PRIVACY AND PERSONAL DATA PROTECTION POLICY

VERSION 1.0
May 2023

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:

- Personally Identifiable Information (PII) data: name, address, phone, email, photo, date of birth, gender, age or other information about an identified or identifiable person;
- PFI data (Personal Financial Information): financial information, income tax return, income and banking information in general;
- Sensitive Personal Data: any personal data concerning racial or ethnic origin, religious conviction, political opinion, union affiliation or organization of a religious, philosophical or political nature, as well as data referring to health (PHI Data - Personal Health Information) or sex life, genetic or biometric data.

Data Protection Officer (DPO): person appointed to act as a communication channel between CI&T, data subjects and the National Data Protection Authority (ANPD).

Security Incident Involving Personal Data ("Incident"): any adverse event, confirmed or suspected, related to the potential breach of confidentiality, integrity and availability of the Personal Data under the responsibility of CI&T.

CI&T person: direct or indirect collaborators, including, but not limited to, people under the CLT contracting regime, people who hold positions of officer and director. This definition also includes people who act as third parties hired by CI&T, such as consultants or freelancers.

Data Privacy Squad: is a multidisciplinary group of CI&T, formed by the areas of Compliance, Information Security, Legal, Information Technology, Internal Controls, Personnel Department and Human Resources.

Third parties: all service providers, outsourced workers, partners and suppliers.

Data subject: natural person to whom the personal data refer.

Treatment: all activity carried out 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 aims to establish the necessary guidelines to ensure that all CI&T Personnel, suppliers and any third parties (individuals or legal entities) who maintain a financial or commercial relationship with CI&T, who carry out any activity involving the processing of personal data (including data from CI&T's own People, from customers and suppliers), are aware of and adhere to the guidelines contained in CI&T's Information Security Policy, but also the local privacy and personal data protection regulations/laws that may impact CI&T's business.

3. Applicability

It applies to the entire set of personal data that is processed and/or controlled by CI&T, regardless of how it is collected. This Policy encompasses legislation such as LGPD (General Data Protection Law), GDPR (General Data Protection Regulation), CCPA (California Consumer Privacy Act), New York Privacy Act, PIPL (Personal Information Protection Law) among other applicable laws.

4. Directives

Compliance with the guidelines and standards established in this Policy must be respected by all people who, directly or indirectly, are related to CI&T. The leadership, in particular, must be aware of situations that may lead to the practice of acts contrary to the guidelines contained in this Policy.

All Personal Data must be considered confidential and must be treated/protected in accordance with the guidelines below.

4.1. Anonymization and Pseudo Anonymization of Personal Data

Anonymization consists of the process through which information loses the possibility of association, directly or indirectly, with an individual, and should therefore not be considered as Personal Data. CI&T people and projects must prioritize the use, whenever possible, of anonymized data.

Anonymization must be conducted:

- Exchanging information from real people for completely random data, so that the resulting set does not carry the identification of an individual and cannot be reversed;
- Eliminating part of the data in such a way that with the remaining subset

it is impossible to identify anyone;
- Using only consolidated data, without the possibility of reversal.

Pseudo anonymization consists of the process by which Personal Data temporarily ceases to be able to identify a Holder.

Pseudo anonymization should be conducted:

- Encrypting some fields of personal data and preventing project people from having access to the keys needed to decrypt such data;
- Using tokens in place of certain fields.

4.2. Basic Principles

All processing of Personal Data must observe the basic principles:

- **Transparency**: ensure the Holder is transparent about the Processing of his Personal Data, giving him the conditions to understand what is done with his Personal Data, with whom this information is shared, and for how long it will be kept, in addition to other aspects in accordance with with provisions of the legislation of each country;
- **Free Access**: the right to consult, in an easy and free way, the entirety of the Personal Data processed by CI&T must be ensured;
- **Purpose:** Personal Data must always be processed for lawful purposes, determined and informed to the Holder;
- **Necessity**: refers to limiting the treatment to the minimum necessary for the fulfillment of its purposes, with the scope of relevant, proportional and not excessive data in relation to the purposes of data processing;
- **Adequacy**: Personal Data must always be treated in a manner compatible with the purpose declared to the Holder;
- **Quality**: the accuracy of the Personal Data processed will be guaranteed, so that they are accurate and up-to-date;
- **Security**: technical and administrative measures capable of protecting unauthorized access to Personal Data must be adopted. Those responsible for projects and other people on the team must ensure compliance with CI&T's information security policy and the best practices recommended by the IT and Information Security areas;
- **Prevention**: all possible measures must be adopted to prevent the occurrence of Incidents involving Personal Data, as well as any act that may be considered as a breach of the data protection law of each country;
- **Non-discrimination**: data processing cannot be carried out for discriminatory, illegal or abusive purposes;
- **Accountability**: CI&T must keep records of measures implemented to

ensure compliance with data protection laws.

