INTERNAL DATA PROTECTION GOVERNANCE POLICY - COGNITTIV DO BRASIL

Version 1.0/2022

CONTROL SHEET

Title	Internal Data Protection Governance Policy - COGNITTIV
Version number	V01/2022
Status	Drawing up the document
Approving Sector	Board of Directors
Date of Approval	11/01/2024
Area responsible for preparation	Compliance Department
Area of application	Brazil
Advertising Classification	Internal public

1. GENERAL PROVISIONS

This INTERNAL DATA PROTECTION GOVERNANCE POLICY - COGNITTIV ("Policy") has been drawn up in compliance with Law No. 13,709/2018 - General Personal Data Protection Law ("LGPD").

In this regard, **COGNITTIV** makes every effort to process the personal data of its employees, clients, suppliers, partners and third parties with the highest level of security, caution, confidentiality and compliance with the LGPD and other applicable legislation.

As an integral part of **COGNITTIV**, our employees must always, in carrying out their activities, ensure that the personal data to which they have access is processed in accordance with the LGPD, other applicable legislation and this Policy.

Therefore, if you have any questions regarding your rights and duties in relation to the processing of personal data, or about this Policy, please contact **COGNITTIV**'s Privacy Officer, by e-mail at lgpd@cognittiv.com

2. DEFINITIONS

In order to assist in the interpretation and application of this Policy, the words below, whether in the singular or plural, should be understood as follows, for the purposes of understanding the terms used throughout this document:

Term	Meaning in this Policy
Politics	Internal Data Protection Governance Policy
LGPD	Law No. 13.709/18 "General Data Protection Law"
Personal data	Any information relating to an identified or identifiable natural person ("Data Subject"). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier (location data, for example). Art. 5, I, of Law No. 13.709/2018.
Sensitive Personal Data	Any personal data concerning racial or ethnic origin, religious conviction, political opinion, union membership or membership of a religious, philosophical or political organization, as well as data concerning health or sex life, genetic or biometric data, when linked to a natural person. Art. 5, II, of Law No. 13.709/2018.

Anonymization	Process by which data loses the possibility of being associated, either directly or indirectly, with a data subject, considering the reasonable and available technical means at the time of processing. Art. 5, XI, of Law No. 13.709/2018.
Privacy Officer	The person responsible for protecting personal data at **COGNITTIV** and communicating with the ANPD and data subjects.
Data Subject	A natural person to whom the personal data refers. Art. 5, V, of Law No. 13.709/2018.
Processing	Any operation performed with personal data, such as collection, production, reception, classification, use, access, reproduction, transmission, distribution, processing, filing, storage, elimination, evaluation or control of information, modification, communication, transfer, dissemination, or extraction. Art. 5, X, of Law No. 13.709/2018.
Controller	A natural or legal person responsible for decisions regarding the processing of personal data. Art. 5, VI, of Law No. 13.709/2018.
Processor	A natural or legal person who processes personal data on behalf of the controller. Art. 5, VII, of Law No. 13.709/2018.
ANPD	National Data Protection Authority (Autoridade Nacional de Proteção de Dados).

3. POLICY OBJECTIVE

COGNITTIV, in the course of its business activities, processes personal data of individuals related to its internal structure as well as third parties directly or indirectly connected to its business.

This Policy aims to serve as a foundational pillar for all internal practices and processes at **COGNITTIV** concerning personal data processing. It demonstrates the company's commitment to protecting the rights of employees, clients, suppliers, partners, and third parties; implementing procedures and rules to ensure compliance with regulations; maintaining transparency in personal data processing; and mitigating the risks of information security incidents, based on the following principles:

- **Purpose:** Personal data shall only be processed for specific purposes, with a legitimate, explicit, defined, and informed purpose for the data subject. Subsequent processing incompatible with the initially identified purposes is prohibited.

- **Adequacy:** The processing of personal data must ensure compatibility with the purposes informed to the data subject, in accordance with the context of the processing.

