



GLOBAL DATA PROTECTION AND TRANSFER POLICY

Legal & Compliance
June 1, 2024

GLOBAL DATA PROTECTION AND TRANSFER POLICY

I. Introduction.

The management of the Global Data Protection and Transfer Policy at Marco Consultora México, S.A. de C.V., Marco Marketing Consultants Corp, Marco Colombia SAS, M2 Consultoría Em Marketing LTDA, Consultora Marco Chile Compañía Limitada, Marco Marketing Consultants Perú Sac, and Consultora Marco S.A. (hereinafter referred to as Marco Mkt) is based on the fundamental right to privacy and the protection of personal data.

This right is recognized in various international instruments, including the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and the European Convention on Human Rights, which establishes the fundamental right to data protection.

The regulation of this right varies by jurisdiction:

- **Mexico:** the primary legal framework includes the Federal Law on the Protection of Personal Data Held by Private Parties, its Regulations, as well as guidelines on Privacy Notices, the Code of Ethics, and data security recommendations.
- **Brazil:** data protection is governed by the General Data Protection Law (LGPD).
- **Colombia:** the primary law on personal data protection is Statutory Law 1581 of 2012.
- **Chile:** personal data protection is regulated under Law No. 19.628 on the Protection of Private Life.
- **Peru:** the applicable legal framework consists of Law No. 29733 (Personal Data Protection Law) and its Regulations (approved by Supreme Decree No. 003-2013-JUS).
- **Argentina:** Law No. 25.326 on Personal Data Protection establishes the general principles for data processing, along with Decree 746/2018, which regulates data protection within the National Executive Branch.
- **United States:** data protection is not governed by a single federal law but rather a combination of federal and state laws addressing specific aspects of privacy and data security. Key federal laws include:
 - HIPAA (Health Insurance Portability and Accountability Act) – governing health information,
 - COPPA (Children’s Online Privacy Protection Act) – regulating data protection for children under 13,
 - GLBA (Gramm-Leach-Bliley Act) – applying to financial institutions,
 - FERPA (Family Educational Rights and Privacy Act) – protecting student educational records and
 - FCRA (Fair Credit Reporting Act) – regulating consumer credit information.
- In Chile, personal data protection is regulated under Law No. 19.628 on the Protection of Private Life.
- In Peru, the applicable legal framework consists of Law No. 29733 (Personal Data Protection Law) and its Regulations (approved by Supreme Decree No. 003-2013-JUS).
- In Argentina, Law No. 25.326 on Personal Data Protection establishes the general principles for data processing, along with Decree 746/2018, which regulates data protection within the National Executive Branch.

This policy also considers all relevant updates and amendments to these regulations.

II. Purpose.

Protecting the personal data of individuals associated with the company is essential to ensuring lawful, controlled, and informed data processing while safeguarding privacy. At Marco Mkt, we implement strict regulations on the handling of personal data to guarantee compliance with data protection standards and prevent unauthorized access. Our policy also ensures secure data transfers in accordance with applicable laws and best practices.

III. Scope and Application.

ELABORÓ	REVISÓ	APROBO
Global Legal & Compliance Manager	Global Legal & Compliance Manager	Gonzalo Elorriaga Varas Chief Financial Officer

This Policy applies to all Marco Mkt subsidiaries in connection with the processing of personal data of applicants, employees, suppliers, clients, and third parties with whom the company has a relationship.

The Personal Data Protection Committee is responsible for drafting and enforcing this Policy. However, this document is binding on all Marco Mkt employees, particularly those who collect, store, use, and/or transfer personal data.

