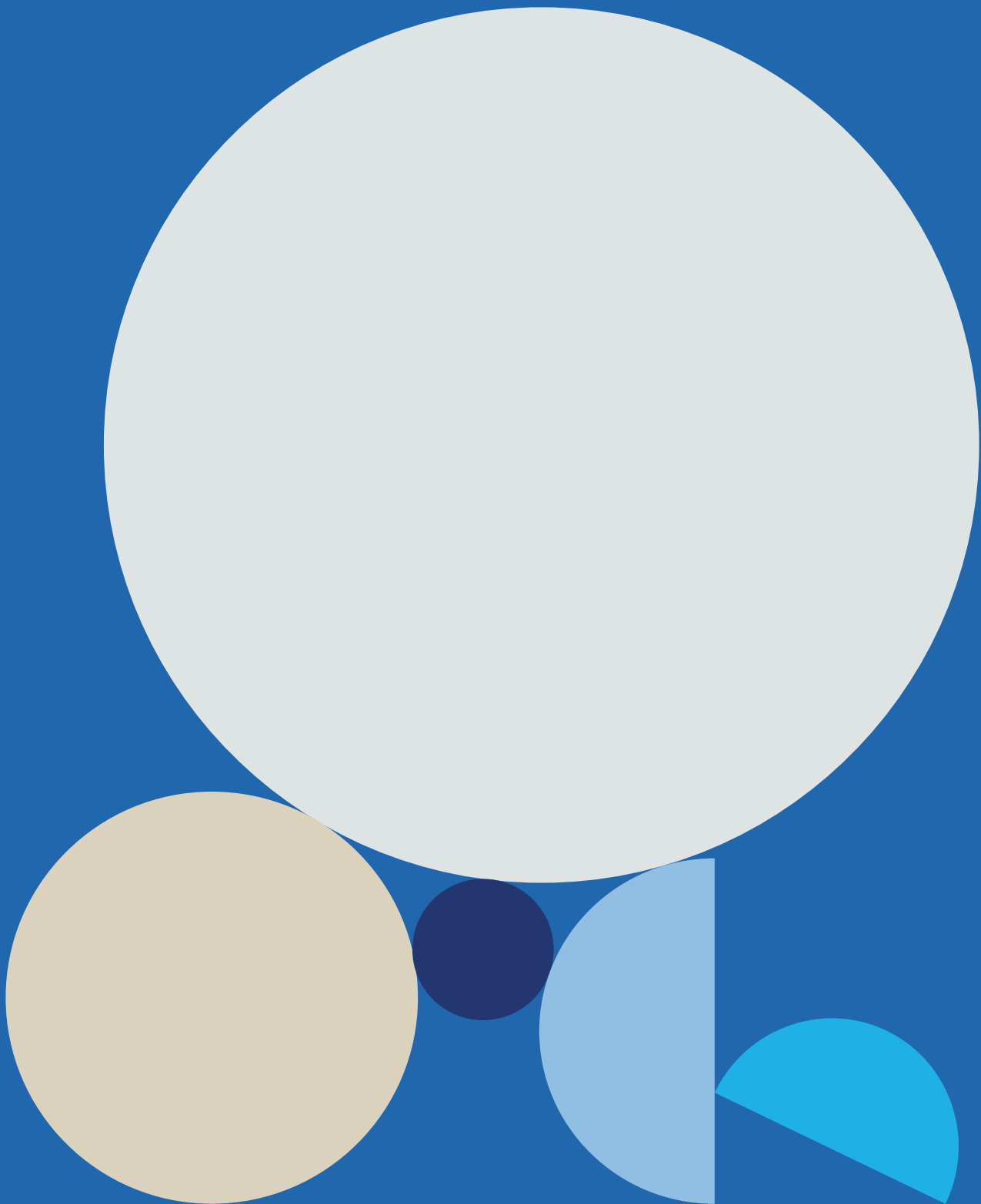
Data Privacy and Records Management Framework

