CODE OF ETHICS AND ARTIFICIAL INTELLIGENCE USE POLICY

INDETGROUP

1. Purpose and Scope

This document establishes the ethical, legal and operational rules governing the use of Artificial Intelligence (AI) tools at INDETGROUP, including generative models such as ChatGPT, AI assistants, and tools for generating text, images, code or data analysis.

It applies to all employees, external collaborators and suppliers who use AI on behalf of the company or within its systems.

It includes the use of tools such as:

- Language models (e.g. ChatGPT, Claude, Gemini or others)
- Image or design generators
- Automated analysis tools
- Programming or automation assistants
- Any AI integrated into corporate software

Corporate reference: INDETGROUP

2. Applicable Regulatory Framework

The use of AI at INDETGROUP must comply with current and future applicable legislation, including in particular:

2.1 European legislation

- General Data Protection Regulation (GDPR) (EU 2016/679): protection of personal data, processing limitations and international transfers.
- EU AI Act (European Artificial Intelligence Regulation): establishes obligations according to the risk level of AI systems (prohibited, high risk, limited risk and minimal risk). It includes requirements relating to transparency, human oversight and risk management.

2.2 Spanish legislation

- LOPDGDD (Organic Law 3/2018 on Personal Data Protection and Guarantee of Digital Rights).
- Legislation on trade secrets and intellectual property, including the Spanish Criminal Code and Law 1/2019 on Trade Secrets.
- Employment legislation applicable to the use of digital tools in the workplace.

2.3 International standards and good practices (recommended)

- ISO/IEC 27001 (Information Security)
- ISO/IEC 42001 (AI Management System)
- OECD Principles on Trustworthy AI

3. Guiding Principles for the Use of AI

The use of AI at INDETGROUP shall be governed by:

- Mandatory human oversight
- Data minimisation
- Confidentiality and trade secrecy
- Transparency regarding the use of AI where relevant
- Prohibition of automated decisions without human review
- Final responsibility always remaining with a human being

3.1 Artificial Intelligence Systems Inventory

INDETGROUP shall maintain an up-to-date inventory of all Artificial Intelligence tools and systems authorised for corporate use.

At a minimum, the inventory shall include:

- Name of the tool or system
- Manufacturer or provider
- User area or department
- Purpose of processing
- Data processed
- Assigned risk level
- Internal owner
- Authorisation date
- Integrations with corporate systems
- Geographical location of the data

No AI tool may be used in the corporate environment unless it has previously been assessed and authorised by the company.

3.2 Risk Classification of AI Systems

INDETGROUP shall classify the Artificial Intelligence systems it uses in accordance with applicable European legislation.

The categories shall be:

Unacceptable-risk systems

Systems that do any of the following may not be used under any circumstances:

- Violate fundamental rights
- Carry out social scoring
- Manipulate people's behaviour through subliminal techniques
- Exploit the vulnerabilities of minors or vulnerable groups
- Are prohibited by applicable legislation

High-risk systems

These shall require prior assessment, express authorisation and enhanced oversight.

Limited-risk systems

These may be used provided that appropriate transparency and human oversight are in place.

Minimal-risk systems

These may be used freely within the conditions established in this policy.

4. User Classification

4.1 Business Users (corporate or authorised licence)

Users with access to AI tools approved by INDETGROUP.

Conditions:

- They may use AI for operational tasks and professional support.
- They may work with internal information only if it is not sensitive or critically confidential.
- They must use approved corporate accounts.
- They are subject to auditing and traceability.

Advantages:

- Access to secure corporate tools
- Greater flexibility for professional use
- Integration with authorised internal systems

4.2 Free Users (free tools or personal accounts)

Users who use free versions or personal accounts of AI tools.

More restrictive conditions:

- It is PROHIBITED to enter any information relating to INDETGROUP.
- It is PROHIBITED to use customer, project or internal-process data.
- Only generic, educational or non-corporate writing use is permitted.
- They may not generate final content for external company use without a full review.

