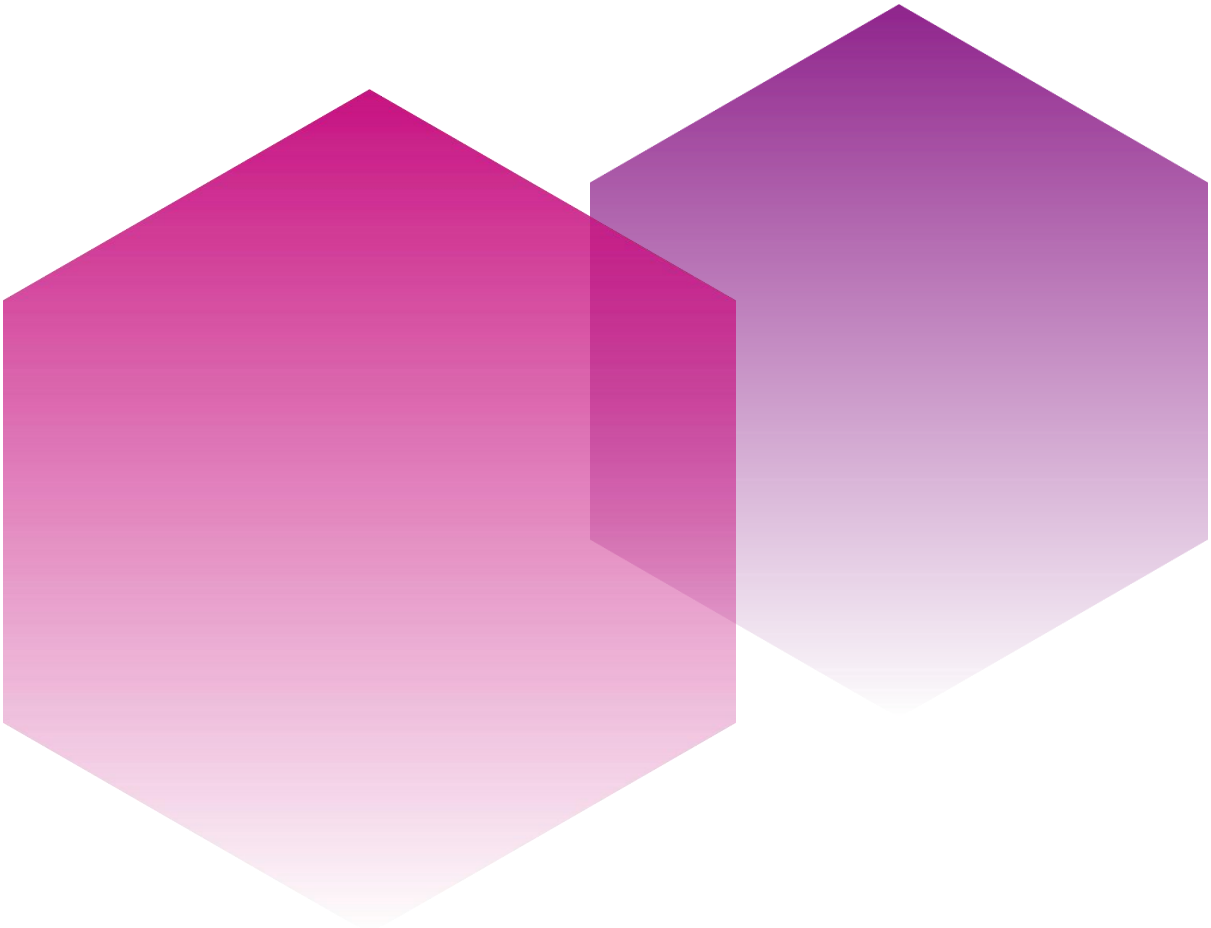
AI Policy



Classified as General

1. Introduction

This AI policy (hereinafter, the "**Policy**") establishes the principles and responsibilities governing the development, deployment, and use of Artificial Intelligence ("**AI**") technologies within the Advania Group.

In this Policy, "**AI**" refers to the ability of computer programs and other technologies to mimic human abilities, such as understanding natural language, recognizing images, solving problems, and making decisions, and that can be used to predict and automate tasks normally performed by humans. AI encompasses several subfields, including machine learning. Advania operates as a Provider and/or as a Deployer of AI Systems (each as defined below).

The objective with this Policy is to ensure that AI Systems used or built within the Advania Group are safe, transparent, ethical, compliant with applicable laws, and aligned with the Advania Group's values of innovation, responsibility, sustainability and respect for human rights (in accordance with the Advania internal Code of Conduct).

