PRIVACY PROGRAM OVERVIEW

PURPOSE

APi Group is committed to establishing oversight for the Privacy Program and safeguarding personal data. This Privacy Program Document articulates principles and approaches related to privacy risk to ensure that APi Group complies with applicable privacy laws and preserves trust through safeguarding and responsible use of personal data. This Privacy Program Document sets forth the key components of APi Group's Privacy Program and serves to set the foundation for privacy compliance.

INTRODUCTION AND BACKGROUND

APi Group has operating locations in [21] different countries and as global privacy laws continue to expand, evolve and become more stringent, this creates a complex environment of data protection laws that are routinely enforced through significant fines and penalties. For example, the General Data Protection Regulation (GDPR), one of the toughest privacy laws in the world, was drafted and passed by the European Union (EU), but imposes obligations onto organizations anywhere, so long as they target or collect data related to people in the EU. Although the United States does not currently have a comprehensive federal law governing privacy, there is a notable increase in state-specific privacy laws. This trend started with the enactment of the first comprehensive US state privacy law, the California Consumer Privacy Act (CCPA).

Privacy laws are based on fundamental privacy principles. These principles are embraced internationally and serve as the foundation for various privacy legislation. While these principles may be articulated differently from one law to another, their core ideas remain consistent across different regulations.

- Lawfulness, Fairness and Transparency
- Purpose Limitation
- Data Minimization
- Accuracy
- Storage Limitation
- Integrity and Confidentiality
- Accountability

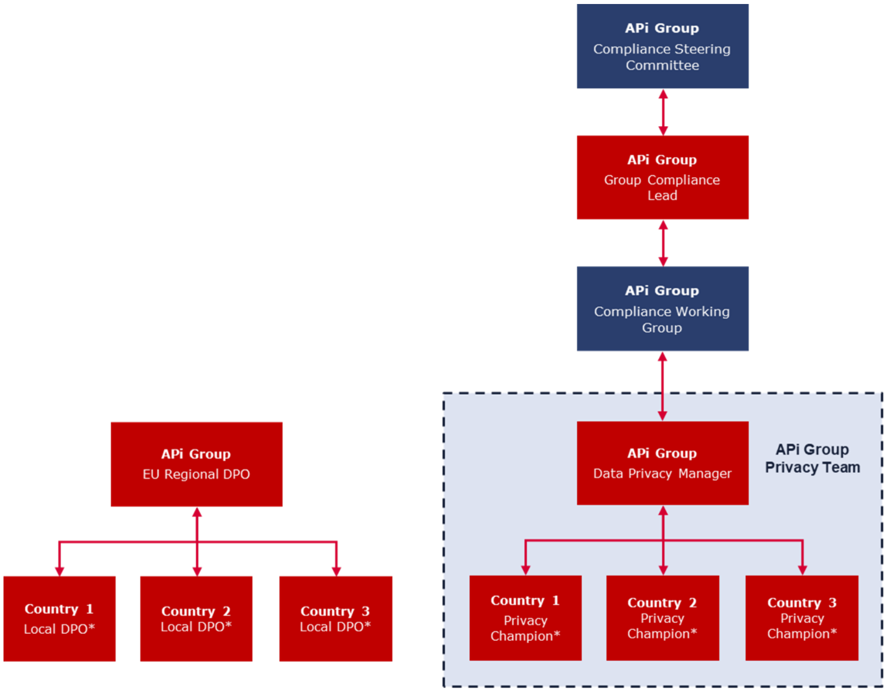
APi Group's Privacy Program is anchored on these principles, and as such, these are guidelines that should be followed by each team member. The principles are outlined in greater detail in the Program Guidelines section.

GOVERNANCE STRUCTURE

The Compliance Steering Committee acts as an advisory body that guides compliance and data privacy decisions for the organization. Its membership includes leaders from various domains of the organization such as APi Group's International, Specialty, and Safety Segments, Corporate Communication/Marketing, Compliance, Finance, HR, IT, and Legal. This committee convenes twice a year.

The Compliance Working Group is a more hands-on group that drives the implementation of Compliance and Data Privacy initiatives across all business units. The group encompasses management from APi Group and Chubb Compliance, Data Privacy and Information Security teams, and meets twice per month.

Under the guidance of the Group Compliance Lead, the APi Group Privacy team is led by the Data Privacy Manager, with future plans for support by Privacy Champions within different countries. Due to requirements under GDPR that EU Data Protection Officers (DPOs) be independent in their roles, the EU Regional DPO and Local Country DPOs are separate from the governance of the APi Group Privacy Team, but the Data Privacy Manager and EU Regional DPO work closely with one another on Privacy and Data Protection issues.