5. Classification of Information and Documents

5.1 Information PROHIBITED in any AI tool

The following may not be entered under any circumstances:

- Personal data of customers, employees or suppliers
- Internal financial information, including margins, revenue and budgets
- Commercial strategies, pricing or negotiations
- Non-public contracts
- Internal legal or tax information
- Access credentials, passwords or security data
- Unpublished proprietary technical information
- Data concerning ongoing customer projects

5.2 Documents permitted for use with AI (subject to oversight)

AI may be used to generate or assist with the following:

Communication and writing:

- Non-sensitive emails
- General internal communications
- Draft non-confidential sales presentations
- Generic marketing copy
- Descriptions of products or services that are already public

Operational documentation:

- General internal procedures (non-sensitive SOPs)
- Generic user manuals
- Meeting summaries without confidential data
- Translations of non-critical content

Creativity and support:

- Idea brainstorming
- Process-improvement proposals
- Alternative advertising copy
- Report structures

Technology:

- Programming assistance without disclosing sensitive proprietary code
- General technical explanations
- Non-production code examples

5.3 Restricted documents (prior authorisation required)

AI may be used only with the express approval of the responsible manager for:

- Commercial proposals for strategic customers
- Draft contractual documentation
- Internal financial reports
- Business analyses with strategic impact
- Legal or regulatory documents
- Content intended for official external publication

5.4 Documents prohibited as direct AI output

AI may not be the final source, without human review, of:

- Legal contracts
- Official company documentation
- External institutional communications
- Employment or disciplinary decisions
- Auditable financial reports
- Regulatory or compliance documents

6. Ethical Use and Prohibited Risks

It is strictly prohibited to use AI for:

- Identity impersonation
- Generation of false or misleading information
- Manipulation of customers or third parties
- Automation of critical decisions without human control
- Infringement of intellectual property
- Improper retraining on or extraction of sensitive data

6.1 Specific Artificial Intelligence Prohibitions

In addition to the prohibitions above, it is expressly prohibited to use AI systems to:

- Directly or indirectly discriminate against individuals
- Create automated profiles that produce legal effects without human intervention
- Make automated employment decisions regarding recruitment, dismissal, promotion or disciplinary action
- Carry out mass surveillance of employees
- Process special categories of data without legal authorisation
- Generate false information that appears authentic
- Develop content intended to deliberately deceive third parties

7. Security and Data Processing

- The entry of unnecessary personal data must be avoided.
- Internal files must not be uploaded to unauthorised tools.
- Only tools approved by IT/Compliance may be used.
- Any incident must be reported immediately.

7.1 Processing of Personal Data Using AI

Whenever an Artificial Intelligence tool involves the processing of personal data, the principles established in the General Data Protection Regulation (GDPR) must be respected at all times:

- Lawfulness
- Fairness
- Transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality
- Accountability

All processing must have a valid legal basis under Article 6 of the GDPR and must be compatible with the original purpose for which the data was obtained. Before processing begins, the responsible area must identify and document the applicable legal basis.

7.2 Special Categories of Data

The entry of special categories of personal data into Artificial Intelligence tools is prohibited unless a valid exception under Article 9 of the GDPR applies, an appropriate legal basis exists, and express authorisation has been obtained from Management together with prior validation by the relevant responsible person.

Special categories of data include:

- Health data
- Biometric data
- Genetic data
- Data concerning racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade-union membership
- Data concerning sexual orientation
- Data concerning an individual's sex life

The same restriction shall apply to information concerning criminal convictions and offences.

7.3 International Data Transfers

Before any AI tool is used, the location of the systems that process the information must be verified.

If data may be processed outside the European Economic Area, the company shall verify in advance:

- The existence of an adequacy decision
- Standard Contractual Clauses or other appropriate safeguards
- Supplementary measures where applicable
- Compliance with GDPR requirements

The use of solutions whose compliance framework has not previously been validated by the company is prohibited.

7.4 Data Protection Impact Assessment

The company shall conduct a Data Protection Impact Assessment (DPIA) before implementing AI systems where such systems may pose a high risk to the rights and freedoms of individuals.

The assessment shall examine, among other matters:

- Nature of the data processed
- Purpose of the processing
- Risks to affected individuals
- Potential bias
- Discriminatory impact
- Mitigation measures

7.5 Data Processors and AI Providers

Any AI solution that processes personal data must be validated in advance.