It is a strategic objective of the Advania Group that its Staff actively adopt and make use of AI in their work. The Advania Group encourages all Staff to make full use of approved AI tools to improve the quality, efficiency and innovation of the work they do and the services Advania provides. This Policy exists to enable the safe, responsible and confident use of AI across the Advania Group: it sets out how to use AI well, and is not intended to discourage, delay, or act as a barrier to the adoption of AI. Where a question of interpretation arises, this Policy should be applied in a way that supports, rather than impedes, the responsible use of AI.

2. Scope

This Policy applies to all Advania Group companies and all its employees, management, board members, part-time employees, consultants, secondees, temporary workers, trainees, and any equivalent roles (jointly "Staff") who deploy or use AI technology in the course of their duties. The Policy is communicated during the onboarding of Staff and is available to read on www.advania.com, as well as on the local websites and intranets. All Staff are responsible for periodically reviewing this Policy and ensuring that they understand its requirements in the context of their respective roles.

3. Definitions

In this Policy, capitalised terms have the meanings set out below. Certain additional terms are defined in the body of this Policy where they appear.

- "**AI Model**" means the underlying large language models, and similar technologies, on which AI Systems are based.
- "**AI System**" means 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 that can influence physical or virtual environments. Further guidance on the interpretation of this definition can be found here: https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-ai-system-definition-facilitate-first-ai-acts-rules-application
- "**High-Risk AI System**" means an AI System that is classified as high risk under the EU AI Act, due to the potential impact of its use on health, safety, fundamental rights, or other significant interests. Examples of High-Risk AI Systems include: (i) AI Systems used in employment, workers' management and access to self-employment, including e.g. AI Systems used for the recruitment and selection of individuals and reviewing CVs; (ii) AI Systems used for biometric categorisation or emotion recognition; and (iii) AI Systems used as safety components of regulated products.

- "**Output**" means any output produced by an AI System including predictions, content, recommendations, or decisions.
- "**Prohibited AI Systems**" means any AI System or AI practice that is prohibited under the EU AI Act. Examples of Prohibited AI Systems include AI Systems that deploy subliminal techniques beyond a person's consciousness or purposefully manipulative or deceptive techniques to distort a person's or group's behaviour by impairing their ability to make informed decisions, where this causes or is reasonably likely to cause significant harm.
- "**Provider**" means an entity that develops an AI System, or has an AI System developed, and places it on the EU market or puts the AI System into service under its own name or trademark, whether for payment or free of charge.
- "**Deployer**" means an entity using an AI System under its own authority.
- "**Personal Data**" means personal data as defined in Article 4(1) of the General Data Protection Regulation (Regulation (EU) 2016/679) (the "**GDPR**") (i.e., any information that relates to any individual who is identified, or identifiable, directly or indirectly, from that information whether in isolation or in combination with any other available information).

4. Policy Statement

Guiding principles

Advania Group endorses the responsible use and development of AI and aims to be at the forefront of innovation in this field. Accordingly, the Advania Group actively encourages all Staff to embrace AI in their day-to-day work, within the framework set out in this Policy. However, Advania recognises the importance of using AI in a responsible, ethical, and legally compliant manner, especially when it comes to generating content and protecting confidential information and Personal Data.

Advania is committed to ensuring that all AI Systems for which any Advania Group company is a Provider and/or a Deployer respect fundamental rights and freedoms, are transparent, fair, and accountable, and comply with applicable laws and regulations in each jurisdiction where Advania operates. This includes, where relevant, the EU AI Act, the GDPR, and other applicable national or regional legal frameworks.

Consequently, the Advania Group has zero tolerance for the use of AI for any purpose which is unlawful, including, without limitation, using or building Prohibited AI Systems. Using or building AI Systems for such purposes is prohibited under all circumstances.

Each member of Staff is responsible for their own use of AI, including the information shared in connection with the use of AI and how the results are used. As part of this responsibility, Staff are required to ensure that they know which information is classified as confidential and/or constitutes trade secrets within Advania Group.

Approved AI Systems, AI Models, and third party Providers

The default position is that Staff members should only use AI Systems and AI Models that have been approved by the relevant local function responsible for information security, data protection and compliance. Staff members should be aware that there are AI Systems that are available on the internet or as standalone apps or programs (collectively, "Non-Approved AI Systems"), that allow the user, as a private individual, to accept the terms of use, and that have not been approved by Advania. Examples of Non-Approved AI Systems are the publicly available versions of ChatGPT, Claude, Gemini, Copilot, and similar services. Since most Non-Approved AI Systems lack adequate confidentiality provisions, data protection provisions, encryption, and security measures, (even where they are provided by highly reputable Providers) Staff members are prohibited from inputting any sensitive company data (even where such information has been anonymised or de-identified),

confidential information, proprietary source code, trade secrets or Personal Data into any such Non-Approved AI Systems, except as specified in this Policy.

