amadeus

Amadeus AI Policy

Amadeus Group Corporate Policy

10 December 2024

amadeus

Table of Contents

amadeus

I. INTRODUCTION AND FOUNDATIONS

1. Purpose

The Amadeus AI Policy ("Policy") establishes the Amadeus Group wide framework for the use, deployment and development of artificial intelligence ("AI"). At Amadeus, the use, deployment and development of AI must be conducted in line with ethical standards and relevant legal requirements, such as the Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonized rules on artificial intelligence ("**EU AI Act**").

As a signatory of the AI Pact, Amadeus has publicly pledged that it will make best efforts to meet and contribute to the commitments of 1) adopting an AI governance strategy to foster the uptake of AI in the organization, 2) work towards future compliance with the EU AI Act and 3) to promote awareness and AI literacy of our staff and other persons dealing with AI tools on our behalf.

This Policy applies throughout our entire organization, i.e., not only to operations taking place within the European Union.

2. Scope of this Policy

This Policy applies to all employees and contractors (here grouped as "employees") of Amadeus IT Group SA and all its affiliated companies, including, insofar as possible, non-fully owned companies and distributors ("**Amadeus Group")**. The policy covers all AI-related activities, whether the employees are involved in the development of AI tools (such as software engineers, data scientists, and R&D teams), and the deployment and use of AI tools (such as business operations, product teams, marketing, People & Culture, and customer service, etc.).

An 'AI tool' is any type of tool (including (underlying) models) that generates outputs (such as predictions, content, recommendations, or decisions) based on an inferencing capability. This includes all machine learning-based systems but could also be systems with e.g., logic-based approaches. It does not only encompass large language models and systems based on them (such as ChatGPT) or other generative AI (such as GitHub Copilot, Midjourney), it could (also) include e.g., search and recommender systems, smart assistants and agents, chatbots, detection and recognition technologies, copywriting systems and text editors and analytics systems. Any type of tool that is being advertised as 'AI' is likely to be caught, but even tools which are not advertised as such and have **inferencing capacities** should be treated as AI tools to which this Policy applies.

The definition of "AI tool" encompasses both "AI Systems" and "AI Models":

An **AI system** is a machine-based system that can work on its own to different extents. It can learn and adapt over time and use the information it receives to produce outputs like predictions, content, recommendations, or decisions that can affect the real or digital world. However, it does not include systems that simplify follow human-defined rules to carry out tasks automatically.

AI models are algorithms trained on large datasets to learn from examples and get better over time. They can perform many different tasks that can be added to other systems or applications, which may then become AI systems.

This Policy applies in addition to other policies that touch on the same subject(s), such as our Artificial Intelligence security standard and security and privacy policies, which can be found here: Security and Privacy Policies & Standards Framework

3. Rationale for this Policy

While AI tools provide many advantages, certain challenges are inherent when deploying, developing or using AI, including:

- Potential shortcomings of AI tools, such as inaccurate/undesirable/unsuitable outputs, persistence of bad patterns, inexplicability/intransparency, security issues, ethical concerns.
- Breach of regulations related to AI, data, including personal data, etc.;
- Leak of Amadeus' confidential information or personal data;
- Infringement of rights of others.

These risks can result in consequences such as:

- **Fines** of up to 7% of the Amadeus total worldwide annual turnover.
- Obligation to **compensate for damages** (including indirect damages) for breach of contracts or infringement of rights of other parties.
- **Leaks of company secrets** or other sensitive or confidential information, including our customers' and partners' data.
- **Reputational damage**, resulting in loss of competitive advantage / hurting our business, or damage to employee motivation/commitment with Amadeus.

Following the principles and rules included in this Policy when handling AI tools will help mitigate these risks.

4. Alignment of our AI Ethics Principles with the AI Act

The EU AI Act is an EU regulation that has been established to ensure that AI tools are safe and respect fundamental rights. Although not all AI tools developed and/or deployed by Amadeus are regulated by the EU AI Act, Amadeus adopts its underlying principles and corresponding key provisions to guide all AI practices within our organization. These principles are closely aligned with our Amadeus AI Ethics Principles (now described in Chapter II below), which aim to ensure that our AI tools are developed and deployed in an ethical and responsible manner.

