for example by preserving evidence, through legal clarifications and by participating in judicial or official proceedings), the evaluation and improvement of internal processes. In the course of developing our business, we may also sell or acquire businesses, operations or companies to or from other companies or enter into partnerships, which may also result in the exchange and processing of data (including from you, for example, as a customer or supplier or as a supplier representative). This also includes the protection of other legitimate interests, which cannot be named exhaustively.

If we ask for your **consent** for certain processing, we will inform you separately about the corresponding purposes of the processing. You may withdraw your consent at any time with effect for the future by notifying us in writing; you will find our contact details in sub-paragraph 0. Once we have received the revocation of your consent, we will no longer process your data for the relevant purposes unless we have another legal basis for doing so. The legality of processing which has taken place up until the point of time at which consent was revoked shall remain unaffected.

We base the processing of your personal data on the fact that it is required or permitted by law, is necessary for the preparation and execution of contracts with you or the body you represent (such as the processing of master and financial data for application verification, for the prevention of fraud, for creditworthiness and borrowing capacity checks, for the processing of transactions, etc.), that it is necessary for legitimate interests of us or third parties (such as processing for administrative and security purposes, for credit checks and purposes of market research, marketing, improvement of our services and product development) or that you have consented to the processing.

If we receive sensitive data (such as health data), we may also process your data on the basis of other legal grounds, for example, in the event of disputes arising from the necessity to process the data for a possible lawsuit or the enforcement or defense of legal claims. In individual cases, other legal grounds

may apply; we will communicate these to you separately where necessary.

5. What applies in the case of profiling and automated individual decisions?

For the purposes stated in sub-paragraph 4, we may process and evaluate your data (sub-paragraph 0) automatically, i.e. in a manner aided by a computer; we may also do so to determine preference data, as well as to determine risks of misuse and security, to carry out statistical evaluations or for operational planning purposes. These processing operations also include **profiling**.

Profiling is the automated processing of data for analysis and forecasting purposes. The most important examples are profiling to combat money laundering and terrorist financing in investment products, to combat fraud, for customer care and for marketing purposes (as described in more detail in sub-paragraph 4). For the same purposes, we may also create profiles, i.e. we may combine behavioral and preference data, as well as master data, contract data and technical data assigned to you, in order to better understand you as a person and your different interests and various characteristics.

In every case we pay attention to the appropriateness and reliability of the results and take measures against the misuse of this profile or **profiling**.

In order to ensure the efficiency and uniformity of our decision-making processes, we can also **automate** certain decisions, i.e. make these with the aid of a computer according to certain rules and without review by an employee. These may, for example, include decisions about concluding a contract, terminating a contract or risk exclusions.

In each individual case, we will inform you or indicate the decision accordingly if an automated decision has been made which creates negative legal consequences or a comparable significant impairment for you. In this case, you shall have the rights set out in sub-paragraph 9 if you do not agree with the outcome of the decision.

6. To whom do we disclose your information?

When processing contracts, we not only exchange information with each other, but also with third parties. This is particularly true in the case of pension agreements. Your data will therefore not only be processed by us. Below you will find an overview of the categories of recipients to whom we may disclose personal data. This sub-paragraph 6 explains the most important data disclosures with references to the corresponding data. For further information please refer to sub-paragraphs 0 and 4.

Disclosures in the initiation, conclusion and settlement of agreements: In connection with the conclusion of a retirement provision or other agreement, we may exchange data with other bodies such as banks.

In the case of a **retirement provision or vested benefits account**, we may exchange data with other bodies such as retirement provision and vested benefits institutions, public authorities and government offices (e.g. social insurance institutions such as, in particular, disability insurers), other insurers, banks and lenders, courts and external lawyers in connection with the notification and occurrence of benefit claims. When executing an asset management mandate, we exchange data with banks and with counterparties. In the case of payments into a vested benefits account, we may also disclose data to the Zurich Investment Foundation. In the context of processing benefit claims and the relevant clarifications, we may gather data from third parties (sub-paragraph 3), but also pass data to them, for example to public authorities, government offices, courts, respondents and lawyers. For example, we inform other social and private insurers about specific benefit claims for the coordination of obligations to pay indemnities and for clarifying and implementing recourse claims. Particularly in the case of divorce or the dissolution of a registered partnership, inheritance disputes or other disputes, we will provide personal data to courts and other retirement provision or vested benefits institutions.

In the context of **asset management**, we exchange data in particular with the custodian bank and with other banks and counterparties. This also applies to **deposits and investments**.

Insurance brokerage: We provide our sales partners (see sub-paragraph 4) with the information they need for their support and advice, for the distribution of our products and for the calculation of their compensation.

In addition to master data, this may include information on the period of insurance, the performance and -termination of the contract, the sum insured and coverage, claims data, further information on the assessment of compensation and for the – also personalized – marketing of our products. Contractual partners are required by law and contract to comply with the provisions of the Swiss Data Protection Act.

