Classification: Public

Personal data protection and privacy policy

Meta Policies are documents that aim to guide the company's relationships through pre-established principles.

Purpose

“Human Growth with Technology.”

Values

- We are people serving people.
- We think and act like owners.
- We are driven by performance.
- We grow and learn together.
- We strive for excellence and simplicity.
- We inspire, encourage, and celebrate a culture of innovation.

What can I find in this document?

1.

This Policy is an integral part of the corporate management system and aims to reinforce META's commitment to society, ensuring that all stages of its activities comply with the General Personal Data Protection Law (LGPD).

META recognizes the importance of privacy and is committed to the principles of good faith, purpose, adequacy, necessity, free access, data quality, security, prevention, non-discrimination, accountability, and transparency when processing personal data.

2. Scope

This document covers all personal data processing of customers, suppliers, shareholders, business partners, employees, and other individuals carried out by META and indicates the guidelines to be followed, whether acting as Controller or Operator, both in digital and physical environments.

META, as a Controller, processes the personal data of its employees, customers, business contacts, shareholders, or users of its web channels. When acting as an Operator processing personal data contained in various types of documents, META will always proceed in accordance with the instructions provided by the Controller, such as in the shared center activities of Netrin and Meta Ventures, and also in the processing of customer databases (technical assistance or software testing, for example).

This Personal Data Protection and Privacy Policy applies to META TI and its wholly owned subsidiaries, wheter directly or indirectly controlled, conducting business nationally and/or internationally[1].

1 The LGPD applies to any processing operation carried out in the national territory, or even outside the national territory, regardless of where the processing agents are based or where the data is located, provided that: a) the processing activity is aimed at offering or supplying goods or services in Brazilian territory; b) the processing activity is aimed at processing data of individuals located in Brazilian territory; c) the personal data subject to processing has been collected in Brazilian territory.

3. References

General Personal Data Protection Law (Law No. 13,709, of August 14, 2018);

ABNT NBR ISO/IEC 27001:2013;

ABNT NBR ISO/IEC 27701:2019.

4.

Personal Data: Any information relating to an identified or identifiable natural person (data subject); A natural person who can be identified, directly or indirectly, in particular by reference to information such as a name, an identification number, location data, electronic identifiers, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person is considered identifiable.

Data subject: The natural person to whom the personal data being processed refers, i.e., the individual.

Identifiable Personal Data: This is any information that identifies or can identify a person, such as geolocation, IP (Internet Protocol) address, car license plate, among others.

Sensitive Personal Data: This is personal data that is, by its nature, particularly sensitive, as it invades a greater level of privacy of the individual and may create significant risks to fundamental rights and freedoms. According to the law, sensitive personal data includes:

i. Data on racial or ethnic origin;

ii. Data on religious beliefs;

iii. Data on political opinion;

iv. Data on trade union membership;

v. Data concerning health or sex life;

vi. Genetic or biometric data, when linked to a natural person.

Processing: An operation or set of operations performed on personal data or sets of personal data, whether by automated means or not, such as those relating to collection, production, reception, classification, use, access, reproduction, transmission, distribution, processing, filing, storage, elimination, evaluation or control of information, modification, communication, transfer, dissemination or extraction.

Life Cycle: Refers to the stages of data processing, including collection, processing, transfer, storage, termination of processing, and disposal.

Consent: Free, informed, and unequivocal statement by which the data subject agrees to the processing of their personal data for a specific purpose.

Anonymization: Use of reasonable technical means available at the time of processing to transform personal data into anonymous data. In this case, data loses the possibility of direct or indirect association with an individual. Thus, anonymization irreversibly de-identifies personal data, making identification impossible using reasonable time, cost, and technology. The principles of personal data processing do not apply to anonymous data, as it is no longer personal data.

Processing agents: the controller and the operator. Controller: a natural or legal person, under public or private law, who is responsible for decisions regarding the processing of personal data.

Processor: a natural or legal person, public or private, who processes personal data on behalf of the controller.

Personal Data Processing Officer or "DPO" - Data Protection Officer: a person appointed by the controller to act as a communication channel between the controller, data subjects, and the National Data Protection Authority.

National Data Protection Authority (ANPD): public administration body responsible for ensuring, implementing, and supervising compliance with this Law.

Blocking: temporary suspension of any processing operation, by storing the personal data or the database.

Deletion: exclusion of data or a set of data stored in a database, regardless of the procedure used.

Shared use of data: communication, dissemination, international transfer, interconnection of personal data or shared processing of personal databases by public bodies and entities in the exercise of their legal powers, or between them and private entities, reciprocally, with specific authorization, for one or more types of processing permitted by these public entities, or between private entities.

