PRIVACY AND PERSONAL DATA PROTECTION POLICY

VERSION 2.0

TABLE OF CONTENTS

1. Definitions

CI&T: all references to "CI&T" include CI&T Inc as well as all CI&T Group companies.

PERSONAL DATA: any information relating to an identified or identifiable natural person, including, but not limited to:

- data from CI&T personnel and third parties;
- Personally Identifiable Information (PII): name, address, phone, email, photo, date of birth, gender, age or other information that identifies or can identify a person;
- Personal Financial Information (PFI): financial details, income tax return, income and general banking information;
- Sensitive/Special Categories of Personal Data: data revealing racial or ethnic origin, religious beliefs, political opinion, union affiliation, or affiliations with religious, philosophical or political organizations. This also includes data related to health (PHI - Personal Health Information), sex life, genetic information or biometric data.

DATA PROTECTION OFFICER (DPO): person appointed to serve as the primary point of contact between CI&T, data subjects, and relevant data protection authorities.

INCIDENTS OR SECURITY INCIDENTS: any adverse event, confirmed or suspected, that may compromise the confidentiality, integrity, or availability of Personal Data under the responsibility of CI&T.

CI&T PERSONNEL: includes all direct and indirect collaborators, including, but not limited to, employees, officers and directors. This definition also includes third parties engaged by CI&T, including independent contractors, consultants and freelancers.

DATA PRIVACY SQUAD: multidisciplinary team within CI&T, consisting of members from Compliance, Information Security, Legal, Information Technology, Internal Controls, Personnel Department and Human Resources.

THIRD PARTIES: includes all service providers, outsourced workers, clients, partners, and suppliers associated with CI&T. It is important to note that companies in the health, financial, and insurance sectors are subject to stricter data privacy regulations, as they handle sensitive information such as medical records, financial data, and insurance policies. Therefore, any third parties operating within these industries must ensure compliance with applicable laws and adopt robust security measures to protect personal data.

DATA SUBJECTS: the natural person to whom the personal data pertains.

PROCESSING OF PERSONAL DATA: all activities performed with personal data, including, but

not limited to the collection, reception, classification, use, access, reproduction, transmission, distribution, processing, archiving, storage, elimination, evaluation or control of information, modification, updating, communication, transfer, sharing and extraction of personal data.

2. Objective

This policy sets forth essential guidelines to ensure that all CI&T personnel and third parties involved in processing personal data are aware of and adhere to this policy and also to CI&T's Information Security Policy. Furthermore, they must comply with applicable local privacy and data protection laws that may affect CI&T's business.

This policy encompasses various laws, such as the LGPD (General Data Protection Law), GDPR (General Data Protection Regulation), CCPA (California Consumer Privacy Act), the New York Privacy Act, Australian Privacy Laws, the Personal Information Protection and Electronic Documents Act (PIPEDA), the Act on the Protection of Personal Information (APPI), PIPL (China Personal Information Protection Law), and Colombia's Personal Data Protection Law (Law 1581 of 2012 and its regulatory decrees), among other applicable laws.

3. Applicability

This policy applies to all CI&T personnel and third parties who process personal data. CI&T leadership, in particular, must remain vigilant to situations that may result in actions contrary to the directives outlined in this policy.

4. Directives

All personal data must be treated as confidential and handled in accordance not only with the guidelines outlined in this policy, but also with each local legislation. CI&T is committed to ensuring that personal data is processed with respect for the following rights of CI&T personnel and third parties:

- The right to know what personal data is being collected;
- The right to update and rectify personal data;
- The right to request a copy of the authorization granted to CI&T;
- The right to be informed about how their data is being processed by CI&T;
- The right to revoke consent and/or request the deletion of personal data;
- The right to access their processed personal data free of charge;
- The right to provide prior authorization for the processing of minors' personal data.

Personal data may be processed for various purposes, always ensuring a legitimate purpose and an adequate legal basis, including but not limited to the following:

- To execute employment contracts for payroll management, track employee working hours, plan and coordinate staff training, oversee personnel and temporary work, ensure compliance with regulations on social benefits and occupational risk prevention, manage and promote employment and lead personnel recruitment and selection;
- To facilitate communication between CI&T and data subjects, by any means, including phone calls, text messages, emails, and physical mail, for any purpose related to the objectives outlined in this policy;
- To assess and improve service delivery through opinion surveys, commercial prospecting, marketing initiatives, proprietary advertising;
- To enhance CI&T's website functionality;
- To audit, study, and analyze the information from the databases not only to design commercial strategies and increase and/or improve the products and/or services offered by CI&T but also to disseminate policies, projects, programs, results, and organizational changes;
- To audit, study, analyze, and use the information from the databases to design, implement, and develop programs, projects, and events;
- To carry out marketing activities for the services and products offered within the framework of direct marketing activities;
- To promote solutions, webinars, seminars, trade fairs, and other current and upcoming events, as well as special promotions and offers;
- To manage, personalize and improve CI&T's websites and the accounts of registered users, analyze trends, according to the preferences selected by the user and personalize and enhance their online experience;
- To display targeted digital ads on third-party websites, the Company uses advertising networks.;
- To incorporate the data into national or international web servers;
- To share personal data with legitimate national or foreign third parties;
- To comply with third parties contracts obligations;
- To share the data with third parties in cases where CI&T participates in processes of merger, integration, split, acquisition, and/or liquidation.