The EU AI Act's core principles emphasize the importance of the ethical principles of human agency and oversight, technical robustness and safety, privacy and data governance, transparency, diversity, non-discrimination and fairness, societal and environmental well-being and accountability in AI tools. The EU AI Act operationalizes these principles through specific requirements, many of which are reflected in this Policy. By keeping in mind these requirements when dealing with AI tools, even with regard to AI tools that are not regulated by the AI Act, Amadeus aims to uphold the highest standards of AI ethics, reduce our legal exposure and contribute to the broader goal of fostering trust in AI technologies.

5. Ensuring appropriate understanding of AI

Amadeus' AI Literacy program aims to provide employees with the skills, knowledge, and understanding that they need to use and manage AI tools responsibly and safely. This includes:

1. **Understanding AI**: Knowing what AI is, how it works, and its potential applications.
2. **Awareness of Risks and Opportunities**: Being aware of both the benefits and the possible harms AI can bring and understanding how certain risks can be mitigated.
3. **Informed Use**: Being able to make educated decisions about deploying and interacting with AI systems, considering the specific context and the people affected by these systems.

This is crucial for making the most of AI while minimizing risks. All Amadeus employees are required to participate in Amadeus's AI training and literacy program.

II. AMADEUS AI PRINCIPLES FOR DEVELOPMENT AND DEPLOYMENT/USE

1. What is AI Ethics at Amadeus?

AI Ethics is a system of moral principles and techniques intended to inform the responsible development and use of artificial intelligence technology. The purpose of setting AI Ethics Principles is to establish a framework to foster "responsible artificial intelligence", by providing stakeholders with guidance when faced with an ethical question arising during the lifecycle of an AI tool.

At Amadeus, we believe that the computational intelligence of AI should be used to build technology that is not only reliable and trustworthy, but also adheres to the highest ethical standards.

The use of AI technologies could have broad impacts on individuals and society, raising complex and challenging ethical questions. For example, in the travel industry, the use of biometrics can be used for making decisions that can impact individuals heavily. For our internal processes, a recruitment system can be used to decide about who gets hired or fired. Because of the potential impacts of AI tools, organizations need to develop AI codes of ethics.

Amadeus is committed to attaining the benefits of AI tools while protecting health, safety and fundamental rights as described in many charters, declarations and constitutions around the globe, including the Charter of Fundamental Rights of the EU[1], that might be impacted by the use of AI technology by Amadeus.

At Amadeus, we adhere to the principles described in the next section that we believe should guide both AI development and use. To achieve these objectives, we must set out from the very beginning of each AI tool's development with an "algor-ethical" vision, i.e. an approach of ethics by design. Ethics must be embedded in the design and development process of an AI tool right from the outset. The same applies to deployment of tools: we should keep these principles in mind from the procurement stage and throughout the entire time that we are using the tool.

2. The 6 Amadeus Principles for Development and Deployment/Use of AI Tools

Embracing the transformative potential of AI for the travel industry in an ethical fashion

When developing AI tools at Amadeus, designers and developers should be aware of and follow our principles, as detailed below. These will help safeguard the trust that our customers put in us already today for future AI products and services that Amadeus will provide.

[1] More information on the Charter and full text : https://commission.europa.eu/aid-development-cooperation-fundamental-rights/your-rights-eu/eu-charter-fundamental-rights_en

Before starting the design and/or development process, please check Annex 1: Amadeus AI Prohibited and High Risk Development and Use List, in order to ensure that you are not developing a prohibited use case and to get approval immediately when you are planning to develop a restricted use case, as these usually have to comply with many technical and organizational requirements before they would legally be allowed to go on the market or be put into service. All AI tools developed by Amadeus need to be registered in the **Amadeus AI Inventory.**

2.1. Fairness and human oversight: AI tools should treat all people fairly

Fairness is a concept rich of facets and no single, unified definition applies. Under EU regulation, it entails non-discrimination and means that AI tools are developed and used in a way that includes diverse actors and promotes equal access, gender equality and cultural diversity, while avoiding discriminatory impacts and unfair biases. For Amadeus, in addition, fairness means that AI tools should treat everyone fairly and decide based on representative data. For example, an AI tool should make the same travel recommendations and provide the same pricing offers to anyone with the same destinations, cabin class, and dates.

We believe that mitigating bias starts with people understanding the implications and limitations of AI predictions and recommendations.

