



VERSION CONTROL			
VERSION	DATE	RESPONSIBLE PARTY	REMARKS
1.0	19/06/2025	Criminal Compliance	Definition and content of the Protocol
	24/06/2025	Board of Directors	Approval
	19/12/2025	Criminal Compliance	Amendment of the scope of application
	27/03/2026	Criminal Compliance	Amendment regarding Data Protection matters

The following is a translation of this policy provided for informational purposes only. In the event of any discrepancy or inconsistency, the Spanish version shall prevail and be considered the sole legally valid and binding text.

INDEX

I.- PURPOSE	3
II.- SCOPE OF APPLICATION	3
III.- DEFINITIONS	3
IV.- PRINCIPLES FOR THE RESPONSIBLE USE OF AI-BASED TOOLS	4
V.- AI TOOLS	5
VI.- PERMITTED AND PROHIBITED USES	5
a) Permitted Uses	5
b) Prohibited Uses	5
VII.- EVALUATION, SUPERVISION AND REVIEW OF AI SYSTEMS	6
VIII.- TRAINING AND AI LITERACY	6
IX.- CONSULTATION CHANNEL	6
X.- PERSONAL DATA PROTECTION	6
XI.-ENTRY INTO FORCE AND REVIEW	7
XII.- REPORTING BREACHES AND DISCIPLINARY MEASURES	7
XIII.- COMMUNICATION AND DISSEMINATION OF THE PROTOCOL.....	8
ANNEX I.-AI TOOLS AUTHORISED BY GRUPO FEDOLA	8
ANNEX II.- PROHIBITED AI PRACTICES	9

I.- PURPOSE

This Protocol establishes the guidelines for the responsible, lawful and ethical use of Artificial Intelligence (AI) systems within Grupo Fedola, in compliance with Regulation (EU) 2024/1689 of the European Parliament and of the Council, with the aim of ensuring that AI is used in an ethical, lawful, secure and transparent manner and in alignment with the Group's corporate values and objectives.

II.- SCOPE OF APPLICATION

This Protocol applies to all autonomous and legally independent companies (whether currently existing or established in the future) that form part of the Grupo Fedola business group.

For the purposes of this Protocol, Grupo Fedola or the Group shall mean all the independent companies comprising the Group, to which this Protocol applies:

GRUPO FEDOLA, S.L.; PREFABRICADOS TEIDE, S.L.; FERRETERÍA HERMANOS LÓPEZ ARVELO, S.L.U.; OFISABEL, S.L.U.; MASQUECARPAS, S.L.U.; FEDOLA, S.L.U.; BROKER FEDOLA CORREDURÍA DE SEGUROS, S.L.U.; PRICEMESA, S.L.U.; AGRO INNOVACIÓN FEDOLA, S.L.U.; GF-TIC, S.L.U.; CAMULSE, S.L.U.; EXPLOTACIONES SANTONEL, S.L.; FELAHOTEL, S.L.; COSTA ADEJE GRAN HOTEL, S.L.; ISABEL FAMILY HOTEL, S.L.U.; NOELIA PLAYA, S.L.U.

It therefore applies to all employees, directors, external collaborators and suppliers who use, develop or manage AI systems within the scope of their professional activities.

III.- DEFINITIONS

Artificial Intelligence (AI): A system based on algorithms that performs tasks normally requiring human intelligence, such as pattern recognition, prediction, text generation, decision automation and similar functions.

AI Tools: Applications or platforms incorporating AI technologies, such as virtual assistants, language models, recommendation systems and similar solutions.

Personal Data: Information that enables the direct or indirect identification of a natural person.

Processing of Personal Data: Any operation or set of operations performed on personal data, whether by manual or automated means, including the collection, recording, storage, use, transmission, dissemination or deletion of such information. This includes activities ranging from the use of website forms to video surveillance systems.

AI Literacy: The skills, knowledge and understanding that enable the informed deployment of AI systems and awareness of the opportunities, risks and potential harm associated with AI.

IV.- PRINCIPLES FOR THE RESPONSIBLE USE OF AI-BASED TOOLS

1. **Confidentiality:** Employees using AI tools authorised by the company must not enter confidential information into such systems, including financial data, personal data, contracts, restricted corporate documentation or sensitive information.
2. **Human Oversight:** Content generated by AI must always be reviewed, validated and, where necessary, corrected by a qualified professional.
3. **Basic Instructions (Prompts):** The use of prompts is recommended in order to achieve better results. Likewise, the use of AI for highly specialised matters is discouraged. AI should primarily be used for preliminary guidance and first-level consultations. For example, where a legal query is submitted, the prompt should specify that it relates to Spanish law, that the AI must not invent information, and that it should indicate sources which must subsequently be verified by a professional.
4. **Transparency:** All documents generated by AI must be clearly identified as such. This shall not be necessary where AI has merely been used for consultation or inspiration purposes and the final document has been prepared by a professional. Furthermore, any significant decisions made with AI assistance must be documented. To ensure transparency in the use of AI tools, employees must be informed whenever they are interacting with an AI system.
5. **Fairness:** Employees using AI tools authorised by company management must ensure that decisions and outcomes generated by such systems are non-discriminatory. The use of fully automated processes shall therefore be limited and always subject to human supervision.
6. **Sustainable Development:** Consideration must be given to the significant environmental impact that may be associated with the use of certain AI tools.
7. **Legality:** All uses of AI must comply with applicable legislation, particularly regulations relating to data protection, employment law, intellectual and industrial property rights, and AI regulation. Under no circumstances may AI tools be used for unlawful purposes or to facilitate the commission of criminal offences.
8. **Quality and Reliability:** AI systems used by the Group must be technically robust and have clearly defined limitations. Their reliability and origin must be verified before use.