Legal and Ethical Compliance

All AI use must comply with applicable laws and regulations in each operating country. Each member of Staff who uses any AI System is responsible for ensuring that they understand whether Advania is the Provider and/or a Deployer of that AI System, and for ensuring that their use of that AI System is compliant with the obligations imposed on Providers and/or Deployers (as relevant) by applicable law. In addition, where Advania is a Deployer of an AI System provided by a third party, each Staff member who uses that AI System must ensure that they have read, and comply with, the Provider's instructions regarding the use of that AI System.

AI must not be used to circumvent legal, ethical, or contractual obligations.

Use of AI does not make it lawful to carry out actions that would otherwise be unlawful.

Compliance with the EU AI Act

All usage of AI Systems that meet the definition of "AI Systems" under the EU AI Act must comply with the relevant requirements in the EU AI Act, even where that usage takes place outside the EU.

Any person or function responsible for the development, procurement, or deployment of an AI System must classify such AI System according to the following risk categories: prohibited (not allowed), high risk, or limited risk and assess what role Advania Group has in relation to the relevant AI System (e.g. Provider or Deployer).

If an AI System is, or is likely to be, a High-Risk AI System (as defined above), the relevant Staff members responsible for that AI System must, prior to any use of that AI System, consult with the CISO Forum and Group legal before procuring or deploying any such system, and for further guidance on how the applicable requirements for such system shall be fulfilled. The contact details for the CISO Forum and Group legal are: aigovernance@advania.com

AI Systems with limited risk are subject to certain transparency requirements, including that the end-user must be made aware that they are interacting with an AI or that content has been produced by AI.

The transparency obligations apply to both Providers and Deployers, but in different aspects. For example, Providers of AI Systems intended to interact with individuals have an obligation when it comes to the design of the limited risk AI System, and Deployers of an AI System that generates or manipulates image, audio, or video content constituting a "deep fake" have an obligation to disclose that content has been AI-generated. It is therefore essential that Staff members understand Advania's role as a Provider or Deployer in relation to each AI System Advania uses or develops.

All Staff members involved in the development or use of AI Systems and/or AI Models must maintain a sufficient level of AI literacy to enable the informed, responsible, and ethical use of AI Systems.

AI Systems must be used fairly and without discrimination. AI Systems used in decisions affecting individuals must be assessed and monitored for bias and discriminatory impact.

Transparency and Accountability

When using AI for any external-facing or internal-facing purposes, Staff members should be transparent about this, especially where a High-Risk AI System is being used.

AI Systems should be explainable (wherever possible), documented, and auditable.

AI-generated or manipulated content not reviewed by humans must be clearly labelled if there is a risk that individuals could be misled into believing that it is genuine.

When AI Systems are used in internal operations, full transparency shall be maintained regarding what AI Systems have been used and the extent to which any material has been generated by AI.

Staff members who use AI Systems in the course of their duties are responsible for ensuring that an appropriate accountability framework is in place, which sets out the responsibilities of management and the relevant Staff members with regard to ensuring that the requirements regarding transparency and compliance are fulfilled.

The use of Non-Approved AI Systems

Staff members must not enter sensitive company data, confidential information, trade secrets, source code, proprietary technology of Advania Group or any customers, or Personal Data of any person, into any Non-Approved AI Systems. This applies even where such information has been anonymised or de-identified. Use of Non-Approved AI Systems with such information is only permitted where:

(a) prior approval has been granted in writing by the CISO Forum;

(b) appropriate legal and practical measures have been implemented to technically and contractually ensure that the input cannot be accessed, retained, or reused by the Provider of the relevant Non-Approved AI System or by other users of the relevant Non-Approved AI System, or by any third party; and

(c) the use of the Non-Approved AI System does not place Advania Group in breach of any confidentiality obligations owed to customers or other third parties.

Staff members must be aware that both inputs and Outputs may be subject to third-party rights and cannot automatically be used by Advania Group. A plagiarism check must be performed to ensure that material that is generated or manipulated by AI, and that is intended for use within or outside Advania's business, does not infringe the intellectual property rights of any third party. Infringement, including copyright violations arising from AI-generated or AI-manipulated content, may result in legal claims.

Staff members must not input unlawful content, infringing content, or any content that includes intellectual property owned by a third party unless the Staff member has the legal right to use such content in this manner.