IV. Key Definitions.

- a. Information Asset: In the context of information security, this refers to any information or element related to its processing (systems, storage media, premises, files, employees, etc.) that has value for the company.
- b. Privacy Notice: A physical, electronic, or any other format document generated by Marco Mkt's administrative area, which is provided to the data subject before their personal data is processed.
- c. Database: An organized collection of personal data related to an identified or identifiable individual.
- d. Encryption: Data that is written using letters, symbols, or numbers that can only be understood if the necessary cryptographic key is available for decryption.
- e. Employee: A person who has an employment relationship with Marco Mkt, either directly or through a third party, under any type of subordinate contractual arrangement.
- f. Informed Consent: A declaration of the data subject's will, given after receiving a description of the data protection process and their rights, through which data processing is carried out.
- g. Personal Data: Any information concerning an identified or identifiable individual, which may be expressed in numerical, alphabetical, graphic, photographic, acoustic, or any other form. Examples include name, surname, marital status, place and date of birth, address, telephone number, email, education level, salary, CURP (Clave Única de Registro de Población), DNI (Documento Nacional de Identidad), Citizenship Card or Identity Card, RUN (Rol Único Nacional), CPF (Cadastro de Pessoas Físicas), SSN (Social Security Number), or other national identification numbers. Personal data describes and identifies an individual, distinguishing them from others.
- h. Sensitive Personal Data: Information that affects the most intimate sphere of the data subject or whose improper use could lead to discrimination or pose a serious risk. Sensitive data includes information revealing racial or ethnic origin, present or future health status, genetic data, religious, philosophical, and moral beliefs, union membership, political opinions, or sexual orientation.
- i. Third Party: Any individual or legal entity external to the company that provides services or performs any work for Marco Mkt. This category includes suppliers, business partners, government institutions, and/or regulatory authorities.
- j. Data Subject: The individual to whom the personal data belongs.
- k. Processing: The collection, use, disclosure, or storage of personal data by any means. "Use" includes any action related to access, management, utilization, transfer, or disposition of personal data.
- l. Transfer: Any communication of personal data to individuals other than the data controller or data processor.
- m. Information Transfer: The exchange of information between internal company departments or between Marco Mkt and any third party.
- n. Marco Mkt and/or the Company: Marco Consultora México, S.A. de C.V., Marco Marketing Consultants Corp, Marco Colombia SAS, M2 Consultoría Em Marketing LTDA, Consultora Marco Chile Compañía Limitada, Marco Marketing Consultants Perú Sac, Consultora Marco S.A.

ELABORÓ	REVISÓ	APROBO
Global Legal & Compliance Manager	Global Legal & Compliance Manager	Gonzalo Elorriaga Varas Chief Financial Officer

V. Policy Guidelines.

- Establish procedures for receiving, processing, tracking, and timely handling of requests submitted by data subjects.
- Supervise and disseminate internal procedures, ensuring compliance with the activities and life cycles of databases containing personal information, in accordance with this Policy and applicable regulations.
- Support Marco Mkt's relevant departments in addressing data subjects' requests to exercise their rights as defined in this Policy.
- Implement necessary measures for the correct execution of this Policy.
- Enforce this Policy and comply with internal procedures and all applicable legal provisions related to data protection, as well as designate a responsible party to manage requests for exercising rights.

VI. Fundamental Principles of Personal Data Processing.

- a. **Accuracy and Retention:** Our systems are regularly updated, and mechanisms are provided to correct or delete inaccurate personal data. Additionally, data is not retained beyond the time necessary to fulfill the legal purpose of its processing.
- b. **Confidentiality and Integrity:** Personal data is kept secure and protected throughout the entire processing cycle. However, in the event of a security incident or data breach, we will respond promptly and appropriately, including timely notification as required.
- c. **Transparency:** Data subjects are adequately informed when their personal data is processed. We clearly explain why we need their data, how it will be used, and the measures taken to process and protect it.

VII. General Guidelines.

The following guidelines apply to all Marco Mkt departments and third parties that manage personal data records and databases:

- **Lawfulness:** The collection and processing of personal data from clients, suppliers, applicants, and employees must be conducted lawfully, in accordance with applicable regulations. The acquisition of data through deceptive or fraudulent means is strictly prohibited. All personal information provided to Marco Mkt organizations and entities must be used as specified in the Privacy Notice and applicable legal provisions.
- **Informed Consent:** It is mandatory to disseminate the corporate Privacy Notice, informing clients, suppliers, and employees about the data collected and its purpose. The Privacy Notice must be made available to data subjects through the designated channels. Consent to privacy notices may be explicit or implied, following the applicable legal provisions on personal data protection and transfer, as well as this Policy.
- **Proportionality:** Only the personal information necessary for operational functions will be collected. Its processing must be justified, with documentation supporting the necessity and adequacy of the data collected.
- **Confidentiality:** All contracts with clients, suppliers, and employees must include a confidentiality clause regarding personal data, approved by the Compliance Officer.
- **Communication:** The essential characteristics of data processing must be disclosed to data subjects through Privacy Notice. Any modifications or updates to this document must be communicated to all stakeholders within three (3) business days through Marco Mkt's official channels.
- **Data Quality:** Database administrators are responsible for keeping client, supplier, and employee data accurate and up-to-date. The retention period must be strictly limited to what is necessary. Once this period expires, data must be blocked for the sole purpose of determining potential liabilities related to its processing, until the expiration of legal or contractual retention periods, after which the data must be deleted. If data is no longer needed for its original purpose, it must be removed from databases and systems, with records maintained of the deletion process. Administrative, technical, and physical security

ELABORÓ	REVISÓ	APROBO
Global Legal & Compliance Manager	Global Legal & Compliance Manager	Gonzalo Elorriaga Varas Chief Financial Officer

measures must be in place to protect personal data against theft, damage, loss, alteration, destruction, unauthorized access, or misuse.

- **Data Sharing and Transfers:** Every exchange of electronic information belonging to Marco Mkt with third parties must be backed by a written document (agreement or contract), including a confidentiality and non-disclosure clause for the information provided.
- **Third-Party Data Exchange:** Any exchange of Marco Mkt's electronic information with third parties must be supported by a written agreement (contract or agreement), including a confidentiality and non-disclosure clause. Requests for data exchange may come from Marco Mkt employees, third parties, or external entities requiring interoperability due to legal or governmental directives. The exchange of information classified as strictly confidential or sensitive must be conducted through encrypted channels that ensure confidentiality and compliance with this Policy. Exceptions to data disclosure must comply with the applicable laws and regulations in each jurisdiction.
- **Data Transfers to Clients and Suppliers:** A confidentiality or data transfer agreement must be signed before allowing any client or supplier access to Marco Mkt's private, confidential, or proprietary information. Awareness campaigns on secure information sharing must be periodically conducted for clients and suppliers. Monitoring of transferred data will be conducted to detect any incidents and implement corrective or preventive actions as necessary.
- **Digital or Electronic Data Transfers:** Sensitive or critical data must only be provided under a signed agreement, contract, or data transfer arrangement, with prior verification of the recipient's authorization and identity. Internal information-sharing tools must be designated with access control and privilege mechanisms.
- **Data transfers must use secure authentication mechanisms and encryption protocols:** Authentication credentials must be shared via secure channels and should never be left on voicemail or in unsecured locations. Preferably, confidential files should not be sent to public email domains unless pre-verified. USB storage devices must not be used for information transfers, as their usage will be blocked; alternative secure sharing methods will be provided.
- **Physical Data Transfers:** Physical documents containing personal data must be properly labeled, and their transfer must include a receipt acknowledgment, listing the documents provided and an estimated return date. A logbook must be maintained for the delivery and receipt of physical media containing sensitive information. The recipient of the physical data must ensure its security during transport and proper storage while in their possession. Special-use documents must be protected against environmental threats while in the recipient's custody. For internal data transfers, only Marco Mkt's authorized communication channels should be used, such as official letterheads and memoranda.
- In all cases, necessary precautions must be taken to maintain confidentiality, such as using sealed envelopes without reference to the contents.

VIII. Compliance.

To prevent a range of risks related to information breaches and its handling, Marco Mkt has established mechanisms to guide the actions of all employees. These policies and tools are accessible to employees on the company's official platform. Below are the main ones:

1. Code of Ethics.
2. Information Security Policy.
3. Confidentiality clause included in all contracts with clients and suppliers.
4. Confidentiality agreements are carried out with clients, suppliers, business partners, and employees.
5. Privacy Notice.
6. Privacy and Personal Data Protection Policy.
7. Mobile Device and Teleworking Policy.