Before it is contracted or used, the following shall be verified:

- Provider identity
- Terms of use
- Privacy policy
- Implemented security measures
- Existence of a data-processing agreement where applicable
- Safeguards for international transfers
- Conditions governing the reuse of data for model training

Providers that do not offer sufficient guarantees of regulatory compliance may not be used.

7.6 Record of Processing Activities

Where the use of AI systems involves the processing of personal data, such processing shall be included in the organisation's Record of Processing Activities whenever legally required.

8. Transparency and Responsible Use

When AI makes a significant contribution to external content:

- Its consistency, accuracy and legal suitability must be reviewed.
- An internal declaration of AI use may be required.
- Final responsibility always rests with the employee or responsible area.

8.1 Transparency towards Customers, Suppliers and Third Parties

Where Artificial Intelligence plays a significant role in generating content, reports or interactions with third parties, the company shall assess whether it is necessary to disclose such use in accordance with applicable legislation and the principles of corporate transparency.

Transparency shall be particularly relevant where:

- Automated interactions take place
- Synthetic content is generated
- Virtual assistants are used
- Automated recommendations are produced

8.2 Enhanced Human Oversight

All use of Artificial Intelligence within the company shall be subject to effective human oversight.

No decision with legal, contractual, economic, financial, employment or reputational impact may be made solely by Artificial Intelligence.

The final decision shall always be made by an identifiable and accountable natural person.

9. Oversight, Audit and Compliance

INDETGROUP may:

- Audit the use of AI tools in corporate environments
- Review the traceability of use through business accounts
- Block unauthorised tools
- Apply disciplinary measures in the event of non-compliance

9.1 Management of Artificial Intelligence-Related Incidents

In addition to cybersecurity incidents, the following shall be considered AI-related incidents:

- Materially incorrect results
- Detected bias or discrimination
- Generation of misleading content
- Information leaks
- Use of unauthorised tools
- Incorrect automations
- Regulatory breaches

Every incident must be reported immediately to the designated internal owner and shall be recorded, analysed and addressed through corrective measures. Where it may constitute a personal-data breach, the internal data-protection procedure shall also apply.

9.2 Audit and Monitoring of AI Systems

The company may conduct periodic audits of authorised Artificial Intelligence systems to verify:

- Regulatory compliance
- Suitability of declared uses
- Quality of results
- Risk management
- Data protection
- Information security
- Compliance with this policy

10. Mandatory Training

The company shall promote training in:

- Responsible use of AI
- Data protection (GDPR)
- Cybersecurity applied to AI
- Good practices for professional prompting
- Risks associated with the use of generative AI

Training shall be proportionate to the level of responsibility and risk associated with each position.

10.1 Artificial Intelligence Officer

Management shall appoint an Artificial Intelligence Officer or, alternatively, an AI Governance Committee.

Its functions shall include:

- Approving new tools
- Assessing risks

- Maintaining the systems inventory
- Monitoring regulatory compliance
- Overseeing incidents
- Promoting training
- Periodically reviewing this policy

11. Regulatory Updates

This code shall be reviewed and, where appropriate, updated when:

- New provisions of the EU AI Act enter into force through its progressive phases
- The interpretation of the GDPR in relation to generative AI changes
- International security and compliance standards evolve
- New AI tools are introduced within the company

12. Acceptance

The use of any Artificial Intelligence tool at INDETGROUP implies express acceptance of this policy.

13. Document Classification Guide for the Use of Artificial Intelligence

This section establishes a practical internal classification system to determine whether a document or information may be processed using AI tools.

Its purpose is to ensure compliance with this code and reduce the risk of improper use of information.

13.1 Information Classification Levels

INDETGROUP adopts a four-level classification:

Level 1 - CRITICAL CONFIDENTIAL (PROHIBITED in AI)

Information that may not be entered into any AI tool under any circumstances.

This includes:

- Sensitive personal data relating to customers, employees or suppliers
- Non-public contracts or contracts under negotiation
- Detailed internal financial information
- Business strategy, expansion or investments
- Security data, access credentials or internal systems
- Unpublished proprietary know-how
- Information concerning ongoing customer projects
- Internal legal or regulatory incidents

Rule: If the information falls within this level, the use of AI is completely prohibited.