If personal data is collected through social media, it will be processed in accordance with this policy and may be transferred to third countries where CI&T operates, which may have different levels of data protection than those required in the individual's country. In such cases, CI&T will comply with the applicable local regulations on personal data protection.

Particularly in Colombia, users who access CI&T's Colombian website (https://www.ciandt.com/co/es-co) and provide their personal data may receive updates or

promotional information. CI&T is committed to guaranteeing third parties' rights to file complaints with the Superintendence of Industry and Commerce for violations of the law, in accordance with local data protection regulations.

4.1. Anonymization and Pseudo Anonymization of Personal Data

Anonymization is the process by which information loses the ability to be associated, directly or indirectly, with an individual, and thus should not be considered personal data. CI&T Personnel must prioritize the use of anonymized data, whenever possible.

Anonymization must be conducted by:

- Replacing real personal information with completely random data, ensuring that the resulting set does not carry any identification of individuals and cannot be reversed;
- Eliminating portions of the data so that the remaining subset makes it impossible to identify any individual;
- Using only consolidated data that cannot be reversed to identify any individual.

Pseudo anonymization is the process by which personal data temporarily ceases to identify an individual.

Pseudo anonymization should be conducted by:

- Encrypting certain fields of personal data and ensuring that project personnel do not have access to the keys required to decrypt this data;
- Using tokens in place of certain fields.

4.2. Basic Principles

All processing of personal data must adhere to the following fundamental principles:

- **Transparency**: ensure the individual is fully informed about the processing of his personal data. This includes providing clear information on how their data is used, who it is shared with, the duration of its retention, and other relevant details in compliance with the legislation of each country;
- **Free Access**: guarantee the individual's right to access their personal data, in an easy and cost-free manner allowing them to view all their data processed by CI&T, and to request its deletion or correction;
- **Purpose:** process personal data solely for lawful, specified and clearly communicated purposes;

- **Necessity**: limit data processing to what is strictly necessary for achieving its intended purpose. Ensure that only relevant, proportional and non-excessive data is collected and used;
- **Adequacy**: treat personal data in a manner consistent with the purpose disclosed to the individual;
- **Quality**: maintain the accuracy and currency of personal data to ensure its reliability and relevance;
- **Security**: implement technical and administrative measures to protect personal data from unauthorized access. All CI&T Personnel must comply with CI&T's information security policies and follow best practices recommended by IT and Information Security teams;
- **Prevention**: take all reasonable steps to prevent incidents involving personal data and any actions that could be considered violations of data protection laws;
- **Non-discrimination**: ensure that data processing is not conducted for discriminatory, illegal or abusive purposes;
- **Accountability**: maintain records of all measures and practices implemented to ensure compliance with data protection laws.
- **Confidentiality:** ensure the confidentiality of information in accordance with applicable laws;
- **International Data Transfer:** the transfer of personal data outside its country of collection must be carried out with appropriate data protection safeguards.

4.3. Protection of Personal Data

All CI&T Personnel must ensure that:

- personal data is processed only for legitimate purposes;
- personal data must be stored only for the period required by applicable laws or as long as a legitimate purpose persists. This period should be communicated to the individual at the time of data collection. Upon expiration of the retention period, personal data must be securely destroyed. For the secure destruction of physical documents, CI&T Personnel must use shredding machines or designated boxes for confidential information disposal. For digital data, assistance from the IT team should be sought;
- Access to personal data should be limited to the minimum number of people necessary, based on the need-to-know principle. Only those individuals who require access to perform their functions or work should have access to the data;