* These individuals are not full-time dedicated resources to these roles – Privacy Champions coming in future

ROLES AND RESPONSIBILITIES

Role	Responsibilities
Compliance Steering Committee	• Advisory group that directs Compliance and Privacy decisions for the organization.

Compliance Working Group	• Actively drives the rollout of Compliance and Privacy initiatives across the organization.
VP – Compliance	• Reports to the steering committee and senior management on Compliance and Privacy risks and/or exceptions • Monitors Principles implementation across APi Group • Owns internal privacy program document and privacy policies • Determines effectiveness of privacy reporting • Approves exceptions to the privacy program or privacy policies
Privacy Team	• Develops and maintains internal privacy program and policies in accordance with privacy laws, regulations and privacy principles • Performs oversight of organizational activities such as privacy impact assessments, records of processing activities, and incident response • Identifies and interprets the impact of new regulatory requirements related to privacy • Develops reporting to communicate privacy risk • Develops training content and ensures assignment/completion by business units
EU Regional DPO	• Serves as the point of contact between the company and the relevant supervisory authority • Provides advice and recommendations for high-risk processing activities and

	guidance on the interpretation of Data Protection regulations in the EU/UK
Business Units/Operating Companies	• Develop and maintain procedures and controls in accordance with privacy program requirements and privacy policies • Collect, store and share personal data in accordance with privacy program requirements and privacy policies • Route potential privacy incidents or concerns through the correct processes/channels • Ensure staff completes training

COMPONENTS OF THE APi GROUP PRIVACY PROGRAM

APi Group's Privacy Program consists of the following parts:

- Policies and Procedures;
- Identifying and Assessing Privacy Risk;
- Monitoring and Controlling Privacy Risk; and
- Reporting.

MINIMUM REQUIREMENTS

- **Policies and Procedures**
    - Policy Management
        - Development of clear, comprehensive, and actionable privacy policies that meet the requirements of relevant laws, regulations, and industry standards. This also includes defining the roles and responsibilities associated with privacy management.
        - Ensuring that the policies are effectively communicated throughout the organization.
        - Regularly reviewing and updating the policies to reflect changes in laws, regulations, technology, organizational structure, or business operations. This should be done at least once a year or following any significant change that impacts privacy management.

- **Identifying and Assessing Privacy Risk**
    - Privacy Impact Assessments (PIAs)/Data Protection Impact Assessments (DPIAs)
        - PIAs enable the organization to evaluate privacy risk within the business activities where personal data processing is involved so they may implement appropriate controls to mitigate those risks. The Privacy team provides oversight of the PIA process to challenge whether activities are permitted under applicable laws and consistent with reasonable individual, regulatory and public expectations. Each PIA includes identification of the types of data involved, applications impacted, safeguards, controls and third parties engaged. APi Group's OneTrust tool is the system of record for PIAs.
        - Where processing is likely to result in a high risk to the rights and freedoms of natural persons, each APi Group, prior to the processing, must carry out a DPIA of the impact of the processing operations on the protection of personal data.
    - Data Mapping/Records of Processing Activities (RoPAs)
        - APi Group must document RoPAs that include significant information about data processing, including data categories, the group of data subjects, the purpose of the processing and the data recipients, as outlined in the Procedure for Records of Processing Activities. APi Group's OneTrust tool is the system of record for RoPAs.
    - Third-party Risk Assessment/Management
        - When the Third Party Risk Management process identifies that an APi Group business seeks to use a new or modify the use of Third-party Supplier, where the Supplier will collect, process, transfer or have access to personal data, a Privacy Impact Assessment must be completed.
        - Contracts with Suppliers where the Supplier will collect, process, transfer or have access to personal data must include a Data Processing Agreement (DPA), which will obligate the Supplier to handle APi Group personal data according to APi Group policies or equivalent requirements.
- **Monitoring and Controlling Privacy Risk**
    - Monitor new/changing privacy regulations
        - Privacy regulations can vary greatly across different regions and industries. They also frequently change, with new rules and policies being implemented. Regularly monitoring these updates ensures that an organization remains compliant and avoids potential fines or legal actions.
        - Changes to the regulatory environment are identified by the Privacy Team and reviewed to determine the applicability of the change. The Privacy Team oversees any required implementation to ensure changes are completed prior to the effective date of the regulatory change(s).