Personal data protection impact report (RIPD): documentation from the controller containing a description of the personal data processing procedures that may pose risks to civil liberties and fundamental rights, as well as measures, safeguards, and risk mitigation mechanisms.

5. General and specific guidelines

META's commitment to personal data protection legislation exists at all stages of information processing, integrating transparency, privacy, and protection into the possibilities for processing personal data, always respecting the life cycle of information, both in physical and digital environments.

META has systems and equipment in place to ensure the security of the personal data processed, creating and updating procedures capable of preventing unauthorized access, accidental loss, and/or destruction of personal data. META will maintain the integrity, confidentiality, and relevance of personal data based on the purpose of processing, providing management to ensure the privacy program and sufficient resources to develop and support operation and continuous improvement.

Appropriate security mechanisms designed to protect personal data must be used to prevent it from being stolen, misused, or violated.

The responsibility for ensuring the proper processing of personal data lies with everyone who works for or with META and who has access to personal data processed by META.

META conducts annual training on personal data protection issues to ensure that employees are aware of their obligations in this area.

META will lawfully carry out the following data processing activities: collection, production, reception, classification, use, access, reproduction, transmission, distribution, processing, filing, storage, elimination,

evaluation or control of information, modification, communication, transfer, dissemination or extraction.

META, when processing the personal data of its employees, customers, shareholders, web portal users, partners, business contacts, and other data subjects, will act as the Controller. In this scenario, the data collected may include:

i. Registration information: name, date of birth, gender, age, address, telephone number, email address, number of children, information about dependents, identification documents, visas, work permits, emergency contacts, marital status, life insurance beneficiaries, photos or images;

ii. Financial information: compensation amounts, benefits and retirement plans, bank account, stock purchase plan, stocks, travel expenses;

iii. Administrative employment information: resume, application form, evaluations, security records, absence records, medical records, accident reports, personal development reviews, official identification numbers, skill records, driver's license;

iv. Employee location information: internal movement records, badge usage;

v. Information about website access and IT details: identification of websites accessed, identification of the machine used;

The processing of META employee data will have the following purposes: compliance with legal or regulatory obligations, maintenance of employment contracts, regular exercise of rights in judicial, administrative, or arbitration proceedings.

i. To achieve the intended purpose, META shall strive to collect as little personal data as possible.

ii. To achieve the intended purpose, META will sometimes need to transfer data to third parties.

Employees, collaborators, shareholders, web portal users, partners, customers, and other data subjects, when data is collected and when legally required, will be asked for their consent and informed about the data lifecycle, as well as the possibility of transferring such information to third parties.

The collection of sensitive personal data by META will be subject to compliance with legal or regulatory obligations by the controller, the regular exercise of rights, including in contracts and in judicial, administrative, and arbitration proceedings, or the specific and explicit consent of the data subject.

META is particularly concerned with the rights of children and adolescents, which is why the collection of personal data from minors under 12 years of age (children) will be subject to specific and highlighted consent given by at least one parent or legal guardian (article 14, § 1 of the LGPD), while also observing the best interests of the child. For adolescents (12 to 18 years old), the processing will occur according to the other legal bases for processing (Articles 7 and 11 of the LGPD), also observing the best interests of the adolescent.

i. Such types of personal data will only be processed when: a) hiring minor apprentices and interns; b) processing information on dependents of META employees; c) interacting with web portals; d) providing services to META customers.

ii. META shall keep public information about the types of data collected, how it is used, and the procedures for exercising rights.

META will ensure that personal data will only be processed in accordance with the purposes for which it was originally collected, implying the existence of a purpose prior to the collection activity.

i. If META needs to process the personal data collected for another purpose, the company doing so must notify the data subject of the change, the new purpose of processing, and the legal basis used, and, if necessary, obtain the consent of the data subjects through a document written in a clear and concise manner. The request must include the original purpose for which the data was collected and also the new or additional purpose(s). The request must also include the reason for the change in purpose(s).

It is META's responsibility, within the processing carried out, to identify the possibility of applying legitimate interest for the processing of personal data. However, such legal basis will only be used when the personal data protection impact report has been duly carried out and authorized by the Data Protection Officer.

META shall keep personal data in a structured manner, enabling the mapping and identification of its location, as well as information about its life cycle.

i. META will seek ways to ensure that personal data stored electronically is protected by passwords and/or encrypted.

ii. Personal data present on digital media (CD/DVD/USB sticks) or paper documents will be catalogued and stored in a locked cabinet, which has infrastructure specially developed to prevent possible security breaches. The law requires the same type of treatment to be given to digital media.

META shall keep a record of all personal data processing operations it carries out:

i. Each META department will be responsible for completing and keeping up to date the document entitled Treatment Record, with regard to the technical fields relating to the flow;

ii. META's IT department will be responsible for filling in the fields related to technical safeguards and storage time;

iii. META's Data Protection Officer will be responsible for legal issues and matters requiring legal and regulatory knowledge and knowledge of the applicability of data security and privacy rules;

iv. The document entitled Processing Record shall clearly and objectively indicate the responsibilities of those involved in filling it out.