V.- AI TOOLS

1. **Corporate AI Tools:** Management shall evaluate, identify and approve AI tools for professional use. Approved tools shall be communicated together with their usage protocols and the persons responsible for them. Their use shall be governed by the principles set out in this Protocol (human review and confidentiality), unless the tool has been specifically designed to operate differently. Corporate AI tools are those listed in ANNEX I – AI TOOLS AUTHORISED BY GRUPO FEDOLA.
2. **Public AI Tools:** The use of publicly available general-purpose AI tools is prohibited unless prior authorisation has been granted by company management and, in all cases, only in accordance with the provisions of this Protocol. Their use must be limited to general knowledge enquiries, publicly available information and the drafting of non-confidential texts. Following each use, generated chats must be deleted to prevent them from being stored within AI systems located outside the European Union. Should an employee use such tools despite management having refused authorisation, they shall assume full responsibility for any consequences arising from their use.

VI.- PERMITTED AND PROHIBITED USES

a) Permitted Uses

- Automation of administrative or repetitive tasks.
- Generation of preliminary content for internal use (texts, summaries and reports).
- Assistance with data analysis and trend forecasting.
- Improvement of customer experience through chatbots or recommendation systems.
- Translation of text from publicly available secondary sources.
- Research on non-sensitive subjects.
- Brainstorming on non-confidential matters.
- Generation of creative content, including text, video and images, under human supervision.

b) Prohibited Uses

The use of any AI system falling within the category of unacceptable risk is expressly prohibited, including:

- Any use involving the mention, processing or use of personal data without the explicit, freely given and informed consent of the data subject, in accordance with applicable data protection legislation.
- Subliminal manipulation or exploitation of vulnerabilities.
- Automated social scoring of natural persons.

- Emotion recognition in the workplace.
- Creation of facial recognition databases through the unauthorised collection of images.
- Use of AI to monitor employees without their consent.
- Generation or dissemination of false or manipulated content (deepfakes or fake news).
- Automated decision-making affecting individuals without human review.
- Use of AI without prior authorisation or assessment by the Technology Compliance Officer.

VII.- EVALUATION, SUPERVISION AND REVIEW OF AI SYSTEMS

The use of AI tools must be assessed before implementation through an ethical and legal impact assessment and approved by company management.

For this purpose, GF-TIC is designated as the organisation responsible for AI and shall be responsible for preliminary assessments, supervision of AI use and periodic reviews of AI systems.

GF-TIC shall also act as the sole administrator and manager of AI tools used by the Group and shall have the authority to restrict or block access in cases of non-compliance.

VIII.- TRAINING AND AI LITERACY

Grupo Fedola companies shall provide regular and mandatory training on:

- Ethical and legal principles relating to AI use.
- Risks and limitations of AI systems.
- Responsible use and supervision procedures.

Such training shall be delivered in accordance with the principles established in this Protocol.

IX.- CONSULTATION CHANNEL

Grupo Fedola provides an internal consultation channel for AI-related enquiries: soporte@gf-tic.com. All communications submitted through this channel must include the employee's direct line manager in copy.

X.- PERSONAL DATA PROTECTION

Grupo Fedola expressly prohibits the use of AI tools involving the processing of personal data, particularly sensitive or confidential personal data. This restriction is intended to safeguard information security, data confidentiality and strict compliance with applicable data protection legislation.

Any intention to use AI tools must be communicated in advance and must receive authorisation from both Management and the Data Protection Officer (DPO).

To obtain such authorisation, the employee must send an email to their direct line manager, who shall be responsible for obtaining the relevant approval.

Without prejudice to the foregoing, any AI system processing personal data must, at a minimum, meet the following requirements:

- Appropriate legal basis.
- Technical and organisational security measures.
- A Data Protection Impact Assessment (DPIA), where required.

XI.- ENTRY INTO FORCE AND REVIEW

This Protocol shall enter into force upon implementation, following consultation with the legal representatives of employees.

The Criminal Compliance function and GF-TIC shall review this Protocol every six months to ensure that it reflects current recommendations and best practices. They shall propose to the Board of Directors any amendments and updates necessary for its continuous development and improvement, taking into account suggestions made by professionals within the Group companies. Notwithstanding the above, this Protocol shall be amended whenever there is a significant legislative change or a material change in regulatory interpretation.

