Digital Transformation Policy

of the Tecniplast Group

Code:	**ESG/GDL07-EN**
Version:	**01.02**
Validity date:	**16.03.26**
Classification:	**PUB -Public**
Type:	**Guideline (Group Policy)**

	Issuance	***Validation***	***Approval***
Role	Group Sust. & DT Director	Sust. Committee (SC)	Sust. Committee (SC)
Name	Roberto Crippa	On behalf of the SC	On behalf of the SC
Signature	*(signed in original)*	Mario Lombardini *(signed in original)*	Alessandro Bernardini *(signed in original)*

Glossary and Acronyms

The following definitions, acronyms or abbreviations are used in this document:

AI -Artificial Intelligence
According to the EU AI Act, a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. AI encompasses a wide range of technologies, including machine learning, deep learning, and natural language processing.

Company
The company for which this policy is effective, as stated by the Sustainability Committee of the Tecniplast Group.

Digital Transformation
The adoption and implementation of digital technologies to create new, or improve existing, business processes, products, or services in order to enhance effectiveness and efficiency by generating value added.

References

A number enclosed between square brackets [n] in the text refers to the following information sources:

[1] "Tecniplast Group Business Code of Conduct", Tecniplast, ESG/GDL01

[2] "EU Artificial Intelligence Act", EU, 2024/1689

[3] "General Data Protection Regulation (GDPR)", EU, 2016/679

Table of Contents

1 Purpose, Scope, Addressees

1.1 Purpose

The purpose of this policy is to define the criteria and guidelines to ensure that the digital transformation within the Tecniplast Group is conducted in accordance with the principles outlined in the Code of Conduct [1] and the applicable international legislation, ensuring in particular an appropriate, transparent and responsible use of the Artificial Intelligence (AI), and monitoring potential economic and social risks, and the impact on people's fundamental rights as well.

As the matter is ruled by local laws and regulations, concerned companies adopt the appropriate procedures for its enforcement.

1.2 Scope

This policy applies to the company’s digital transformation processes and AI use.

1.3 Addressees

This policy is addressed to all members of the company, and particularly to deployers and anyone in charge of managing digital transformation and AI use.
It also applies to the company's suppliers that develop and provide AI systems and services.

2 Introduction

The Tecniplast Group promotes the development of digital transformation and the use of AI as a tool to improve productivity and business processes to increase competitiveness in full compliance with human rights, current applicable laws, and adopted policies and governance models.

Coherently with the above, this policy addresses:

- Guiding principles informing digital transformation and AI use.
- AI management systems.
- Enforcement and control mechanisms.
- AI Providers’ requirements.
- Expected/sanctionable behaviors.

2.1 Risk Classes

As digital transformation may involve the use of AI systems, this policy complies with the risk classification provided by the EU AI Act [2], which aims to ensure that AI systems are implemented in a way that minimizes the risks of harming health, safety and fundamental rights of individuals.

In more details, the EU AI Act [2] identifies the following risk classes:

- **Unacceptable risk AI systems (prohibited AI)**
  These are all those systems that may constitute a clear threat to the individuals' safety and rights, or that may manipulate human behaviour in an attempt to circumvent free will, or that allow the attribution of a social scoring.
  In particular, they are systems aiming to:
  - Exploit human vulnerabilities.
  - Influence, alter or control in an explicit or subliminal manner individual behaviour to alter the autonomy of free choice by inducing concerned individuals to make decision that they would not have otherwise made.
  - Apply social scoring practices (i.e. evaluation of individuals on the basis of their behaviour, interactions and other personal data for discriminatory or illicit purposes).
  - Apply emotional recognition practices in working areas, regardless of the type of employment relationship in place.
  - Apply biometric categorization practices based on sensitive characteristics such as race, political opinions, trade unions membership, religious or political beliefs, sexual orientation.
  - Non-targeted collection of facial images from the internet or from closed-circuit cameras to create facial recognition databases.

  Remarks
  1. Recognition of physical states such as pain or fatigue is permitted

- **High-Risk AI systems**
  These are all those systems that can significantly impact people's lives.
  Their use is permitted but only in the presence of a series of requirements.
  In particular, and by way of example, they are systems falling into one of the following areas:
  - Hiring or selection of individuals, in particular to publish targeted job advertisements, analysis or filtering candidates' applications and evaluation.
  - Making decisions entailing the employment relationship conditions, promotion or termination of contractual employment relationships, assigning tasks on the basis of individual behaviour or personal traits and characteristics.
  - Monitoring and assessment of individuals' performance and behaviour within such employment relationship.