Amadeus recognizes the importance of training its developers to understand the meaning and implications of AI decisions so that they can supplement those decisions with sound human judgment. Amadeus also enforces strict governance over how training, testing and validating data is collected, processed, and analyzed. This includes a special focus on minimizing biases that could lead to discrimination, especially against vulnerable groups. When designing and building AI tools, developers should understand how bias can be introduced (without the intent to do so) and how it can affect AI-based recommendations. To help mitigate bias, algorithms should be trained with datasets that reflect the diversity of society. The design models used should allow the AI tool to learn and adapt throughout its lifecycle without developing biases. To help developers create AI tools that treat everyone fairly, Amadeus enables them to leverage tools, methodologies, techniques, and other resources that help detect and mitigate biases.

Besides risks of bias, fairness entails that the tool's risks more generally to health, safety and fundamental rights should be assessed and managed. This includes not only risks related to use in accordance with the tool's intended purpose, but also risks related to reasonably foreseeable misuse of the tool. Risk monitoring and management should be done throughout the lifecycle of the tool and should also continue after deployment. These risk management and monitoring efforts should be proportionate to the amount of risk the tool entails, meaning that very risky tools (for example those employing biometrics and/or facial recognition or those making decisions about individuals) should be subject to more intense risk management processes than tools that entail low risk (such as tools for internal administration practices).

In addition, human oversight is integral to Amadeus' AI tools. We incorporate mechanisms that allow human operators to monitor and, if necessary, intervene in the AI tool's operations. This includes the ability to override, halt, or modify the tool's actions if the outcomes are deemed inappropriate or harmful.

Requirements for implementing fairness practices:

- Understand the scope, intent, and potential uses of the AI tool.
- Ensure diversity in the group of designers and developers.
- Throughout the lifecycle, test and validate AI tools for fairness.
- Measure possible biases on both the input data and outcomes of the tools. Take corrective actions if these biases could lead to discriminative behavior.

2.2. Reliability and safety: AI tools should perform reliably and safely

To build trust, it's critical that AI tools operate reliably, safely, and consistently both under normal circumstances and in unexpected conditions. Amadeus maintains an appropriate level of accuracy throughout the entire lifecycle of the AI tool, and we should implement technical measures to protect our tools from faults and errors.

A reliable AI tool relies on accurate data. Amadeus already has dedicated data quality management systems in place. We will build on these systems to meet the challenges presented by advancing AI tools. These systems should also be able to operate as they were originally designed, respond safely to unanticipated conditions, and resist harmful manipulation. For that reason, risk management should be conducted throughout the lifecycle of the AI tool, to continually identify, evaluate, and address potential risks to health, safety, and fundamental rights of individuals.

Additionally, a bespoke resilience by design approach for AI tools should be part of every new development. It is also important to be able to verify that these tools are behaving as intended under actual operating conditions. How they behave and the variety of conditions they can handle reliably and safely largely reflects the range of situations and circumstances that developers anticipate during design and testing. We believe that rigorous testing is essential during system development and deployment, to ensure AI tools can respond safely in unanticipated situations without unexpected performance failures and evolve in ways that are inconsistent with original expectations. We should also ensure that our tools are resilient against misuse, and avoid negative impacts on vulnerable groups, including minors.

After testing and deployment, it is equally important that we properly operate, maintain, and protect the AI tools throughout their life cycle. Otherwise, AI tools can become unreliable or inaccurate over time.

Requirements for implementing reliability and safety practices:

- Involve domain experts in design and implementation processes.
- Conduct rigorous testing throughout the entire lifecycle of the AI tool
- Perform regular maintenance and monitoring of AI tools

- Provide a feedback mechanism for deployers and other stakeholders to report performance issues.

2.3. Privacy and security: AI tools should be secure and respect privacy

Protecting privacy and securing personal and business information is paramount for Amadeus. However, as AI becomes more prevalent, achieving this is more critical and complex than ever. With AI, privacy and data security issues require especially close attention since access to data is essential for AI tools to make accurate and informed predictions and decisions about people. Existing privacy laws already set the standards AI tools must adhere to in order to be compliant. For instance, they require transparency about what data is collected, how it will be used and stored, and who has access to it, demand appropriate means to safeguard the processed data and mandate a concrete legal basis for the processing for a specific purpose. AI tools must therefore prioritize and safeguard individuals' privacy and data rights and provide explicit assurances about how personal data will be used and protected.

