Privacy and Personal Data Protection Program CI&T

VERSION 1.0 | September 2023

Table of Contents

Definitions

CI&T: all references to "CI&T," "company," or "firm" include CI&T Inc, Cayman, as well as all its subsidiaries.

PERSONAL DATA: Personal data is any information that enables the direct or indirect identification of a natural person.

DPO (Data Protection Officer): A person appointed by the controller and processor to act as the communication channel between the controller, Data Subjects, and the National Data Protection Authority (ANPD), when data processing is subject to LGPD. The DPO must assess the compliance of this Program, related documents, as well as all Company practices with LGPD through periodic evaluations.

THIRD PARTIES: Individuals or legal entities that are directly or indirectly related to CI&T, such as: service provider(s), supplier(s), partner(s), consultant(s).

DATA SUBJECT: The natural person to whom the Personal Data that is the subject of Processing refers.

PROCESSING: Any operation performed on Personal Data, such as collection, production, reception, classification, use, access, reproduction, transmission, distribution, processing, archiving, storage, disposal, assessment, or control of information, modification, communication, transfer, dissemination, or extraction.

Objective

This document aims to reinforce CI&T's commitment to compliance with all applicable legislation related to privacy and data protection. This underscores CI&T's diligence towards this information and its individuals, creating a transparent and secure environment.

Applicability

This applies to the entire set of personal data that is processed and/or controlled by CI&T, regardless of how it is collected.

This Program encompasses legislations such as LGPD (Lei Geral de Proteção de Dados), GDPR (General Data Protection Regulation), CCPA (California Consumer Privacy Act), New York Privacy Act, PIPL (Personal Information Protection Law), among other applicable legislations.

CI&T acts as both a controller and processor, and this program aims to demonstrate how the Company ensures compliance with applicable legislations, preventing, detecting, and correcting actions.

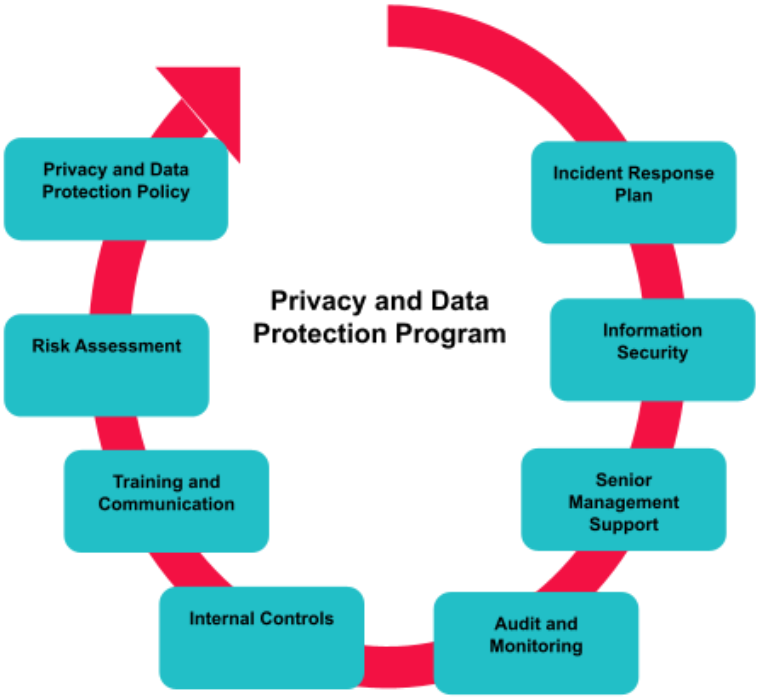
Duties and Responsibilities

Compliance with the rules and procedures established in this document must be ensured by all individuals who, directly or indirectly, are associated with CI&T.

In case of doubt, please send an email to **dataprivacy@ciandt.com.**

The Program at CI&T

CI&T's Privacy and Data Protection Program consists of the following pillars: Privacy and Data Protection Policy; Information Security; Risk Assessment; Training and Communication; Internal Controls; Audit and Monitoring; Senior Management Support; and Incident Response Plan.



