Data Privacy Governance

The protection of personal data and privacy in communications is crucial for telecommunications companies. Society's demands for better privacy have resulted in strict regulations for processing personal information to guarantee confidentiality and the right of each person to decide on the use of their personal data.

At América Móvil, we introduced our Privacy Program to enhance our protection standards and developed a Privacy Policy that governs all relevant business lines and subsidiaries, aligned with the highest international standards defining the corporate benchmark for personal data protection across operations beyond local applicable legal provisions.

Our Privacy Program is based on five fundamental initial points:

I. The creation of a Privacy Team including local experts in the laws and best practices of personal data protection.
II. A Privacy Risk Assessment to identify threats and reduce our exposure, including mitigation plans to reduce their incidence.
III. The implementation of standard policies in our operations in compliance with the highest international standards.
IV. The implementation of a comprehensive training program and a coordinated communication strategy.
V. Continuous monitoring of our subsidiaries to ensure compliance with all privacy requirements.

We have dedicated teams in every subsidiary supervising privacy issues, working on risk assessments and improving guidelines for the appropriate use of personal information. Also, they supervise the physical, technical, and administrative security measures that all our operations, employees, subcontractors, and authorized Third Parties must comply with to prevent any breach of applicable Personal Data Protection Policy, laws, rules, and regulations.

Our Privacy Team is responsible for supervising, and auditing the compliance of our Privacy Policy provisions, by periodically assessing its effectiveness.

Audits are conducted regularly and randomly in the various departments of the Company. Internal and external audits are conducted at least once every two years, as part of our certification processes. Most operations (over 80%) have been certified under ISO 27001. To learn more about our certifications, visit the Certifications Appendix in our Annual Sustainability Report.

Our Chief Compliance Officer reports to the Board's Audit and Corporate Practices Committee, the highest governance body that supervises risk management within the Group, and holds extraordinary meetings as needed.

To ensure that all América Móvil employees comply with these data security standards and privacy-related risks and procedures, in 2021 we developed the material for an online training course that is mandatory for all permanent employees (including part-time and contractors) and must be completed in 2022.

The same training protocol is also being extended to retailers and other Third Parties in our value chain. Additionally, our business partners and suppliers are required to have data protection policies or abide by our Company's Policy.

América Móvil does not rent, sell, or provide personal data to Third Parties without prior consent for purposes other than completing transactions or services.

We continue implementing communication campaigns to ensure a comprehensive understanding of our policy and best practices.

User Rights Regarding the Control of Personal Data

All our users are entitled to the following rights regarding the withholding and processing of their personal data:

I. In any processing of personal data, we will endeavor to process and limit the collection of personal data to the minimum necessary in relation to the purposes for which they are sought. Accordingly, we will make efforts to avoid processing personal data that is excessive and/or is not relevant to the purposes for which they are processed.
II. We will make every effort to limit the Processing and processing periods of sensitive data or special categories of personal data. Where possible, we will use pseudonymization techniques to mitigate the inherent risks relating to certain personal data processing.
III. We will only retain Personal Data for as long as it remains necessary for the purposes (previously informed in our Privacy Policy and Privacy Notice) of providing the requested Services and for fulfilling our legal or contractual obligations.
IV. We will securely and permanently delete personal data after the applicable retention periods have expired. Where required to do so in every jurisdiction, we will procure to inform Data Subjects about the applicable personal data retention periods for each processing activity.
V. Under applicable laws in each of the countries where we operate, Data Subjects may have the right to access their Personal Data, free of charge and in a way that is accessible, electronically, or otherwise, in a structured, machine-readable format, including a copy of such data, and to be informed of the characteristics of any Personal Data Processing activities (right of access and data portability).
VI. Users may request to rectify, modify, or update any inaccurate Personal Data.
VII. Users have the right to request the deletion of Personal Data that is no longer necessary for the purposes for which it was processed.
VIII. Users may object to the processing of Personal Data concerning them for certain specific purposes, provided such data is not necessary for the performance of our contractual obligations and/or the provision of Services (object); and to request the establishment of safeguards to prevent their alteration, erasure, or suppression (restriction of Processing).

América Móvil is committed to responding without undue delay to the requests of our users regarding the exercise of the following rights, and to their claims or complaints, provided they are within our purview. Each of our subsidiaries will establish the means, procedures, deadlines, and formats, in accordance with local applicable laws.

Data Breach prevention and Incident Response Plan

We seek to implement appropriate physical, technical and organizational measures, both when determining of the means for processing personal data and at the time of processing itself, considering the state of the art, the cost of implementation and the nature, scope, context, and purposes of processing, as well as the risks that certain processing could imply for the rights of data subjects.

Furthermore, we apply appropriate technical and organizational measures to ensure that, by default, only personal data which is necessary for each specific purpose of the processing is processed.

We monitor on an ongoing basis the proper operation of our systems, applications, and technological infrastructure to ensure that privacy and personal data are protected appropriately, including access controls and encryption/de-identification techniques.

Notwithstanding, the security and/or confidentiality of personal data may be compromised by certain incidents. In such cases, we will act in accordance with our Information Security Policy and with such other policies and/or procedures as designated for each operation.

In addition, if we determine that a security incident may have compromised the fundamental rights of the data subjects we will, as required by law, notify the security incident to the data subjects concerned and/or to the supervisory authority having competent jurisdiction to prevent any further impact on their rights.

In the event of a privacy or security incident, we commit to analyze and implement any corrective measures that are deemed necessary within our operations to prevent a breach from happening again.

Failures to comply with our Privacy Policy may lead to administrative, labor, or even criminal sanctions, both for employees and Third Parties, depending on the seriousness of the particular event, which will be determined in accordance with internal workplace regulations and/or local applicable laws, rules, and regulations.

Within América Móvil, the Ethics Committee of each Subsidiary shall be the authority of last resort to determine sanctions in the event of a breach to this Policy, without prejudice to such defaults being also penalized by applicable laws and authorities having jurisdiction.

Privacy Enhancing Technologies and Services that Contribute to Cyber Resilience

We integrate data protection safeguards into our product and services development, particularly if it involves new technologies. If a type of processing is likely to pose a high risk to the rights of data subjects owing to its nature, scope, context, or purpose, we carry out a Personal Data Protection impact assessment, prior to processing, in accordance with international best practices and local applicable regulations.

In addition, to contribute to our customers' cyber-resilience we developed a business-line operated by Scitum[1] (subsidiary of Telmex) that offers comprehensive cybersecurity solutions, covering: cyberintelligence, risk and cybersecurity governance, end-to-end application security management, protection of digital infrastructure, human factor management, as well as threat detection and response.

[1] If you need more information on Scitum, please visit our website: https://www.scitum.com.mx/