- **Limited/minimal Risk AI systems**
  These are systems that pose a moderate risk and are subject to transparency obligations. Concerned users should be informed that they are interacting with an AI system. (e.g. chatbots like ChatGPT, antispam software).

3 Guiding Principles

3.1 AI Ethical Guiding Principles

Activities entailing the digital transformation and the use of AI shall be systematically based on the consideration and application of the following guiding principles:

- The use by the company is intended to improve working conditions and productivity of work performance in full respect of people, their fundamental rights and information security.
- It cannot be carried out in conflict with human dignity, nor can it violate the confidentiality or availability of personal data, or violate cybersecurity principles. Data processing shall always be carried out in compliance with the GDPR [3] provisions.
- Access to AI systems shall ensure compliance with the principles of diversity, equity and inclusion.
- Diversity includes demographic and personal characteristics such as gender, gender identity, age, disability, sexual orientation, ethnicity, nationality, race, political or personal opinions, and religious belief.
- The use of AI systems must be guaranteed without prejudice to:
- Freedom of expression and association.
- Thoroughness, impartiality and fairness of communication.
- Cybersecurity shall be ensured throughout the AI systems and models lifecycle, in compliance with Tecniplast Group policies and applicable laws and regulations.
- In particular, resilience against illicit attempts to modify their use, behaviour and security features shall be ensured.
- AI systems' inputs and behaviour shall be monitored.
- Particular attention shall be paid to managing system updates, as they may affect AI models' behaviour.
- The company shall ensure lawful, correct and transparent processing of personal data and compatibility with the purposes for which they were collected.
- Proper information shall be appropriately communicated or made available to concerned parties.

3.2 AI Use Guidelines

In addition to the afrementioned ethical guiding principles and in order to properly use AI in business operations, the following guidelines are set:

- Only use the chatbot (Copilot, Chat GPT, etc.) enterprise versions: free versions offer no security or non-disclosure guarantee of information, with potential extremely serious business and legal consequences.
- Be specific in requests and interactions with AI: generic or approximate requests generate generic or approximate outcome. Always provide context and give precise instructions on expectations (e.g., writing style, content length, what to include and what to exclude, level of detail).

- Avoid providing redundant or inconsequential information to the request: unnecessary information generates “background noise” and defocuses AI.
- Always scrutinize the outcome: AI does not reason like a human and is susceptible to hallucinations or wrong conclusions if not properly guided. Human oversight of the outcome (Human-In-The-Loop) is essential.

3.3 Technical Guiding Principles

Coherently with the definition of digital transformation, and in addition to the aforementioned ethical guiding principles, eligible digital transformation initiatives shall meet the following technical guiding principles:

1. The number of actors and steps in a process shall be reduced to the bare minimum, and shall exclude activities that do not generate objective value.
2. Homogeneous tasks shall be performed with homogeneous processes.
3. For each process, manually entered information shall be entered once, and only once.
4. Manually entered information shall be limited to what is strictly necessary.
5. Manual activities that can be performed automatically or digitally are not permitted, unless doing so manually is more economically convenient.
6. For every piece of information or process element there shall be one, and only one, source of origin (master).
7. All slave sources shall be fed by the concerned master sources.
8. Homogeneous activities shall be performed with homogeneous systems.
9. Data structures that are not exclusively used by a process or system shall be shared and traceable to the same logical structure.
10. Systems limiting data exchange are not permitted. Ease of data exchange is a key requirement.

As a general rule:

- Initiatives meeting all ten guiding principles are deemed as “eligible”.
- Initiatives meeting less than eight guiding principles are deemed as “non-eligible”.
- Initiatives meeting eight or nine guiding principles shall be scrutinized to be deemed as “eligible” or “non-eligible.”

Eligible initiatives are then further assessed in terms of similarities, dependencies and cost/benefits in order to build the Digital Transformation Roadmap.
The Roadmap is re-assessed every year, or when the situation calls for.

The aforementioned technical guiding principles materialize the logic according to which an eligible digital transformation initiative shall be approached by a cascaded consideration of:

- The optimization of concerned processes.
- The build-up and tuning of data and information needed for their correct functioning.
- The concerned IT architecture and software applications used to manage the aforementioned processes.

4 AI Management System

In order to ensure a responsible and safe development, use and management of AI systems in compliance with the guiding principles set out in this policy, the company shall adopt the below listed practices.

4.1 Surveillance

- The company shall establish appropriate surveillance mechanisms on the adopted AI systems, ensuring the possibility of human intervention (Human-In-The-Loop), as well as that the AI system complies with applicable laws.
- Designated personnel shall possess the necessary skills, as well as adequate training and authority.
- In particular for High-Risk AI systems, the company shall carry out a preventive assessment before authorizing their use.

