Transformamos el presente.
Fortalecemos el mañana.

Privacy Policy

Approved by the Board of Directors of CELSA STEEL on 30 October 2025

Table of Contents

1. Purpose and scope

Purpose:

The purpose of this policy is to establish the fundamental principles and obligations regarding privacy within CELSA. It seeks to ensure respect for the fundamental right to privacy of all members of the organisation, business partners and third parties. Furthermore, it sets out guidelines to ensure privacy and document compliance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR), including all the necessary requirements to demonstrate such compliance.

Scope:

This Policy applies to CELSA and all the companies comprising its Group, in accordance with their specific characteristics, as well as to the processing of personal data carried out by CELSA, including the information systems, media and equipment used for such processing of personal data, the persons involved in the processing and the premises where they are located.

The activities covered by this Policy are all those carried out by CELSA, or which it may undertake in the future, in the course of its business activities, which involve, relate to or may entail the processing of personal data, including, amongst others, that of members of the organisation, business partners and third parties.

The principles and guidelines set out in this document shall be applied in accordance with the specific legal and regulatory provisions on privacy in each jurisdiction where CELSA operates. In cases where local legislation establishes specific, additional or divergent requirements with respect to the general principles set out herein, specific annexes to this policy may be drawn up to ensure full compliance with the applicable regulations in each territory, whilst maintaining in all cases the minimum protection standards established in this document.

This policy was approved by the Board of Directors of CELSA STEEL, S.A. on 30 October 2025.

2. Definitions

To ensure the clear and consistent application of this policy, the following definitions are established:

Personal data: any information that allows a natural person to be identified directly or indirectly. By way of illustration, personal data shall be considered, for example, a name, an identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

Processing: any operation or set of operations performed on *personal data* or sets of *personal data*, whether by automated means or not, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

AEPD (Spanish Data Protection Agency): An independent authority responsible for ensuring compliance with personal data protection regulations in Spain and for protecting citizens' rights in this area. It is the Lead Supervisory Authority for the CELSA Group, to the exclusion of other authorities.

PIA (Privacy Impact Assessment): an analysis of the risks that a specific information system, product or service may pose to the personal data processed within an organisation.

Privacy Manual: a set of documents comprising this Privacy Policy and all the

procedures mentioned therein, which form CELSA's internal regulatory framework on privacy.

Security incidents: Among other things, any breach of the regulations set out in the General Data Protection Regulation (GDPR) and/or any regulations that replace or update it, as well as any anomaly or event that affects or may affect the security of personal data in its three aspects of confidentiality, integrity and availability.

Security breach: Any incident causing the destruction, loss, alteration or unauthorised access to personal data.

3. Development of the Privacy Policy

This document summarises the general guidelines for compliance with CELSA's Privacy Policy, which are set out in the collection of documents comprising the CELSA Privacy Manual. It includes the key steps for the proper management of personal data processing, risk prevention and incident response.

3.1 General Principles

CELSA establishes the following principles for the processing of personal data:

- **Lawfulness, fairness and transparency** – To process personal data lawfully, there must be a legitimate basis and the data subject must be informed
- **Purpose limitation** – Personal data shall only be used for specific and legitimate purposes and may not be used for other purposes without justification
- **Data minimisation** – Only data that is necessary and appropriate for the intended purpose will be processed
- **Accuracy** – Data must be accurate and up to date.
- **Storage limitation** – Personal data shall be retained only for as long as necessary and shall be deleted when no longer used, unless there is a legal obligation or it is retained for specific purposes.
- **Transparency and information** – Individuals will be informed in a clear and accessible manner about how their personal data will be processed.
- **Integrity and confidentiality** – Personal data shall be protected by appropriate security measures and shall always be treated confidentially

- **Active accountability** – The data controller shall comply with data protection principles and keep records of such compliance.
- **Lawful collection** – It is prohibited to obtain personal data from sources that are unlawful or do not guarantee its lawful origin.
- **International transfers** – Data transfers outside the European Economic Area shall strictly comply with applicable European regulations.
- **Data subjects' rights** – CELSA will ensure that individuals can exercise their rights regarding their data through appropriate procedures.

3.2 Risk analysis and security measures

CELSA implements technical and organisational measures to ensure the security of personal data, such as encryption, access control, incident recovery and regular reviews. These measures are based on an annual risk analysis that identifies threats, vulnerabilities and potential harm.

3.2.1 Privacy Impact Assessment (PIA)

CELSA will carry out a PIA, or *data protection impact assessment*, prior to any data processing that may pose a high risk to individuals' right, particularly where new technologies are used. This is required in cases such as:

- Automated profiling with legal effects.
- Mass processing of sensitive or specially protected data.
- Systematic surveillance in public spaces.

The official list of processing operations requiring a PIA is available on the AEPD website and can be consulted at https://www.aepd.es/prensa-y-comunicacion/notas-de-prensa/la-aepd-publica-el-listado-de-tratamientos-en-los-que-no-es.

Where a new personal data processing operation is identified or a substantial change to an existing processing operation is planned, the person responsible for the processing must notify the Privacy Team at gdpr@gcelsa.com in good time to allow for an assessment of whether a PIA is required. This notification must include a detailed description of the proposed processing, the categories of personal data involved, the purposes of the processing, the retention period for the personal data, the categories of data subjects affected, and any specific technology or methodology intended to be used. The Privacy Team will assess whether the proposed processing poses a high risk to the rights and freedoms of natural persons and, where appropriate, will

determine the need to carry out a DPIA in accordance with the criteria set out in Article 35 of the GDPR and the guidelines of the competent data protection authorities.