Level 2 - INTERNAL CONFIDENTIAL (RESTRICTED)

Sensitive but non-critical internal information. It may be used with AI only if it has been anonymised and prior authorisation has been obtained.

This includes:

- Non-public internal processes
- Internal operational reports
- Draft commercial proposals
- Non-strategic internal business analysis

- Non-critical internal technical documentation
- Sensitive internal communications

Mandatory conditions:

- Remove customer names, sensitive figures and identifying data.
- Use only authorised AI tools available to Business Users.

Level 3 - GENERAL INTERNAL USE (PERMITTED WITH BUSINESS AI)

Non-sensitive internal information. It may be used with AI without major restrictions within the corporate environment.

This includes:

- Standard operating procedures (SOPs)
- Internal support documentation
- Training materials
- Meeting summaries without sensitive data
- Non-confidential marketing content
- General service descriptions

Condition: Human review is always required before external use.

Level 4 - PUBLIC (FREE USE WITH AI)

Information that is already public or non-sensitive. It may be used freely with AI, including free tools.

This includes:

- Content from the INDETGROUP corporate website
- Public product or service catalogues
- Published marketing materials
- Press releases
- Public social-media content
- General industry information

Rule: Even if the information is public, its consistency must be reviewed before final use.

13.2 Quick Decision Tree: How to Determine Whether AI May Be Used

STEP 1 - Does it contain internal INDETGROUP data?

- Yes: proceed to Step 2.
- No: Level 4 (permitted).

STEP 2 - Does it contain customer data, financial information or strategy?

- Yes: PROHIBITED (Level 1).
- No: proceed to Step 3.

STEP 3 - Is it operational or non-critical internal information?

- Yes: restricted use; Business AI and possible anonymisation are required.
- No: proceed to Step 4.

STEP 4 - Is it only generic or public content?

- Yes: permitted.
- No: consult the responsible person.

13.3 Mandatory Anonymisation Rules

If a document is Level 2 (Internal Confidential), before AI is used the user must:

- Remove customer names and replace them with “Customer A”, “Customer B”, etc.
- Remove actual figures and use ranges or percentages.
- Remove specific locations if they are sensitive.
- Avoid descriptions that identify real projects.
- Do not include exact dates of strategic projects.

13.4 Practical Examples

BAD (prohibited in AI)

“Customer Telefónica has awarded us a EUR 250,000 project to implement X in Madrid.”

Level 1 - PROHIBITED

ACCEPTABLE WITH ANONYMISATION

“A customer in the telecommunications sector has awarded a high-volume project to implement a solution in Europe.”

Level 2 - Business AI only

PERMITTED

“Example structure for a commercial proposal for a customer in the telecommunications sector.”

Level 3

FREE USE

“Best practices for drafting commercial proposals.”

Level 4

13.5 User Responsibility

Each employee is responsible for:

- Correctly classifying information before using AI
- Not entering data without first reviewing its sensitivity level
- Consulting the compliance officer in case of doubt

13.6 Final Golden Rule

“If there is even the slightest doubt as to whether data is sensitive, it shall automatically be considered CRITICAL CONFIDENTIAL and shall not be entered into AI.”

14. Intellectual Property Rights and AI-Generated Content

Users shall be responsible for verifying that the use of content generated by Artificial Intelligence does not infringe third-party rights.

Before AI-generated content is used for commercial or contractual purposes, the following shall be reviewed:

- Ownership of rights
- Provider restrictions
- Copyright
- Image rights
- Registered trademarks
- Applicable licences

Content generated using AI must be reviewed before commercial exploitation or external publication.

15. Final Responsibility Clause

Artificial Intelligence is a tool that supports professional activity, but it does not replace professional judgement, legal responsibility or human decision-making.

Every person who uses Artificial Intelligence tools at INDETGROUP shall remain fully responsible for the information generated, reviewed, validated or disseminated using those tools.

16. Approval and Review Control

This policy must be approved by INDETGROUP Management. It shall be reviewed periodically and whenever there are regulatory, technological or organisational changes, or changes to the AI systems used. Each version must identify, at a minimum, the approval date, the current version, the approving body and the person responsible for maintaining it.