The period of time during which data is stored and retained may vary depending on the purpose for which the information is used. However, there are legal requirements that require data to be retained for a certain period of time. Therefore, unless there is a specific legal requirement, data will be stored and retained only for the period necessary for the purposes for which it was collected.

The end of the processing and, consequently, the definitive disposal of personal data will occur in the following situations:

(i) Verification that the purpose of the processing has been achieved;

(ii) That the period for processing the specified data has expired;

(iii) When the data subject revokes consent;

(iv) When the National Data Protection Authority so determines.

The retention of personal data is authorized in the following situations:

i. Compliance with legal or regulatory obligations by the controller;

ii. Study by a research body, ensuring, whenever possible, the anonymization of personal data;

iii. Transfer to a third party, provided that the data processing requirements of national legislation are respected; or

iv. Exclusive use by the controller, with access prohibited to third parties, and provided that the data is anonymized.

When acting as an Operator, META shall process data in accordance with the instructions provided by the Controller, for a specific purpose and in accordance with the legal requirements for such activity.

i. The responsibility for determining the valid legal basis for data processing shall lie with the Controller, and the Operator may, in this case, refuse to process the data when there is inconsistency between the purpose and the processing.

META, in view of the need to comply with legal or regulatory obligations, maintain and execute contracts, exercise rights in judicial, administrative or arbitration proceedings, or through legitimate interest, may share data with other companies and even with the public administration.

i. META contractually requires these third parties to provide appropriate technical and organizational guarantees to protect personal data, so that the processing meets the requirements of applicable law and ensures the security and protection of the rights of data subjects.

ii. When transferring personal data externally, the third party must keep records of the processing carried out and ensure that the purpose initially intended is not altered.

iii. Regular inspections shall be carried out at the companies receiving the personal data. META shall assess the conditions offered for the processing of transferred personal data. Such inspections shall be documented so that, if necessary, they can be presented as evidence in future proceedings.

iv. If minor inconsistencies are found, META may provide a deadline for third-party companies to comply with legal requirements and/or contractual requirements. In this situation, the contracting company will assume any risks during the period of compliance by the supplier/outsourced service provider.

v. If a major inconsistency is detected, the possibility of immediate termination of the contract shall be considered, avoiding any risk to the personal data shared.

vi. Transfer of digital and physical media must be carried out using secure means of transport, guaranteed against loss and unauthorized access.

For international data transfers, META must obtain the data subject's consent in a specific and prominent manner for the transfer, with prior information about the international nature of the operation, clearly distinguishing it from other purposes.

If consent is not obtained, international transfer may only take place in the following cases:

i. To countries or international organizations that provide a level of personal data protection similar to that provided by national legislation;

ii. When the Controller offers and provides guarantees of compliance with the principles, the rights of the data subject, and the data protection regime in the same manner as national legislation;

iii. When the transfer is necessary for international legal cooperation between public intelligence, investigation, and prosecution agencies, in accordance with international law instruments;

iv. When the transfer is necessary for the protection of the life or physical safety of the data subject or third parties;

v. When the national authority authorizes the transfer; (vi) When the transfer results from a commitment made in an international cooperation agreement;

vi. When the transfer is necessary for the execution of public policy or legal assignment of public service;

vii. For compliance with a legal or regulatory obligation by the controller;

viii. When necessary for the performance of a contract or preliminary procedures related to a contract to which the data subject is a party, at the request of the data subject;

ix. For the regular exercise of rights in judicial, administrative, or arbitration proceedings;

META will create and appoint a Data Protection Committee, which will be formed by professionals appointed from the following areas of the company: Legal and Compliance, Information Security, Human Resources, Communication, and Projects/Services, and chaired by the Data Protection Officer or "DPO."

i. The identity and contact information of the person in charge must be disclosed publicly, in a clear and objective manner, preferably in the Privacy Policy of the web channels.

ii. The Committee and DPO will also be responsible for working with META VENTURES and NETRIN. The activities of the Personal Data Protection Officer consist of:

   a. Accepting complaints and communications from data subjects, providing clarifications and taking appropriate measures;

   b. Receiving communications from the national authority and taking the necessary measures, requesting internal departments to comply;

   c. Guiding, through the Data Protection Committee, the company's employees and contractors on the practices to be taken in relation to personal data protection; and

   d. When necessary or as required by law, request the responsible department to prepare the Data Protection Impact Report and validate such document;

   e. Perform other duties determined by the controller or established in complementary rules;

   f. Evaluate the data processing record whenever there is any change in processing. In case of inconsistency in the analysis or risk in the processing, you may request the department responsible for the data to prepare a Data Protection Impact Report for the processing in question.