4.3. Protection of Personal Data

All CI&T Personnel must ensure that:

- Personal Data are only Processed for a legitimate purpose;
- The Personal Data must be stored only during the period foreseen in any laws that make reference to the storage of data or as long as the existence of a legitimate purpose persists, observing the period previously informed to the Holder at the time of collection of the Personal Data. Once the storage period has expired, Personal Data must be securely destroyed. For the secure destruction of printed data, CI&T Personnel must use shredding machines or identified boxes to dispose of confidential forms. For the disposal of media or information in digital format, CI&T People must seek help from the IT team;
- As few people as possible have this access to Personal Data, based on the need-to-know principle, which restricts access to certain data or information to those people who legitimately need this data or information to perform their function or work;
- Audit trails are maintained for all access to Personal Data (showing who accessed what, when and what they did);
- Access passwords are never shared for these systems with Personal Data;
- Any suspected or confirmed Incidents are immediately notified to CI&T's Security area. Communication channels: securitytalk@ - google chat (internal public) and security@ciandt.com (external public);
- Whenever possible, at least 2 authentication factors must be used to access the systems where Personal Data processing operations are carried out;
- Passwords used are strong enough and changed from time to time (as per CI&T Password Policy guidelines).
- In remote access, the use of secure (encrypted) virtual tunnels is ensured, using protocols such as TLS, HTTPS, IPSEC, SSH;
- The copying and/or distribution of data to third parties should only be carried out, in respect and with the aim of serving a legitimate purpose and with the authorization of the customer controlling this data or, in the case of suppliers, with authorization from CI&T and duly registered in clauses contracts between the parties. All processing of personal data must be done in accordance with the relevant privacy and data protection laws and regulations;
- Customers' Personal Data must only be processed by CI&T People based on legitimate purposes, being necessary to verify, before starting

the Processing operation, the specific rules of the contract;

- The data subject's access to information about the treatment must be made available in a clear and adequate manner, allowing the verification of the specific purpose, duration of the treatment, information about the controller as well as the possible shared use of data and responsibility of the Treatment Agents (controller or operator). The holder has the right to revoke consent by means of an express request;
- The transfer of files containing personal data must be carried out securely and in compliance with the 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 persons have access to that data. In addition, it must be ensured that the transfer of files only takes place to countries or organizations that offer an adequate level of data protection.

4.4. Data Governance

Within CI&T projects involving the Processing of Personal Data, the project manager or an individual appointed by him is responsible for the data privacy issue. This person's responsibilities are:

- Have a critical view of all Personal Data Processing within the scope of that contract, based on the principles of law, technical recommendations and this policy;
- Be aware of risk management related to Data Processing within the scope of that contract, providing inputs and supporting the actions of the Person in Charge or the Data Privacy Squad to mitigate such risks;
- Be a multiplier agent of good practices in the protection of personal data, raising awareness and/or guiding key elements of the scope of your project;
- Support the top management of the contract, the Person in Charge and the Data Privacy Squad in discussions related to privacy and protection of Personal Data with CI&T clients;
- Immediately report any violation or imminent violation of the rules contained in this policy, as well as any Incident to the contacts described in section 4.7.

4.5. Personal Data Protection Impact Report (RIPD)

CI&T, when acting as a controller and when a high risk is identified in data processing operations, must prepare a RIPD before starting the treatment or whenever there are significant changes in the requirements thereof. The RIPD fulfills the function of

demonstrating that the controller has assessed the risks in the operations of processing personal data and has adopted measures to mitigate them. In other words, it constitutes a privacy risk management tool.

4.6. Data Privacy Training

All CI&T Personnel undergo mandatory annual information security training. In this training, the topic of protection and confidentiality of information, including personal data, is addressed. In addition, CI&T People undergo safety training on their first day of work, in which good practices for protecting and protecting information are also presented.

4.7. Reporting Incidents or Potential Violations

CI&T People must notify any risks or suspected Incidents (leakage, unauthorized access, collection without any legal basis) to the Information Security team. To report Incidents, the following communication channels are available: securitytalk@ - google chat (internal public) and security@ciandt.com (external public).

Questions and requests related to this Policy or the guidelines mentioned herein should be sent to the following contacts:

- LGPD: DPO Marcelo Barbosa Lima (marcelobl@ciandt.com);
- Other legislation: dataprivacy@ciandt.com.

5. Responsibilities and Violations

Failure to comply with this Policy may result in disciplinary action, ranging from a verbal warning, through a written warning, to termination of the employment contract, or even dismissal for just cause, in accordance with the relevant legislation. In some 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.

The management and all collaborators of the CI&T Group are obliged to comply with and protect this Policy.

A violation of the guidelines of this Policy may result in disciplinary action, including, but not limited to, a warning, suspension, or termination of employment. In addition to CI&T Group sanctions, violations may result in referral to civil or criminal authorities where necessary or otherwise appropriate.

6. Document Control

Version	Date	Description	Author
1.0	DEC/2022	Policy creation	Álvaro Santana (Information Security Team)
1.0	MAY/2023	Compliance review	Rodrigo Sabino and Flávia Cabral
1.0	MAY/2023	Legal review	Mariana Queiroz
1.0	JUN/2023	Audit Committee Review	Members of the Audit Committee
1.0	JUL/2023	Policy Approval	Board Of Directors