- **Necessity:** The processing of personal data is limited to the minimum required to achieve its purposes, covering data that is pertinent, proportional, and not excessive in relation to the intended purposes.

- **Free Access:** Data subjects shall have facilitated and free access to consult the form and duration of processing, as well as the entirety of their personal data.

- **Data Quality:** Personal data processed must be clear, accurate, relevant, and updated according to its necessity and the purposes of the processing. Outdated or irrelevant personal data should not be processed for the indicated.

- **Transparency: COGNITTIV** shall provide data subjects with clear, precise, and easily accessible information about the processing activities and respective data agents, especially the form and duration of the processing, while respecting trade and industrial secrets.

- **Security: COGNITTIV** will implement security measures—technical, administrative, and legal—capable of protecting personal data from unauthorized access and from accidental or unlawful situations of destruction, loss, alteration, communication, or dissemination.

- **Prevention: COGNITTIV** will adopt measures to prevent harm caused by personal data processing.

- **Non-Discrimination: COGNITTIV** shall never process data for discriminatory, unlawful, or abusive purposes.

- **Accountability: COGNITTIV** will adopt effective measures capable of demonstrating compliance with personal data protection standards and the effectiveness of these measures.

Additionally, **COGNITTIV** believes that ensuring the legitimate, correct, and transparent processing of personal data is essential for the success of its activities and business, as well as for safeguarding its image and credibility before stakeholders, employees, clients, suppliers, partners, third parties, the general public, society, and the ANPD. In the event of a conflict between this Policy and applicable data protection legislation, the latter shall prevail.

4. SCOPE OF THE POLICY

This Policy applies to all employees who, in the course of their activities, may come into contact with personal data processed by **COGNITTIV** or on its behalf.

Additional policies may be created in specific cases, particularly when required by law or regulation.

5. HYPOTHESES FOR PROCESSING PERSONAL DATA

5.1. COMMON PERSONAL DATA

In the case of processing non-sensitive personal data, **COGNITTIV** will only carry out processing in accordance with the legal bases authorized by the LGPD. Among the legal bases provided by the legislation and directly applicable to **COGNITTIV** are the following:

- When necessary to comply with a legal or regulatory obligation of the controller (Art. 7, II, Law No. 13,709/2018);

- When necessary for the execution of a contract or preliminary procedures related to a contract to which the data subject is a party (Art. 7, V, Law No. 13,709/2018).

- When necessary for the regular exercise of rights in judicial, administrative, or arbitration proceedings (Art. 7, VI, Law No. 13,709/2018).

- When necessary to meet the legitimate interests of **COGNITTIV** or third parties, except where fundamental rights and freedoms of the data subject prevail (Art. 7, IX, Law No. 13,709/2018); and

- For credit protection (Art. 7, X, Law No. 13,709/2018).

In exceptional circumstances, **COGNITTIV** will collect the data subject's consent, which must be granted freely, spontaneously, unequivocally, prominently, and for specific purposes. This legal basis will only be used as a last resort, in cases where no other legal basis applies to justify the processing of personal data. (Art. 5, XII and Art. 7, I, Law No. 13,709/2018).

5.2. SENSITIVE PERSONAL DATA

COGNITTIV may also process sensitive personal data based on the hypotheses outlined in Art. 11 of the LGPD, provided that the potential risks are assessed with the Privacy Officer or Privacy Task Force, according to the criticality of the data involved.

6. PRIVACY AND PERSONAL DATA PROCESSING PROGRAM

For the privacy and personal data processing program at **COGNITTIV** to be effective and yield positive results, it is essential for employees to follow the procedures below, ensuring they are consistently observed during the processing of personal data.

6.1. GOVERNANCE

COGNITTIV, through its Data Privacy Governance structure, has adopted the hybrid operational framework outlined in the following items to ensure that personal data

processing is carried out in compliance with this Policy and all legal obligations. All actions related to privacy must be well-defined, documented, and recorded.