Risk assessment and assertion of claims: We may involve third parties for risk assessments and for the enforcement of claims.

We may involve third parties for risk assessments and the enforcement of any claims and disclose data to them in the process, such as data concerning a planned conclusion of a contract, contract documents, outstanding claims and communication between you and us.

Companies of the Zurich Group: We may transfer personal data to other Zurich Group companies in Switzerland and to joint foundations providing occupational retirement provision to support our risk management, for reinsurance solutions and for marketing purposes.

Where necessary and permitted, we may share your information with other companies belonging to the Zurich Group as well as joint foundations that provide occupational retirement provision, in particular -for the purpose of risk measurement and assessment and the provision of reinsurance solutions. We may also engage companies of the Zurich Group as service suppliers (see below). In order to offer you the best possible insurance coverage and individualized financial solutions, we may also disclose your data – in particular your master data, contract data and registration data as well as behavior and preference data – to other companies belonging to the Zurich Group for the purpose of offering their products and services tailored to your individual needs (this data is not especially worthy of protection).

Public authorities and agencies: We may disclose personal data to public authorities, agencies, courts and other public bodies if we are legally obliged or entitled to do so, or if this is necessary to protect our interests.

In the context of exercising of rights, defense of claims and fulfillment of legal requirements, we may disclose personal data to public authorities, agencies, courts and other public bodies, for example in the context of official, judicial and pre- and extra-judicial proceedings and in the context of legal obligations to provide information and to cooperate. Recipients are, for example, offices for bankruptcy proceedings, criminal courts, law enforcement agencies and tax offices. Data is also disclosed if we obtain information from public bodies, for example, in connection with the processing of pension claims (see above). Public authorities are responsible for processing data about you that they receive from us.

Additional individuals: Should data from third parties for the purposes outlined in sub-paragraph 4 be included, data can also be disclosed to other recipients.

We may disclose data, for example, to individuals involved in proceedings before courts or authorities (in the case of retirement provision or vested benefits account, for example, in the event of regress to the liable third party or its liability insurer), as well as potential purchasers of companies, receivables and other assets and, in the case of securitizations, to financing companies and to other third parties, about whom we will inform you separately where possible, for example, in declarations of consent or special privacy policies. Other individuals include, in particular, payment recipients, authorized representatives, correspondent banks, other financial institutions and other bodies involved in a legal transaction.

Service suppliers: We work with service suppliers at home and abroad who process data about you on our behalf or in joint responsibility with us, or receive data about you from us within their own sphere of responsibility. This may also include health data.

We procure services from third parties to ensure that we can deliver our products and services securely and cost-effectively and that we can concentrate on our core competencies. These

services include, for example, sales via other sales partners (see sub-paragraph 3) IT services, the dispatch of information, marketing, sales, communication or printing services, facility management, security and cleaning, the organization and holding of events and receptions, debt collection, credit agencies, anti-fraud measures and services provided by consulting firms, auditing firms and claims service suppliers. In each case, we provide service suppliers with the data necessary for their services. One example is hosting service suppliers who store electronic data on our behalf, which may include sensitive data such as health data. Our service suppliers are each subject to contractual and/or statutory confidentiality and data protection obligations. They may exceptionally use such data for their own purposes in justified cases, for example, information on outstanding debts and your payment history in the case of credit agencies or anonymized information for the purpose of improving services.

To the extent provided by law, these categories of recipients may in turn involve third parties, meaning that your data may also become accessible to them.

We also reserve the right to make these data disclosures if they affect confidential data subject to mandatory legal provisions.

In many cases, it is also necessary to disclose confidential data in order to process contracts or provide other services. Even non-disclosure agreements neither generally exclude this type of data disclosure, nor disclosure to service suppliers. However, given the sensitivity of the data and other circumstances, we take care to ensure that these third parties handle the data in an appropriate manner.

We also allow certain third parties to collect personal data from you on our website and at events organized by us (such as media photographers, providers of tools that we have embedded on our website, etc.). Where we are not decisively involved in these cases of data collection, these third parties are solely responsible for them. If you have any concerns or wish to exercise your data protection rights, please contact these third parties directly.

The aforementioned disclosures to within and outside Switzerland (see sub-paragraph 7) are required for legal or operational reasons.

Therefore, legal and **contractual confidentiality obligations** do not prevent these disclosures.