3.3 Notification, management and response to incidents

3.3.1 Incident register

The DPO must maintain an incident register to implement corrective measures, prevent future attacks and hold those responsible for compromising the security of data processing to account.

Any user who detects an incident must report it as set out in *PR-00144 Management and notification of security breaches.*

3.3.2 Notification of security breaches

CELSA must notify the AEPD within a maximum of 72 hours if a security breach affecting personal data occurs.

It must also inform those affected if there is a high risk to their rights, unless the data is protected, the risk has disappeared or the communication would be disproportionate.
All breaches must be documented, including details, consequences and corrective measures.

3.4 Rights of data subjects

Data subjects may exercise the following rights with CELSA: access, rectification, erasure (right to be forgotten), restriction of processing, data portability, objection, and the right not to be subject to automated decision-making.

Upon receiving a request to exercise rights, CELSA must respond within a maximum period of one month (extendable by two months in complex cases) in accordance with the procedure for handling requests to exercise rights.

The request is free of charge, unless it is manifestly unfounded or excessive, in which case a fee may be charged or the request may be rejected on justified grounds. Such requests may be made by sending an email to gdpr@gcelsa.com.

3.5 Privacy Governance System

CELSA has appointed its Cybersecurity and Privacy Committee as the Data

Protection Officer (DPO), responsible for advising, informing and acting as a liaison with the supervisory authorities.

The DPO can be contacted by email (GDPR@gcelsa.com) or by post at Castellbisbal:

Attn: Data Protection Officer. C/Ferralla 12, 08755 Castellbisbal, Barcelona, Spain.

Regular internal or external audits will be carried out to verify compliance with security measures and privacy regulations. Extraordinary audits will also be carried out if there are significant changes to the information systems.

4. Roles and responsibilities

Compliance with applicable privacy regulations is the responsibility of all members of the CELSA Group, who must act in accordance with the principles set out in this Policy.

In addition, the following responsibilities are defined:

Board of Directors:

- To review and approve this policy and associated procedures.
- To approve the governance of the Cybersecurity and Privacy Committee from a privacy perspective.

Management Committee:

- Ensure that the policy and its procedures are properly implemented throughout the organisation.
- Promote a culture of compliance and accountability regarding privacy at all levels of the organisation.

Data Protection Officer (DPO), collectively represented by the Cybersecurity and Privacy Committee:

- Advise and inform CELSA employees on the processing of personal data.
- Coordinate with all the group's business units.
- Act as the point of contact with supervisory authorities.

Privacy team, members of the legal and compliance teams designated to

provide support as a point of contact for all matters relating to the processing of personal data. Their main functions are:

- To provide technical and regulatory advice.
- Monitor compliance with the policy and other internal regulations on privacy.
- Identify, analyse and mitigate risks related to the processing of personal data.
- Coordinate the various business areas to ensure the correct implementation of the privacy policy and its alignment with the GDPR.
- To train and raise awareness among all members of the organisation, in collaboration with the network of Data Privacy Advisors.

Data Privacy Advisors: these are the individuals designated within the various business units to act as an operational link with the Privacy Team. Their main functions are:

- To advise their teams on the correct application of data protection regulations in day-to-day activities.
- To promote compliance with the policy and other internal regulations regarding privacy and information security.
- To identify and report potential risks or breaches relating to the processing of personal data.
- To assist in the management of security incidents affecting personal data.
- Channelling queries, concerns or requests to the Privacy Team.
- Participate in training and awareness-raising initiatives on privacy within your area

All Celsa Members:

- Be familiar with and apply data protection regulations.
- Report any security incident through the channels established by the organisation in document *PR-00144 Management and Reporting of Security Breaches*.
- Maintain due secrecy and confidentiality regarding personal data they become aware of in the course of their work.

Business Partners and Third Parties (including suppliers, subcontractors, data processors, business partners, customers, external consultants and any other entity that has access to personal data within the framework of

their contractual relationship with CELSA):

- Comply with the security and confidentiality measures set out in this document.

5. Approval, communication and updating

The DPO will review this policy once a year and update it as necessary to ensure its relevance and effectiveness. Updates to this policy must be approved by both the Cybersecurity and Privacy Committee and the Board of Directors, following validation by the Management Committee.

To ensure its proper implementation and compliance, this Policy is published on CELSA's corporate website (CELSA Policies), as well as through the Group's internal channels. In addition, appropriate measures will be taken to promote awareness of the Policy and ensure compliance by all relevant departments.

6. References and Related Documents

This policy is supplemented by a series of procedures and appendices that make up the Privacy Manual, which sets out in greater detail the operational and specific aspects of its implementation.

Specifically, the following procedures and appendices are included:

- Procedure for managing the exercise of rights
- Procedure for the retention, erasure and blocking of personal data
- Procedure for the management and notification of security breaches
- Procedure for the use and processing of personal data in paper format
- Procedure for conducting a Data Protection Impact Assessment
- Annex I. Staff roles and responsibilities
- Annex II. Record of processing activities
- Annex III. Risk analysis
- Annex IV. Security measures implemented

Furthermore, this policy is aligned with current privacy legislation, in particular:

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data

(GDPR).

- Organic Law 3/2018 of 5 December on the Protection of Personal Data and the Guarantee of Digital Rights (LOPDGDD).
- Any other applicable national or sector-specific regulations depending on the context and jurisdiction of the processing carried out.