4.2 Technical and Organizational Measures

No matter the AI system risk class, the company shall:

- Perform a risk assessment identifying potential risks and harms associated with the use of AI systems, as well as their likelihood and impact (e.g.: bias risks of pre-training data (data poisoning), or risks from the use of pre-trained components used for training models (model poisoning).
- Implement security standards (protection from breaches, losses, etc.) and transparency (understandability and clear documentation of AI models, in compliance with the GDPR [3] accountability principles).
- Assess data process compliance with the GDPR provisions [3].
- Strengthen security measures to -where possible and applicable- protect AI systems from cyberattacks and data breaches.
- Ensure - by adopting verification and review practices- that AI algorithms are bias-free from and do not generate discrimination.
- Establish mechanisms for effective human supervision on AI systems.
- Train concerned staff in the responsible use of AI systems and in respecting workers' rights.
- Keep detailed documentation of the AI systems in use and concerned risk assessment procedures.

In particular, when dealing with High-Risk AI systems, the company shall also:

- Adopt appropriate technical and organizational measures for compliant use, ensuring that such systems meet security and transparency requirements.
- Entrust human oversight and use of AI systems to competent persons.
- Monitor the system functioning.
- Perform an impact assessment on fundamental rights pursuant to AI Act [2] art. 27.

4.3 Training, Notification, Whistleblowing

- The company shall provide concerned personnel and users with the appropriate training so that they can fully understand and assess the potential risks associated with the systems they are using, and act accordingly.
- Image, video and audio content generated by AI systems that appreciably resembles existing persons, objects, places (Deep Fakes) shall clearly be disclosed as artificially generated.
- This is also to ensure compliance with the principle of transparency and copyright legislation.
- The company shall adequately protect those reporting actions or practices contrary to this policy, in compliance with the company's provisions and applicable laws on whistleblowing.

5 AI Providers' Requirements

When choosing providers of AI systems and models, priority shall be given to solutions that ensure localization and data processing in data centres equipped with robust disaster recovery and business continuity procedures, and capable of ensuring the highest standards in terms of security and transparency in the methods of developing and training applications based on generative AI.

In particular, concerned providers shall:

- Ensure compliance with all the obligations set out in the AI Act [2] and other applicable European standards, as well as the provisions contained in this policy, to the extent of their competence.
- Ensure the functioning transparency of AI systems (how they operate, their capabilities and limitations), and provide the necessary information so that decisions based on them are made in an informed manner.
- Notify whether the system provided can be deemed as an AI system, and what its risk level is.
- Adopt security measures that take due account of:
  - Complexity of AI models (architecture and number of parameters).
  - Model appropriateness with their intended use.
  - Ability to interpret and explain the obtained outputs.
  - Training dataset characteristics (size, integrity, quality, sensitivity, age, relevance, diversity).
  - Value of using model hardening techniques (e.g. adversarial training).

6 Enforcement and Control Mechanisms

Compliance with this policy is assessed through:

- Establishing supervisory bodies.
- Internal audits by bodies appointed by the company.

The company shall set procedures and operating instructions for the enforcement of this policy and the assessment of its effectiveness.
As an example, effectiveness measures may be statistics entailing:
- Internal and external dissemination.
- Policy understanding.
- Number of audits and their outcome.
- Reported policy infringements.

7 Behaviours

7.1 Expected Behaviours

In reference to the aforementioned guiding principles, and regardless of the type of activity performed, the following behaviours are expected:

- Every company's employee, no matter the role or grade, shall behave -both in form and substance- according to the principles stated in this policy.
- Every person accountable for personnel management shall ensure the application of the principles stated in this policy, acting appropriately in case of critical situations.
- Every AI provider shall comply with the requirements of this policy, to the extent of its concern.

7.2 Sanctionable Behaviours

The following are deemed sanctionable behaviours:

- Violation, by anyone, of the principles stated in this policy.
- Failure, by concerned personnel appointed by the company, to ensure compliance with this policy.
- Infringement by AI providers of the applicable principles set by the Code of Conduct [1] and by this policy.
- Failure of application, or incorrect application of this policy.

In case of sanctionable behaviours by the addressees of this policy, the company reserves the right to sanction them proportionally to their severity and the consequent proven or potential effects, and always in compliance with current labour matter laws and regulations.

In case of sanctionable behaviours by AI providers, the remedies provided by applicable law are put in place, as well as the provisions regulating the supply relationship.

END OF THE DOCUMENT

(This page intentionally left blank)