The Data Privacy Governance aims to organize and implement policies, procedures, company culture, roles, and responsibilities of each processing agent to address the current and future needs regarding Data Protection issues.

6.2. PROGRAM PRIVACY OFFICERS

The management and implementation of the privacy and personal data protection program must be conducted, managed, and controlled by the **Working Group** and the **Privacy Officer** to facilitate the monitoring of content, publication dates, deadlines for review, and other measures and procedures involving this, Policy.

6.3. WORKING GROUP

The **Working Group**'s primary objectives, but not limited to, are to manage and ensure the implementation of the privacy and personal data protection program. It must meet (monthly/quarterly) or whenever necessary to present and monitor **COGNITTIV**'s privacy and personal data protection program. The group will operate through a hybrid model, comprising members from key areas of the company capable of deliberating and making decisions on matters related to privacy and data protection, as follows:

- Privacy Officer.
- Leaders from each major team.
- Information Technology Department.

Additionally, the External Legal Counsel specializing in data protection compliance, NDM Advogados, may be invited to deliberate on specific matters.

O **The Working Group** can autonomously deliberate and make decisions regarding processing activities classified as low and medium risk. For activities classified as high or very high risk, decisions must be escalated to **COGNITTIV'**s responsible director, Mr. Rafael Farias.

6.4. TRAINING

All **COGNITTIV** employees involved in personal data processing activities must receive periodic training, as determined by the **Working Group**, specifically on:

- General concepts of Privacy and Data Protection, including an introduction to this Policy and study materials on the principles of the LGPD.
- Specific concepts of Privacy and Data Protection applied to the activities of each department.

- Updates involving the ANPD and the LGPD.
- How to use security controls in IT systems related to daily work.
- How to avoid falling victim to common security incidents, such as:
- Virus contamination or phishing attacks, which can occur, for example, by clicking on links in pop-up promotional offers or unknown email links.
- Keeping physical documents containing personal data in drawers rather than on desks.
- Not sharing login credentials.

In addition, a (semi-annual/annual) training session or additional training as necessary must be conducted for other employees not directly involved in personal data processing activities. These sessions will be decided by the **Privacy Working Group** and organized by the Privacy Officer, specifically covering the same topics outlined above.

6.5. Record of Processing Activities

COGNITTIV must maintain a Record of Processing Activities (ROPA) and update it quarterly or whenever changes are identified in the flow of processing activities.

7. TRANSPARENCY

All activities conducted by **COGNITTIV** involving the processing of personal data of external subjects (third parties, partners, clients, etc.) must adhere to the Privacy Policies available at www.cognittiv.com and this Policy. All operations involving the processing of personal data of internal subjects (employees) must comply with this Policy, the contract between the parties, and the internal data protection communication.

8. SECURITY

To ensure the security of personal data processed in the course of its activities and to prevent unauthorized or unlawful access, loss, destruction, or any other actions compromising the integrity, availability, or confidentiality of this information, **COGNITTIV** implements all measures suggested by the National Data Protection Authority (ANPD) in its Guidance Guide for Small-Scale Data Processors. This includes a variety of security technologies and procedures to help protect personal data.

The **Working Group**, the Privacy Officer, and the Information Technology Department at **COGNITTIV** must work together to ensure that all processed personal data remains secure, mitigating risks associated with information security incidents.

9. COLLECTION, USE, STORAGE, AND DELETION OF DATA

All personal data processing activities carried out by **COGNITTIV** must adhere to all principles outlined in this Policy and be associated with a specific legal basis

9.1 COLLECTION OF PERSONAL DATA

The personal data collection process must be restricted to what is essential for fulfilling the primary purpose established and communicated to the data subject, always considering the need to keep collected data up to date.

Direct Collection: Occurs when the data subject provides their data, for example, for contract execution with the company. In this case, data subjects must be informed, prior to collection, of all details regarding the data processing activity.

Indirect Collection: Occurs when the data subject does not consciously provide their data, such as through cookies.

