

## Duty of Confidentiality

The Pillar 3 Pension Foundation of Zürcher Kantonalbank, the Vested Benefits Foundation of Zürcher Kantonalbank and the Vested Benefits Foundation II of Zürcher Kantonalbank (hereinafter the “Foundations”) are required by law to maintain confidentiality. In addition, its client data in Switzerland is subject to Swiss data protection law, i.e. it must be treated confidentially by the Foundations.

Within the Foundations or Zürcher Kantonalbank, which as managing director is responsible for the Foundation’s client administration, access to client data is only granted to those offices that require it in order to enter into, implement or terminate a contractual or business relationship or due to legal and regulatory obligations.

The Foundations and Zürcher Kantonalbank may engage third-party service providers in addition to their Group companies to perform client administration tasks. These process client data on behalf of and for the purposes of the Foundations, e.g. for the development and operation of information and communication technologies (e.g. IT infrastructures, platforms or applications), marketing, sales and communication services or for the purpose of fraud prevention.

If customer data is disclosed to service providers of this kind, they are only permitted to process the data contained therein to the extent that the Foundations itself does. The Foundations or Zürcher Kantonalbank select their service providers carefully and contractually oblige them to warrant confidentiality by means of technical and organisational measures.

Due to the Foundation’s or Zürcher Kantonalbank’s operating model and the technologies used, it may be that the service providers have a foreign connection. For example, this may be the case if a service provider belongs to a foreign parent company, if its registered office is abroad or if it processes data abroad.

Service providers with a foreign connection can be contracted to develop and operate IT infrastructures, platforms and applications in particular, e.g. in order to use cloud-based services such as Microsoft Office applications, to use filters against viruses or to ward off attacks against the IT infrastructure (so-called DDoS attacks).

In such cases, Zürcher Kantonalbank, appointed by the Foundations as managing director, also agrees on technical and organisational measures to ensure the confidentiality of client data with the service providers and, for example, to protect it against cyber criminals. However, the possibility remains that foreign authorities may order the disclosure of client data on the basis of the foreign connection and the foreign law applicable as a result. Swiss bank-client confidentiality cannot prevent such a disclosure, and the data may be processed by the foreign authorities in accordance with their applicable foreign law, e.g. for their own investigations or proceedings. Depending on the applicable foreign law, there may not be an adequate level of data protection in place compared to Switzerland, and comparable rights (e.g. access or disclosure restrictions) may be lacking.