ELABORÓ	REVISÓ	APROBO
Global Legal & Compliance Manager	Global Legal & Compliance Manager	Gonzalo Elorriaga Varas Chief Financial Officer

8. Password Management Policy.

Marco Mkt's policies allow employees, suppliers, clients, and any third party to recognize potential risks in transferring confidential information. They also facilitate avoiding prohibited conduct when evident and seeking immediate advice in case of doubts. Additionally, they will have access to the Protection and Transfer Procedure.

Failure to comply with this Policy will result in the corresponding internal consequences, which will be determined after evaluating the violation committed. Furthermore, legal action may be taken in accordance with the applicable laws in the country where non-compliance occurred.

IX. Protection and Transfer Procedure.

This must be subject to the following parameters and process:

a. The personal data owner or their legal representative will be the only ones authorized to request the exercise of this procedure from Marco Mkt through any of the following means:

- Via email at datospersonales@marcomkt.com;
- In person at Marco Mkt's offices; and
- Through the website www.marcomkt.com.

b. The request must be submitted to the Personal Data Protection Committee via the email indicated above, which will verify that it contains the following:

- The name of the owner, phone number, and physical address, email, or another means to communicate the response to their request;
- Documents proving the identity or, where applicable, the legal representation of the owner (valid photo ID, passport, professional license);
- A clear and precise description of the personal data and/or the reasons for which the request is being made;
- Any other element or document that facilitates locating the personal data;
- If the request seeks to establish an enforceable guideline under the applicable data protection laws of their country, the owner must also indicate the modifications to be made and provide documentation supporting their request;
- The procedure described above is free of charge, except for justified shipping expenses (courier services), which may be borne by the owner.

c. If the request does not meet any of these formal requirements, it will be rejected, and the requester will be informed.

d. If the request meets all formal requirements, it will be processed according to the following procedure:

e. The Personal Data Protection Committee will inform the owner or their legal representative, within a maximum period of 20 (twenty) business days from the date of receipt of the access, rectification, cancellation, or opposition request, of the adopted resolution. The response will be provided via the means indicated in the request.

f. If the request is deemed valid, it will be executed within 15 (fifteen) business days following the date of communication of the response. The above deadlines may be extended once for an equal period if justified by the circumstances.

g. In the case of access requests to personal data, prior verification of the requester's identity or legal representation must be conducted. The data will be made available to the owner through physical copies, electronic documents, or other means. This right will be granted free of charge once per year; additional copies or requests within a 12-month period may be subject to costs.

h. The Personal Data Protection Committee may request assistance from individuals managing personal data on behalf of Marco Mkt to implement necessary measures to comply with the request.

ELABORÓ	REVISÓ	APROBO
Global Legal & Compliance Manager	Global Legal & Compliance Manager	Gonzalo Elorriaga Varas Chief Financial Officer

- i. Access to personal data may be denied in the following cases:
- If the requester is not the data owner or their legal representative is not duly accredited;
 - If the requested personal data is not found in the company's database;
 - If there is a legal impediment or an authority's resolution restricting access, rectification, cancellation, or opposition to the data; and
 - If the request has already been processed previously.
- j. The Personal Data Protection Committee must inform the requester of the decision within the established deadlines and provide any relevant supporting documentation.
- k. If the data owner needs to submit additional documentation related to their request, they may do so via email at datospersonales@marcomkt.com.
- l. The Personal Data Protection Committee will use the collected personal data exclusively to process requests received under this procedure.

X. General Recommendations.

Everyone, including clients, suppliers, and employees of Marco Mkt, owns their personal data and decides how, when, to whom, and for what purpose they share their personal information. It is crucial to safeguard this information for security reasons and protect it from misuse, such as identity theft, unauthorized transmissions, or unlawful access.

We encourage collaboration with Marco Mkt to gain knowledge in this area, contribute to improved information security, and protect all personal data that may be processed by our company in daily interactions with visitors, clients, employees, suppliers, or any other legal relationship involving Marco Mkt.

For any questions, suggestions, or additional information on this subject, please contact our Personal Data Protection Committee at datospersonales@marcomkt.com

Last Updated: May 27, 2024.

ELABORÓ	REVISÓ	APROBO
Global Legal & Compliance Manager	Global Legal & Compliance Manager	Gonzalo Elorriaga Varas Chief Financial Officer