Collection by Third Parties: Occurs when the data subject provides data to a specific company, and due to the nature of the activity, it becomes necessary to share the data with a third party unrelated to the company's business. In such cases, data subjects must be informed beforehand, for example, through Privacy Policies, Terms of Use, or Contracts containing privacy and personal data protection clauses, as directed by the legal department and the Privacy Officer, who must ensure the reliability of all third parties involved.

9.2 USE OF PERSONAL DATA

The use of personal data must be limited to the expectations the data subject had at the time of data collection (including if the data was collected indirectly or by third parties). In cases where the purpose initially communicated to the data subject needs to be altered, the data subject must be informed again, evaluating whether any adjustments are necessary.

9.3 STORAGE AND DELETION OF PERSONAL DATA

Personal data storage must be limited to the minimum time necessary to achieve the intended purpose and comply with any legal obligations governing a specific processing activity, following the Data Retention Policy. Once the purpose is fulfilled, and the necessary legal retention periods are observed, the data must be deleted using appropriate means.

10. PROCESSING OF SENSITIVE PERSONAL DATA

The data protection legislation classifies certain types of personal data as sensitive due to their potential to cause discrimination against the data subject. The LGPD identifies the following as sensitive personal data: racial or ethnic origin, religious beliefs, political opinions, union membership, or affiliations with organizations of a religious, philosophical, or political nature, as well as data concerning health, sexual life, genetics, or biometrics when linked to an individual.

For the processing of sensitive personal data to be considered lawful and legitimate, it must be based on one of the legal grounds provided by the LGPD and must be given the highest priority in security measures, as per the applicable legislation.

11. PROCESSING OF CHILDREN'S AND ADOLESCENTS' PERSONAL DATA

The processing of personal data from "children" and "adolescents" must be treated as exceptional. It should only occur after obtaining specific and highlighted consent from at least one parent or legal guardian, making public the information regarding the type of data collected, its use, and guarantees of other rights of the data subjects as provided by law.

12. DATA PROTECTION IMPACT ASSESSMENT

Article 5, XVII, of the LGPD defines the Data Protection Impact Assessment ("DPIA") as "a document prepared by the data controller, describing the data processing activities that may pose risks to civil liberties and fundamental rights, as well as the measures, safeguards, and mechanisms to mitigate such risks."

In other words, when a data processing activity is identified as potentially risking civil liberties and fundamental rights, a DPIA must be prepared to mitigate these risks.

Although mandated by law, the ANPD has yet to provide regulations and guidelines on DPIAs, leading to their occasional misuse. The regulatory process for DPIAs, as outlined in the ANPD's agenda, remains in its initial phase. Until ANPD issues appropriate regulations, DPIAs are not mandatory documents, except in cases explicitly outlined by the LGPD.

According to the ANPD's regulatory agenda, the RIPD (Data Protection Impact Report) is in the first phase of the regulatory process, expected to conclude in the second half of 2022.

Thus, until the ANPD provides proper regulation, the RIPD is not yet a mandatory document, as indicated in the LGPD. However, it may become mandatory in the future, depending on regulations and determinations by the ANPD, which could list activities requiring this document.

Nevertheless, as stated in Article 10, §3 of the LGPD, the "national authority may request the data controller to provide a data protection impact report when processing is based on legitimate interest, respecting commercial and industrial secrecy." In such cases, the preparation of the RIPD becomes mandatory.

For this reason, it is crucial to assess the specific case through personal data mapping to determine whether an RIPD is necessary for high-risk processing or to continue monitoring within the Data Processing Records (ROPA).

13. DATA SUBJECT RIGHTS

In all personal data processing activities, **COGNITTIV** must strive to ensure the following rights of data subjects. In all cases, the identity of the requesting subjects must be verified, and responses should occur under the guidance of the Privacy Officer.

For receiving requests regarding data subject rights, **COGNITTIV** provides a **communication channel** through the email address: lgpd@cognittiv.com, Rights can be exercised by employees, clients, suppliers, partners, and third parties whose personal data is under **COGNITTIV**'s processing scope. Requests must always be validated by the Privacy Officer and external legal counsel.