- Audit trails are maintained for all access to personal data (documenting who accessed what, when and what actions were taken);
- Access passwords for systems containing personal data must never be shared;
- Any suspected or confirmed security incidents must be immediately reported to CI&T's Security team via the following communication channels: securitytalk@ - google chat (internal public) and security@ciandt.com (external public);
- Whenever possible, systems where personal data is processed should use at least two authentication factors for access;
- Passwords must be strong, periodically changed, and adhere to CI&T's password policies and procedures;
- Ensure the use of secure, encrypted virtual tunnels (e.g., TLS, HTTPS, IPSEC, SSH) for remote access to systems;
- The copying and/or distribution of data to third parties must only occur for legitimate purposes and with proper authorization. For customers, ensure authorization from the data controller; for suppliers, obtain authorization from CI&T and include it in the contractual agreements. All data processing must comply with relevant privacy and data protection laws and regulations;
- Customers' personal data must only be processed by CI&T based on legitimate purposes, with specific contract rules verified before starting processing operations;
- Provide clear and adequate information to data subjects about processing of their data, including the purpose, duration, data controller details, potential data sharing and the roles of the Treatment Agents (controller or processor). Data subjects have the right to revoke consent via an express request;
- Ensure that the transfer of files containing personal data is secure and compliant with legal requirements of each country. This includes implementing appropriate technical and organizational measures to ensure that data is protected during transfer and that only authorized personnel have access to that data. In addition, confirm that transfers are made only to countries or organizations that offer adequate data protection levels.

4.4. Data Governance

In CI&T projects involving the processing of personal data, the project manager or a designated representative is responsible for ensuring data privacy. Their key responsibilities include:

- Critically evaluating all personal data processing activities within the project

scope, ensuring compliance with legal principles, technical recommendations and this policy;

- Staying informed about data processing risks related to the project, providing insights, and supporting the designated representative or data privacy squad in mitigating such risks;
- Promoting best practices in personal data protection by raising awareness and providing guidance on key project elements;
- Supporting senior management, the designated representative, and the data privacy squad in discussions with CI&T third parties regarding privacy and data protection;
- Immediately reporting any policy violations, imminent threats, or incidents to the contacts specified in section 4.7.

4.5. Data Protection Impact Assessment (DPIA)

When CI&T acts as a data controller and identifies a high risk in data processing operations, it must conduct a DPIA (Data Protection Impact Assessment) before initiating processing or whenever significant changes occur in the requirements. The DPIA serves as a key privacy risk management tool, demonstrating that the controller has assessed the risks associated with personal data processing and implemented appropriate measures to mitigate them.

4.6. Data Privacy Training

All CI&T Personnel are required to complete an onboarding security training, which covers information protection, confidentiality and personal data processing, introducing essential practices and protocols for safeguarding information. Additionally, they must complete mandatory annual information security training to reinforce these critical security and data protection concepts.

4.7. Reporting Incidents or Potential Violations

CI&T personnel must promptly report any risks or suspected incidents, such as data breaches, unauthorized access, or collection without a legal basis, to the Information Security team. Incidents can be reported through the following communication channels: securitytalk@ (Google Chat - internal) and security@ciandt.com (external).

Questions and requests related to this policy or the guidelines mentioned herein should be

sent to the following contacts:

- LGPD: DPO GIGLIO SILVA SOCIEDADE INDIVIDUAL DE ADVOCACIA, (dataprivacy@ciandt.com);
- Other legislation: dataprivacy@ciandt.com.

5. Responsibilities

Failure to comply with this policy may result in disciplinary action, which can range from a verbal warning and written warning to termination of the employment contract or even dismissal for cause, in accordance with the relevant legislation. In certain cases, CI&T may have a legal or moral obligation to report the results of an investigation to the appropriate legal authorities, or may choose to do so.

6. Response Timeframes for Inquiries and Complaints

The time for CI&T to respond to your requests is as follows:

- For inquiries: within ten (10) business days from the date of receipt. If we are unable to address the inquiry within this timeframe, we will notify you, explaining the reason for the delay and providing a new date by which we will respond, not exceeding five (5) business days after the initial deadline;;
- For complaints: within fifteen (15) days from the day following the date of receipt. If we are unable to address your complaint within this period, we will inform you of the reasons for the delay and provide a new date for addressing your complaint, which will not exceed eight (8) business days after the initial deadline. You can exercise your rights by submitting your request to the email address dataprivacy@ciandt.com. Additionally, in Colombia, you may file a complaint with the Superintendence of Industry and Commerce (SIC) after completing the inquiry or complaint process with CI&T.

7. Document Control

This document is reviewed annually by the owner's department, with support from the Compliance team. The most recent review with changes was conducted on the dates listed in the table below.

Version	Date	Description	Author
1.0	DEC/2022	Creation	Álvaro Santana (Information Security Team)
2.0	FEB/2025	Review	Legal Team, Compliance Team and Information Security Team
2.0	APR/2025	Audit Committee Review	Audit Committee Members
2.0	MAY/2025	Final Approval/Effective Date	Board Of Directors