- ○ Data Subject Rights Requests
    - ▪ Individuals are entitled to certain rights over their personal data, such as the right to access, erase, correct or restrict processing, which may vary by jurisdiction. APi Group has established various procedures for processing these requests to enable individuals to exercise these rights effectively, within the required timeframes according to applicable local law. These requests may also be referred to as Data Subject Access Requests, Consumer Requests, DSARs, Employee Access Requests, etc.
        - For requests in the EEA/UK, please consult the Internal Data Subject Rights Procedures GDPR.
        - For requests in the state of California, please consult the Internal Data Subject Rights Procedures California.
- ○ Incident and Breach Management
    - ▪ The key objective of incident and breach management is to ensure that potential or actual PI exposures are investigated, contained and reported internally and externally (as required) in a timely manner. The Privacy team participates in incident and breach management as outlined in the Data Breach Response Policy.
- ○ Information Security Program
    - ▪ Through the Information Security Program Policies, APi Group has implemented appropriate administrative, technical, and physical security measures designed to protect personal data from loss, theft, and unauthorized use, disclosure, or modification.
- ○ Record and Information Management
    - ▪ APi Group has implemented a Records and Information Management Policy in order to support the implementation and maintenance of an effective and efficient records and information management program.
    - ▪ For specific retention requirements in the EEA/UK, see the Personal Data Retention and Deletion Policy for the United Kingdom and European Economic Area.
- ○ Privacy Training and Awareness
    - ▪ Privacy training serves as a tool for educating and raising awareness among employees about privacy requirements and best practices in handling personal data.
    - ▪ The Privacy team is responsible for reviewing and updating the content of privacy related trainings, taking into consideration new or updated requirements of privacy laws and regulations.

- **Reporting**

- Reporting keeps all stakeholders, including senior management, informed about the status and effectiveness of the organization's privacy efforts.
- Each quarter, the Privacy Team reports on topics, including but not limited to, privacy incidents/breaches, number of PIAs completed, number of DPAs recommended, number of DSRRs, training completions, etc.

PROGRAM GUIDELINES

- **Lawfulness, Fairness and Transparency**
  - We should always process Personal Data in a fair, lawful and transparent manner, in line with the requirements of the applicable Data Privacy Laws.
- **Purpose Limitation**
  - We should only process Personal Data for a specified and lawful purpose. We cannot use the data for another purpose unless conditions are met.
- **Data Minimization**
  - We must ensure we are only processing the Personal Data which we truly need to conduct our business and nothing more.
- **Accuracy**
  - We should ensure Personal Data is kept up to date, and that necessary measures are in place for correcting and updating inaccurate data.
- **Storage Limitation**
  - We must not keep Personal Data for longer than we need it. It should be securely destroyed after the defined retention period.
- **Integrity and Confidentiality**
  - We must implement adequate security controls to ensure that Personal Data is protected against loss, destruction or damage.
- **Accountability**
  - We must have appropriate measures and records in place to be able to demonstrate our compliance.

PRIVACY PROGRAM ROADMAP

API Group has taken a regional approach to privacy management, which is reflected through program development in each region of EEA/UK, North America and APAC. Privacy compliance within the EEA/UK region is developed and is underway in North America and APAC, as outlined in the Privacy Workplan.

As privacy laws continue to develop and evolve, the APi Group Privacy Program will be regularly reviewed and updated.

DEFINITIONS

- "personal data" means any information that relates to a living individual and allows that individual to be identified from it (either on its own or along with other information in the company's possession). There is also a sub-category of personal data known as "sensitive personal data". Personal data is sensitive if it relates to matters such as race or ethnic origin, sexual life, sexual orientation, trade union membership, religious / political / philosophical beliefs, genetic data, biometric data, health or any criminal offence or related proceedings. Please refer to the Privacy Notice which outlines information that will constitute "personal data" and which categories of personal data are being processed.
- "privacy risk" means the risk of improper creation or collection, use, disclosure, retention, or destruction (collectively, "processing") of personal data that identifies an individual or can be reasonably used to identify an individual. Personal data includes the personal data entrusted to APi Group by its clients and employees. Privacy risk includes the risk of failure to safeguard personal data against unauthorized access or use.
- "processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

SUPPORTING DOCUMENTS

Document Name
Data Breach Response Policy
Information Security Program Policies
Internal Data Subject Rights Procedures California
Internal Data Subject Rights Procedures GDPR
Personal Data Retention and Deletion Policy for the United Kingdom and European Economic Area
Procedure for Records of Processing Activities
Records and Information Management Policy

DOCUMENT HISTORY

Version	Date	Modifications	Prepared/Revised by	Executive Sponsor