- **Right of Access:** You have the right to access any personal data we hold about you (subject to certain restrictions). In exceptional circumstances, we may charge a reasonable fee to provide such access, but only when permitted by law (e.g., when your request is manifestly unfounded or excessive).

- **Right to Rectification:** You have the right to request the correction of any incorrect information. You may also ask us to complete information you believe is incomplete.

- **Right to Erasure:** In some cases, you have the right to have your personal data erased or deleted. Note that this is not an absolute right, as we may have legal or legitimate grounds to retain your data.

- **Right to Restrict Processing:** You can request that we restrict the processing of your data under certain circumstances.

- **Right to Object to Processing:** You have the right to object to processing if it is based on legitimate interests pursued by us or for purposes other than those for which the data was collected.

- **Right to Data Portability:** This applies only to the information you have provided. You have the right to request the transfer of your information to another organization or to yourself. This right only applies if we process the information based on your consent or a contract and the processing is automated.

- **Right to Withdraw Consent at Any Time:** You may withdraw your consent for processing personal data when it is based on consent. Withdrawing consent does not affect the legality of processing conducted prior to withdrawal.

14. COMMUNICATION CHANNEL

As mentioned previously, **COGNITTIV** provides a **communication channel** via email: lgpd@cognittiv.com, available for submitting rights requests as outlined in Articles 17–22 of Law 13,709/2018 – the General Data Protection Law (LGPD).

The Privacy Officer is responsible for handling complaints and communications, providing clarifications, or taking actions in the interest of data subjects. They will also receive communications from the ANPD and perform other duties established by law or by the ANPD.

14.1. RESPONSE PROTOCOL

Data subjects (employees, third parties, partners, clients, etc.) must submit their rights requests via email to the above address.

Upon receiving a request, the Privacy Officer will review it with external legal counsel. Simple responses will be provided within 24 (twenty-four) business hours. For cases requiring more extensive effort and a detailed format, responses will be given within 15 (fifteen) days from the request date.

Responses will be provided free of charge, electronically, and with confirmation that the requester is the data subject or their legally constituted representative. **COGNITTIV** may require additional documentation to verify the requester's identity or representation to ensure privacy.

15. INTERNATIONAL TRANSFER OF PERSONAL DATA

The LGPD does not prohibit international data transfers and allows them under the following conditions:

> Article 33. International personal data transfers are only permitted in the following cases:
> I - to countries or international organizations with adequate personal data protection as per this law.
> II - when the controller offers guarantees of compliance with LGPD principles, data subject rights, and protection standards through:
> a) specific contractual clauses.
> b) standard contractual clauses.
> c) global corporate rules.
> d) regularly issued seals, certificates, and codes of conduct.
> III - when the transfer is necessary for international legal cooperation between public agencies for intelligence, investigation, or prosecution.
> IV - to protect the life or physical safety of the data subject or third party.
> V - when authorized by the ANPD.
> VI - based on international cooperation agreements.
> VII - to fulfill public policy or legal service requirements, ensuring transparency as per Article 23, Item I.
> VIII - With the data subject's explicit, distinct consent for the transfer, including prior information about its international nature; or
> IX - For other circumstances outlined in Article 7, Items II, V, and VI.

The ANPD will assess the adequacy of the foreign country's data protection level. However, no rules currently exist on this matter. The ANPD may, in the future, define the content of standard contractual clauses, global corporate rules, seals, certificates, and codes of conduct for better guidance.

COGNITTIV must adopt technical and administrative measures to safeguard personal data from unauthorized access and accidental or unlawful destruction, loss, alteration, or disclosure and to ensure data integrity, availability, and confidentiality in compliance with ANPD regulations.

16. VALIDITY

This Policy was approved by the Board of Directors and takes effect on 11/01/2024. It will be reviewed annually or earlier if necessary to ensure the document remains current.