   g. Validate the actions of the Data Protection Committee;

The Data Protection Committee is responsible for the company's compliance with the law and its activities consist of:

i. Holding biweekly meetings and preparing minutes;

ii. Developing key success indicators to evaluate the implementation of the data protection program, seeking excellence in the lawful processing of data;

iii. Develop a mechanism for informing data subjects when such information is collected.

iv. Developing and maintaining policies, rules, procedures, and standards of conduct on the subject and ensuring that personal data is collected legally;

v. Conduct annual training on personal data protection issues to ensure that employees are aware of their obligations in this area;

vi. Interact with internal departments to resolve legal issues related to privacy and data protection;

vii. Investigate and investigate possible data privacy violations, as well as formalize and take appropriate corrective measures in a timely manner;

viii. Ensure and provide support to the Data Protection Officer in preparing communications to data subjects and the National Data Protection Authority;

ix. Implement guidelines and develop the Register of personal data processing operations;

x. Implement guidelines and develop the Personal Data Protection Impact Report;

xi. Develop and implement a reasonable access mechanism to allow data subjects to request the correction, deletion, or transmission of their personal data, if appropriate or required by law, or in cases of withdrawal of consent;

xii. Maintain a record of requests to correct, change, or destroy personal data;

xiii. Implement and ensure that data subjects' requests for confirmation of data processing are complied with within 15 days, as required by law. All other requests will be responded to within a reasonable time, until a decision is made by the National Data Protection Authority (ANPD).

xiv. Ensure that operators or other controllers to whom personal data has been transmitted are informed, in a timely manner, of requests for erasure, rectification, or other interactions arising from the rights of the data subject;

xv. Prepare, when collecting personal data from a person under the age of 12 (child), the Legal Guardian Consent Form, and ensure that the legal guardian's consent is given before collection.

META guarantees data subjects the exercise of their rights, upon request, to:

i. Confirmation of the existence of processing;

ii. Access data;

iii. Correct incomplete, inaccurate, or outdated data;

iv. Anonymize, block or delete unnecessary, excessive or unlawfully processed data in accordance with Law No. 13,709;

v. Transfer data to another service or product provider, upon express request and in compliance with commercial and industrial secrecy, in accordance with the regulations of the controlling body;

vi. Access information about which public and private entities with whom the controller has shared data.

vii. Upon request, Data Subjects have the right to obtain from META the deletion of their personal data. When META acts as Controller, the Data Protection Committee shall take the necessary measures (including technical measures) to inform third parties who use or process such data to comply with the request.

When META verifies a suspected or actual personal data breach, after investigation by the Data Protection Committee, if there is any risk to the rights and freedoms of data subjects, the Personal Data Processing Officer shall notify the ANPD without undue delay and, where possible, within 48 hours.

META, through its Data Protection Committee and Officer, will update the website's Privacy Policy every six months or at any time when a significant change occurs.

META reserves the right, at any time, to update or modify this Policy and the privacy policies by publishing an updated version on its respective portals and websites. In the event of a modification to this Policy or any privacy policy, the modifications will only apply to personal information collected after the publication of the revised version of this Policy or privacy policy.

META considers the risk to individuals whose personal data is processed by conducting a thorough risk analysis that supports decision-making and the personal data impact report (PDIR).

6. Responsibilities

DATA PROTECTION COMMITTEE AND DATA PROTECTION OFFICER The Data Protection Committee, together with the Data Protection Officer, is responsible for reviewing and approving this Policy and its annexes annually or whenever there is a significant change in the processing of personal data carried out by META. Whenever there is a significant change to this Policy or the Privacy Policy, the necessary privacy notices will be made.

INFORMATION USERS It is the responsibility of information users to read, understand, and comply fully with the terms of the Personal Data Protection and Privacy Policy, as well as other applicable personal data protection rules, policies, and procedures. Report to the DPO any event that violates this Policy or puts personal data at risk.

7. Disciplinary measures

Failure to comply with the requirements of this Policy will be subject to disciplinary sanctions and may also be subject to civil and/or criminal liability if your conduct violates laws or regulations.

8. Validity

This document shall come into force upon its publication and shall be reviewed annually or whenever necessary due to changes in the processing of personal data.

9. Confidentiality

Although this document is the exclusive property of META, it must be read by employees, service providers, consultants, temporary staff, partners, shareholders, and suppliers, and may not be used for personal gain or for the benefit of third parties. Its reproduction, in whole or in part, must be controlled.

History		
Date	Revision	Modification
03	01	Policy issued and approved by the Committee and DPO.

Meta Digital. Simple. Human.

Questions?

Contact: compliance@meta.com.br