XII.- REPORTING BREACHES AND DISCIPLINARY MEASURES

If any employee of the Group companies becomes aware of, or has reasonable grounds to suspect, any breach of this Protocol, they must immediately report it through the channel established within Grupo Fedola's Internal Information System.

This channel is managed privately and confidentially.

Grupo Fedola will not tolerate any retaliation against any person who, in good faith, reports facts that may constitute a breach of this Protocol or any other internal policy or procedure.

Failure to comply with this Protocol shall be considered a breach of the Group's internal rules and may result in disciplinary measures.

Likewise, the Group companies reserve the right to adopt any measures they consider appropriate against business partners who fail to comply with this Protocol.

Grupo Fedola considers compliance with this Protocol to be the responsibility of all personnel.

XIII.- COMMUNICATION AND DISSEMINATION OF THE PROTOCOL

Employees are informed of the existence of this Protocol through the Group's internal communication channels. The Protocol is available to all interested parties through the corporate App.

ANNEX I – AI TOOLS AUTHORISED BY GRUPO FEDOLA

The AI tools authorised for professional use within Grupo Fedola companies, for which valid licences are held, are listed below in order of preference:

- 1st – Gemini. AI Assistant for Google Workspace.
- 2nd – ChatGPT Pro. AI tool developed by OpenAI.



1. The following AI practices are prohibited:

- a)** The placing on the market, putting into service or use of an AI system that deploys subliminal techniques beyond a person's consciousness, or deliberately manipulative or deceptive techniques, with the objective or effect of materially distorting the behaviour of a person or a group of persons by significantly impairing their ability to make an informed decision, thereby causing them to take a decision that they would not otherwise have taken, in a manner that causes, or is reasonably likely to cause, significant harm to that person, another person or a group of persons.
- b)** The placing on the market, putting into service or use of an AI system that exploits any vulnerabilities of a natural person or a specific group of persons due to their age, disability, or a particular social or economic situation, with the purpose or effect of materially distorting the behaviour of that person or of a person belonging to that group, in a manner that causes, or is reasonably likely to cause, significant harm to that person or another person.
- c)** The placing on the market, putting into service or use of AI systems for evaluating or classifying natural persons or groups of persons over a certain period of time based on their social behaviour or known, inferred or predicted personal or personality characteristics, resulting in a social scoring system that leads to one or more of the following situations:
 - i)** Detrimental or unfavourable treatment of certain natural persons or groups of persons in social contexts unrelated to those in which the data was originally generated or collected.
 - ii)** Detrimental or unfavourable treatment of certain natural persons or groups of persons that is unjustified or disproportionate to their social behaviour or the seriousness thereof.
- d)** The placing on the market, putting into service for this specific purpose, or use of an AI system to carry out risk assessments of natural persons in order to assess or predict the likelihood of a person committing a criminal offence based solely on the profiling of that person or on an assessment of their personality traits and characteristics. This prohibition shall not apply to AI systems used to support a human assessment of a person's involvement in criminal activity where such assessment is already based on objective and verifiable facts directly related to criminal conduct.

use of AI systems that create or expand facial recognition databases through the untargeted scraping of facial images from the internet or from closed-circuit television (CCTV) footage.

f) The placing on the market, putting into service for this specific purpose, or use of AI systems to infer the emotions of a natural person in workplaces or educational institutions, except where the AI system is intended to be placed on the market or put into service for medical or safety reasons.

g) The placing on the market, putting into service for this specific purpose, or use of biometric categorisation systems that classify individuals on the basis of their biometric data in order to deduce or infer their race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation. This prohibition shall not include the labelling or filtering of lawfully acquired biometric datasets, such as images, based on biometric data, nor the categorisation of biometric data in the context of law enforcement activities.

h) The use of real-time remote biometric identification systems in publicly accessible spaces for law enforcement purposes, except where, and insofar as, such use is strictly necessary to achieve one or more of the following objectives:

i) The targeted search for specific victims of abduction, human trafficking or sexual exploitation, as well as the search for missing persons.

ii) The prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons, or a genuine and present or genuine and foreseeable terrorist attack.

iii) The location or identification of a person suspected of having committed a criminal offence for the purpose of conducting a criminal investigation or prosecution, or executing a criminal penalty, in relation to one of the offences listed in Annex II and punishable in the relevant Member State by a custodial sentence or detention order with a maximum duration of at least four years.

The first paragraph, point **h)**, is without prejudice to Article 9 of **Regulation (EU) 2016/679** concerning the processing of biometric data for purposes other than law enforcement.

Systems:

The use of real-time remote biometric identification systems in publicly accessible spaces for law enforcement purposes, for any of the objectives referred to in paragraph 1(h) above, shall be deployed solely for the purposes established therein and only to confirm the identity of the specific individual who is the target of the operation. The following factors must be taken into account:

- a)** The nature of the situation giving rise to the potential use, and in particular the seriousness, likelihood and scale of the harm that would result if the system were not used.
- b)** The impact of the system's use on the rights and freedoms of the persons concerned, and in particular the seriousness, likelihood and scale of those consequences.