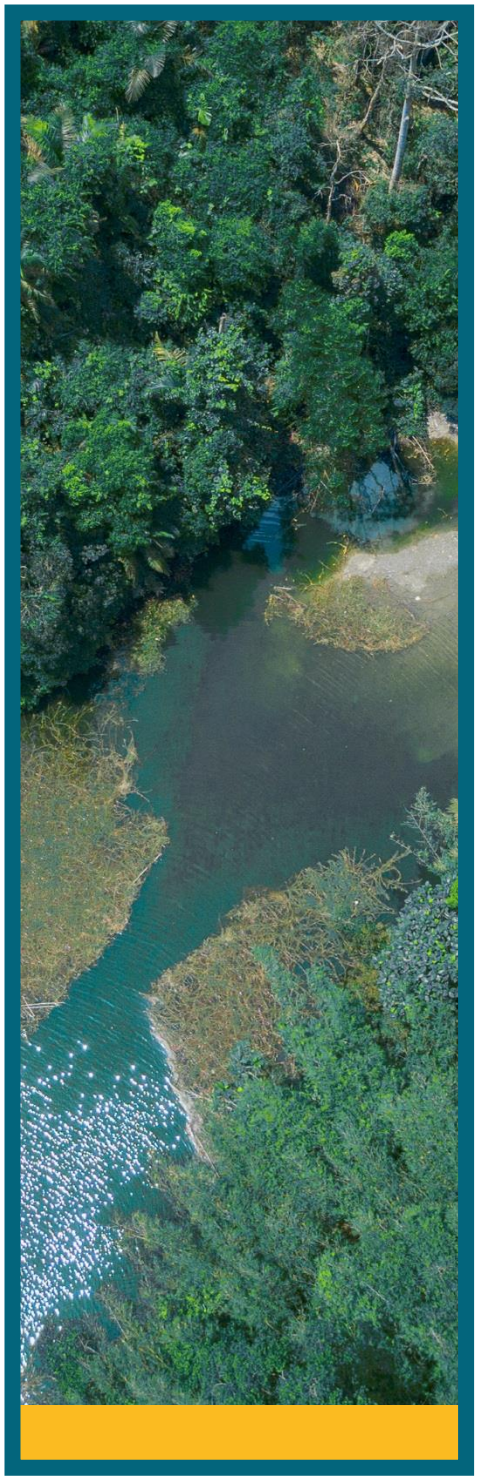

General Policy

Indra Privacy Policy

1. Introduction

Indra is aware of the importance of processing personal data properly, and the Company regards the protection of personal data as particularly important.

Data Protection management therefore forms an integral part of any activity involving the processing of personal data and is included as part of Indra's strategic planning.

2. Purpose

The purpose of the Indra Privacy Policy, which is supplemented by the Company's Personal Data Protection Manual, is to ensure effective and consistent personal data protection in all of Indra's activities.

3. Scope

This Policy is applicable to and binding on all Indra Group companies.

4. Principles

To achieve these aims, the following principles have been established:

- The personal data being processed must be sufficient, pertinent and not excessive, they must be collected for explicit, legitimate purposes, and they may not be processed in a way that is incompatible with these purposes. They must be kept up-to-date and retained for the minimum amount of time necessary.
- When it collects data, Indra will comply with the data subjects' right to be informed and at least provide them with information regarding:
    - Its name.
    - The purpose for which it intends to process the data.
    - The recipients to whom it is planning to forward any personal data.
- Indra only processes personal data in the following cases:
    - After obtaining the data subject's voluntary, explicit, unequivocal and informed consent, the company will provide a simple way of withdrawing that consent.
    - When the Company has a legitimate interest that justifies processing, provided that the interests, rights and freedoms of the data subject do not take precedence.
    - When processing the data is necessary in order to maintain or comply with a legal relationship between the Company and the data subject.
    - When processing or forwarding the data is required in order to comply with an obligation imposed by the national legislation in force, or when the data are processed by a Public Authority or Administration that requires this in the legitimate exercise of their powers, with maximum guarantees for the data subject's right to privacy.

- When exceptional situations arise that endanger the life, health or safety of the data subject or other people or groups.

- As a general rule, the processing of data that are sensitive or that may affect the data subject's most intimate affairs must be avoided, and if it cannot, then particular attention must be paid to the legal requirements that are to be applied and the security measures to be implemented.

- Generally speaking, sensitive data are understood to be data relating to health, sexuality, genetics, racial or ethnic origin, political opinions, religious conviction, union membership and biometric data used for the purposes of identifying a data subject.

- Indra applies security measures based on standards that are recognised as effective and that are aimed at ensuring the confidentiality, integrity and availability of the personal data in question. Indra's Information Security Policy provides the reference framework for these security measures and must be complied with.

- Any person who has access to personal data as a result of their professional duties at Indra is obliged to comply with the strictest duty of secrecy and with the obligations set out in the Code of Ethics that the Company has published to this end. These obligations will remain in place even after such people have ended their relationship with the Company.

5. Governance model

Indra has defined a Data Protection Governance Model that ensures coordination between its organisational units and its Management.

The governance of Data Protection is the responsibility of the Data Protection Officer (DPO), who has the duty to oversee compliance with Indra's data protection regulations. He/she is the person responsible for attending to the rights of data subjects and for working together with the regulatory authorities (e.g. the Spanish Data Protection Agency).

The DPO performs his/her duties under the supervision of the Information Security Department (ISD), which is the body charged with ensuring Information Security and which is responsible for managing Indra's Information Security Committee.

The Information Security Committee (ISC) is the body charged with managing Information Security at Indra. Its main purpose is to promote Information Security, with support and backing from the Company's Management, and to this end it defines strategic security targets and plans as required, along with business targets and processes.

The ISD, acting through the CISO and the DPO, prepares reports on a regular basis, and at least once a year, independently of the Auditing and Compliance Committee and the Risk Coordination Unit.

6. Channel for exercising rights and reporting incidents

Data subjects may exercise their rights of access, correction, deletion or encryption, and objection to processing by contacting the Data Protection Officer at dpo@indra.es.

7. Approval

By approving this policy, the Board of Directors expresses its determination and commitment to achieve a level of security appropriate to the needs of the business that guarantees data protection in a homogeneous manner in all Indra Group companies.