High level Summary



High level summary of Zurich's Data Privacy and Records Management Framework

Introduction and Contact Information

At Zurich, we recognize privacy as a fundamental human right and are committed to managing personal data with integrity and in accordance with our Code of Conduct and Data and Responsible AI Commitment. We have a standalone Group Policy on Data Protection and Records Management that is reviewed on an annual basis as well as dated, approved and signed by the Group CEO. Local Policies are the responsibility of the local CEOs. The Group Policy outlines our approach to data privacy and records management, ensuring that we remain a trusted stakeholder for our customers, employees, partners and other stakeholders.

Please note that this document is a high-level summary of Zurich's Data Privacy and Records Management Policy to explain some key elements how personal data and business records are handled. The actual Group Policy is only shared on a need-to-know basis and based on contractual agreements. Requests are to be sent to the mailbox privacy@zurich.com together with a detailed justification. Zurich reserves the right to deny such requests without further explanation.

Purpose

The purpose of the Group Policy is to provide a framework for the management of data privacy and records management, aligning with Zurich's values. We aim to protect Zurich against violations and uphold our responsibilities in data handling.

Scope

The Group Policy applies to all operations within Zurich Insurance Company Switzerland Ltd, its subsidiaries and employees, ensuring compliance with both Group and local requirements.

Local Policies

Zurich and its employees must adhere to the relevant privacy regulations where it operates. Where Business Units are governed by requirements that are stricter than those outlined in Zurich's Group Policy – these are adhered to through supplementary local policy documents, processes and controls.

Roles and Responsibilities

Local CEOs are accountable for implementing the policy and managing associated risks, with support from Information Governance Officers and Data Privacy Officers, where appointed, all employees and dedicated Data Compliance Contacts in the Compliance function.

Data Privacy Principles

The Group Policy requires Zurich and its employees to adhere to Data Privacy principles such as lawfulness, transparency, fairness, purpose limitation, data minimization, accuracy, privacy by design and by default and data protection in line with local regulations.

Requirements

For all Legal Entities in scope the following requirements apply:

- **Governance**: Establish a framework that complies with local data privacy and records management laws and defines roles and responsibilities and implement standardized control requirements across the Group.
- **Data Privacy Risk Assessments**: Conduct Data Privacy risk assessments.
- **Records of Processing Activities:** Maintain an inventory of processing activities.
- **Third Parties**: Conclude agreements with third parties that process data on our behalf, conduct due diligence, monitor compliance mandated by our separate governance documents Third-Party Governance Framework and Group Third-Party Risk Policy. This is also reflected in our Supplier Code of Conduct that sets expectations in terms of privacy compliance for all the relevant third parties we are working with.
- **Respecting Privacy Rights**: Privacy rights are respected, and mechanisms are in place that allow individuals to access, erase, rectify, complete or amend their personal data, and Zurich informs them about how we process their personal data. Material changes to privacy notices must be communicated to data subjects.
- **Sale of Personal Data:** Our customers' personal data must not be sold to third parties[1].
- **Cross-Border Data Transfers**: Ensure that cross-border transfers comply with local regulation.
- **Data Protection**: Protect personal data in line with the Information Security Risk Policy Manual.
- **Incident Response**: Manage personal data incidents and breaches and report to Group, authorities and impacted individuals as relevant.
- **Records Management**: Maintain a retention schedule and ensure proper retention, deletion and disposal of records as per legal requirements. Keep personal data only as long as necessary and delete, dispose or anonymize afterward.
- **Training and Awareness**: Provide mandatory training and additional enhanced training on data privacy and records management relevant to employees' roles.
- **Compliance Assurance**: Monitor and assure compliance with this Group Policy through independent reviews by Group Compliance.

[1] According to our DPRM Guidance selling of data also incudes renting out data as this could be a circumvention of the prohibition to sell customer data.