All AI-generated or AI-manipulated Output must be verified by the relevant Staff member responsible for the use of the AI System, for accuracy, legality and alignment with Advania Group values before being used internally or externally. In addition to the plagiarism checks noted above, this includes fact-checking, assessing reliability, and reviewing for coherence and completeness.

AI Systems in product and software development

Members of Staff must treat all Output from AI Systems as draft material and not the final product. Output from AI Systems is never considered final and must always undergo human review. Staff members must review all Output critically, verifying that it is correct and appropriate for the intended use. The use of AI may not act as a substitute for Staff members' judgement and expertise.

To improve the prospects of copyright protection, Staff members must maintain records of the human creative process, including the sources of information used, the AI Systems used, model/version, prompts/instructions, key settings, dates/times, the resulting Output, and the developer's own contributions (design choices, edits, refactoring and any original code), together with the reviewer/approver.

If AI Systems are used in product or software development, Staff members must enable and maintain duplicate or similarity monitoring tools and configure these safeguards to block identical or near identical matches to publicly available code (such as GitHub's blocking and reference matching features) and set minimum

detection thresholds to prevent the generation of suggestions that replicate code licensed under open-source software license terms.

System Integration

- AI Systems must not be integrated into Advania's internal systems (e.g., by creating dependencies on AI Systems, or requiring the use of an AI System in order for internal systems to function as intended) without documented approval from the relevant internal system owner.

- All AI Systems used by Staff members in the course of their duties (including any Non-Approved AI Systems used in accordance with this Policy) must be continuously monitored for compliance, performance and improvement opportunities.

- If the use of AI Systems affects organizational data, approval must be obtained from the relevant data owner to ensure lawful and compliant data handling.

- AI Systems must be designed to identify and mitigate security vulnerabilities, including risks such as data leakage, unauthorized disclosure of sensitive information (even where such information has been anonymised or de-identified), data poisoning, and other cybersecurity threats.

- All use of AI Systems shall be documented in an appropriate level of detail, to the extent necessary to comply with applicable legislation, regulatory requirements, and contractual obligations, including requirements for traceability and auditability.

Internally developed AI solutions

Staff members may build internal AI Systems, agents, or automations using AI and embed AI functionality into existing systems, subject to the following requirements:

- Internally developed AI Systems must comply with all legal requirements applicable to AI Systems and all requirements in this Policy.
- Internally developed AI Systems must comply with the same governance, security and review principles as any externally sourced AI.

Governance and Oversight

- All use and development of AI Systems is subject to continuous monitoring and review.

- Governance processes must be implemented by the Staff members responsible for deciding to use and/or develop AI Systems, to ensure compliance with this Policy, relevant laws, and internal standards.

- Violations of this Policy may result in disciplinary action or termination of AI use.

Human Oversight

- AI must support, not replace, human decision-making in critical areas.

- Human oversight is especially important with regards to High-Risk AI Systems.

5. Roles, Responsibilities and Accountability

1. Staff members have a duty to read, understand and act in alignment with this Policy, and any other supporting documents provided by Advania Group, as well as, if required, undergo mandatory trainings at the interval set by Advania Group or each local company. A Breach of this Policy may result in disciplinary action.

2. System Owner: Each AI System in use must have a designated system owner who is responsible for the risk classification, appropriate use, and ongoing oversight of that AI System. The system owner is also responsible for reviewing the applicable Advania policies and ensuring that the AI System is compliant with those policies, and documenting that compliance assessment. **No Staff member may use an AI System for which such a compliance assessment has not been completed.**
3. Managers at all levels are responsible for ensuring that the Staff members within their respective business area understand and comply with this Policy and that anyone working with AI on behalf of Advania has a sufficient level of AI literacy. Training and competence requirements shall be adapted to the individual's role, technical background, and the context in which the relevant AI Systems are used. This is a delegated responsibility from the local CEO.
4. The local CEO of each Advania Group company is responsible for the local implementation of and compliance with this Policy within each respective company.
5. The General Counsel is responsible for reviewing this Policy, at least annually or when deemed necessary due to legal or technological changes, adopting necessary updates and ensuring its effective communication and implementation, including by raising relevant issues with the Group CEO.
6. The ultimate responsibility for the review and approval of this Policy lies with the Board of Directors of Advania Holding.

6. Policy Review

This Policy shall be reviewed annually or upon significant regulatory or technological changes.

Revision history

Version	Author and position	Comment	Date of Board approval
1.0	Group General Counsel	Version created by Advania Group and White & Case	16 June 2026