7. Do we disclose personal data abroad?

As explained in sub-paragraph 6, other organizations also process your personal data in addition to us. For example, when transferring personal data to banks and other bodies in connection with assets located abroad or to service suppliers, your data may also end up abroad. These recipients are not only based in Switzerland. Your data may therefore be processed worldwide, including outside the EU or the European Economic Area (in so-called third countries such as the USA). Many third countries do not currently have laws that guarantee a level of data protection equivalent to that provided by Swiss law. We therefore take contractual preventative measures in order to balance out the weaker legal protection, provided the data protection legislation does not allow disclosure in individual cases for other reasons. For this purpose, we generally use the standard contractual clauses issued or recognized by the European Commission and the Swiss Data Protection and Information Commissioner (FDPIC) (for further details and a copy of these clauses, please see <https://www.edoeb.admin.ch/edoeb/en/home/daten-schutz/arbeit-wirtschaft/datenuebermittlung-ausland.html>), unless the recipient is already subject to a legally recognized set of rules to ensure data protection and we cannot 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 processing of a contract requires such disclosure, if you have granted your consent or if it is a matter of data concerned that you have made generally accessible and whose processing you have not objected to.

Many countries outside Switzerland or the EU and EEA currently do not have laws that guarantee an adequate level of data protection from the perspective of the Swiss Federal Act on Data Protection or the GDPR. The contractual arrangements mentioned above may partially compensate for this weaker or missing statutory protection. However, contractual precautions cannot eliminate all risks (with particular regard to state intervention abroad). You should be aware of

these residual risks, even though the risk may be low in individual cases and we have taken additional measures (such as pseudonymization or anonymization) to minimize it.

Please also note that data exchanged over the Internet is often routed via third countries. Your data may therefore be sent abroad even if the sender and recipient are in the same country.

8. How long do we process your data for?

We store your data for as long as our processing purposes, the legal retention periods and our legitimate interests in processing for documentation and evidence purposes require, or for as long as the storage is technically necessary.

Therefore, the period for which we retain data depends on legal and internal regulations and on the purposes of processing (see sub-paragraph 4), which also include the protection of our interests (for example, to enforce or defend claims, for archiving purposes and to ensure IT security). If these purposes have been achieved or no longer apply, and if there is no longer a retention obligation, we shall delete or anonymize your data as part of our normal procedures.

Documentation and evidence purposes include our interest, processes, interactions and other facts in the event of legal claims and other discrepancies, for IT and infrastructure security purposes and to provide evidence of good corporate governance and compliance. Retention may be technically necessary if certain data cannot be separated from other data and we therefore need to retain it with this other data (such as in the case of backups or document management systems).

9. How do we protect your data?

We handle your data confidentially and take appropriate technical and organizational security measures to protect the confidentiality, integrity and availability of your personal data, to protect it against unauthorized or unlawful processing and to protect it against the risk of loss, accidental alteration, unauthorized disclosure or access. We

use recognized security standards such as ISO 27001 as a guide.

Our security measures may include measures such as encrypting and pseudonymizing data, logging, access restrictions, storage of backup copies, instructions to our employees, confidentiality agreements, audits, etc. We also oblige our contracted data processors to take appropriate security measures. In general, however, security risks cannot be completely ruled out; certain residual risks are unavoidable.

When your data is transmitted via our web pages, we protect it during transport using suitable encryption mechanisms. However, we can only secure areas that are under our control.

If you contact us by email, you do so at your own risk and agree that we may respond to you at the sender's address via the same channel. If you send us emails via the Internet in unencrypted form, third parties may be able to access, view and manipulate them. When we contact you by email, we encrypt the emails.

In addition, we take appropriate technical and organizational security measures to reduce the risk within our Internet pages. However, your end device is outside the security area that lies within our control. You are therefore required to learn about the necessary safety precautions and to take appropriate measures in this regard.

10. What are your rights?

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

In order to give you more control over the processing of your personal data, you have various rights in connection with our data processing:

- The right to request information from us as to whether we are processing your data, and which data we are processing;
- the right to have data corrected by us if it is inaccurate;

- the right to object to our processing for specific purposes and to request the deletion of data unless we are obliged or entitled to continue processing it;
- the right to obtain from us the disclosure of certain personal data in a commonly used electronic format or to request that we transfer this to another controller;
- the right to revoke consent, provided our processing is based on your consent.

If we inform you about an automated decision (sub-paragraph 5), you have the right – with certain exceptions – to express your position on this and request that the decision be reviewed by a natural person.

Please note that certain conditions must be met in order to exercise these rights and that exceptions or restrictions may apply (e.g. to protect third parties or trade secrets). We will inform you accordingly where necessary.

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

If you wish to exercise any rights against us, please contact us in writing (see sub-paragraph 2). To enable us to rule out abuse, we must identify you (such as with a copy of an identity card, if not otherwise possible). 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 any rights in relation to their processing.

If you do not agree with our handling of your rights or data protection, please let us know via the contact details listed under sub-paragraph 2. You can contact the Swiss supervisory authority via <https://www.edoeb.admin.ch/edoeb/en/home/dere.doeb/kontakt.html>

11. Can this privacy policy be changed?

This Privacy Policy does not form part of any contract with you. We may amend this Privacy Policy at any time. The version published on this website is the current version.

Zürich Versicherungs-Gesellschaft AG
Hagenholzstrasse 60
8050 Zürich
Telefon 0800 80 80 80, www.zurich.ch