Guidelines for the Pillars of the Privacy and Data Protection Program

Privacy and Data Protection Policy (available on the Investors Portal): This policy aims to establish the necessary guidelines to ensure that all individuals within CI&T and third parties, who engage in any personal data processing activity, comply with the applicable privacy laws regarding personal data. The policy is monitored by the Information Security team and is shared with business units and administrative areas, which should create procedures that best address their respective privacy and personal data protection risks.

Risk Assessment and Monitoring: The DPO responsible for LGPD must assess the compliance of this program with Brazilian legislation and monitor it. To support them in this mission, CI&T has a Data Privacy Squad that assists in the implementation of LGPD. This Squad also works on monitoring and implementing other applicable local legislations. The Squad is multidisciplinary, composed of Compliance, Information Security, and Legal departments.

Internal Controls: Internal controls aim to ensure that processes and actions adhere to the company's objectives and guidelines, thereby preventing deviations. They also seek to mitigate risks or potential failures during the

execution of activities, ensuring a healthy control environment. The Information Security team collaborates with business units and administrative areas in implementing internal controls for data privacy.

Training and Communication: CI&T conducts communications and provides training to ensure the dissemination of various topics within the company. This includes a mandatory annual Information Security training for all employees, which covers the topic of data privacy.

Due Diligence: The process of contracting and monitoring third parties aims to identify the best options for CI&T while assessing the associated risks. The Information Security team evaluates the risks related to data privacy in vendors selected by the Procurement team. Some vendors with a high risk in information security and data protection for CI&T undergo an annual assessment to enhance their level of maturity and commitment to CI&T's guidelines.

Audit: The responsibility of the audit function is to provide independent opinions to the Board of Directors, through the Audit Committee, regarding the risk management process, the effectiveness of internal controls, and corporate governance. The prioritization of audited topics is in accordance with the approval of the Annual Audit Plan.

Senior Management Support: This pillar represents CI&T's ethical identity, demonstrating the company's culture in practice, both for employees and for third parties who interact with its business. By practicing this pillar, the organization strengthens an environment committed to the values, principles, and attitudes of CI&T as outlined in the Code of Ethics and Conduct and its policies.

Information Security: Information Security aims to ensure the confidentiality, integrity, availability, and authenticity of information.

- Confidentiality – Ensuring that information is only accessed by authorized individuals, preventing it from being disclosed to an unauthorized user, entity, or process;
- Integrity – Ensuring that information is not altered or deleted without proper authorization;
- Availability – Ensuring that access to systems, data, and services is only performed by authorized users or entities;
- Authenticity – Ensuring the identity of the sender of the information.

Information Security Incident Response Plan: CI&T has an Information Security Incident Response Plan in place, which defines the structure and processes developed to detect and respond to information security incidents, determine

their scope, risks, and appropriate response, communicate the results and risks to all relevant stakeholders, and reduce the likelihood of recurrence.

Key Contacts

Questions or requests related to this Program or the mentioned documents should be sent to the following contacts:

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

Violation Notification

Any risks or suspicions of incidents (leakage, unauthorized access, collection without legal basis) should be reported to the Information Security team. The following communication channels are available: securitytalk@ - google chat (internal audience) and security@ciandt.com (external audience).

Sanctions and Consequences

In addition to the penalties imposed by current laws and regulations, any violation of such laws and regulations may result in irreparable damage to CI&T's reputation and consequently, the loss of business and continuity of commercial relationships.

The consequence of a violation will lead to disciplinary action, ranging from a warning to dismissal for just cause, potential removal from office, or termination of the service contract, in accordance with applicable laws and regulations, without prejudice to the filing of civil and criminal actions.

Applicable Documents

"Privacy and Data Protection Policy" and "Information Security Policy," available on CI&T's website - Investors Portal.