Compliance with privacy laws will be facilitated by minding the principle of data minimization from the outset of creating an AI tool and throughout its lifecycle, ensuring that only the minimum data necessary to fulfil the purpose of the AI tool is stored and collected. Additionally, accuracy is important. Training, testing and validating data sets must be relevant, representative, and, where possible, free of errors. Further, data processing activities, such as labelling, cleaning, and updating, must be carried out meticulously to ensure the data accurately represents and keeps representing the real-world conditions that the AI tool is designed to address.

As new intelligent technology emerges, we must also be prepared for emerging and evolving privacy and security threats. Data protection begins with designing and deploying solutions that employ privacy and security practices such as encryption and access control methodologies. Amadeus is very well equipped to face these upcoming challenges. We build upon a sophisticated privacy and security environment that will evolve to safeguard the personal and business data processed in our AI tools.

Also, beyond privacy, we should maintain an appropriate level of robustness and cybersecurity and implement technical measures to protect our systems from faults, internal and external threats, including data poisoning and adversarial attacks aimed at manipulating AI outputs., ensuring system integrity and security throughout the AI tool's lifecycle. Our tools should be designed to withstand environmental challenges, human interactions, and system failures. Amadeus includes fail-safes and redundancies where necessary. For tools that learn from real-world data, we ensure that feedback mechanisms do not introduce new biases over time.

Requirements for implementing privacy and security practices:

- Conduct security and privacy reviews throughout the lifecycle of the AI tool, in accordance with the relevant Privacy and Security policies.

- Adhere to the Artificial Intelligence Security Standard

2.4. Transparency: AI tools should be explainable and otherwise transparent

Deployers of our AI tools should be able to understand and contextualize how and why the tool arrived at a particular output, especially where the tool is making determinations or recommendations with potential implications. An AI tool is truly explainable if its functionality and operations can be explained non-technically to a layperson. This applies to the tool's decision-making processes, including the logic behind the algorithms used to make decisions. This will help not only ensure that outputs can be explained to impacted individuals, but will also help identify potential performance issues, safety and privacy concerns, biases, exclusionary practices, or unintended outcomes.

Not only the decision-making criteria of AI tools need to be understandable, but also their purpose and objectives. Those who operate AI tools should be clear about when, why, and how they choose to deploy them. Remember that if we cannot interpret a tool, neither can deployers.

Requirements for implementing transparency practices:

- Ensure that clear, comprehensive technical documentation is prepared that contains the necessary information about the workings of the AI tool.
- Ensure that deployers can understand, interpret, and utilize the AI tool's outputs appropriately.
- Provide instructions for our AI tools, explaining their capabilities, limitations, and associated risks.

2.5. Accountability: People should be accountable for AI tools

Accountability norms aim to ensure that AI tools are not the final authority on any decision that impacts people's lives and that humans maintain meaningful control over AI tools and ensure that care and scrutiny are present to avoid and monitor issues such as bias.

Amadeus has established a dedicated internal review body, the AI Office, to provide oversight and guidance to the highest levels of the company on which practices should be adopted to help address the concerns discussed above and on particularly important questions regarding the development and deployment of AI tools. This body also helps with tasks like defining best practices for documenting and testing AI tools during development or providing guidance when an AI tool will be used in sensitive cases (e.g., employing facial recognition or other biometric technologies).

Requirements for implementing accountability practices:

- Have roles and responsibilities defined in our organization covering the earliest stage of development and until the end of the lifecycle of an AI tool. Always assume you are responsible for a tool you are helping to design and develop but ensure that it is also clear who carries final responsibility and that they have signed off on your choices. Always ensure that people with relevant expertise are in the loop.

- Design AI tools to automatically log events throughout their lifecycle. These logs are critical to maintaining the traceability of the AI tool's operations and should be capable of capturing any events that could result in risks or system modifications. We should ensure that these logging capabilities support monitoring the tool after it enters the market and facilitate the identification of risks.

- Register and keep track all of fine-tuning and/or modifying of third-party models (including LLMs and other foundation models).

2.6. Sustainability

Travel industry sustainability and climate change in particular, are global challenges by definition, and Amadeus will work in cooperation to provide global solutions. In this context, Amadeus has been reinforcing its strategy to address environmental concerns, especially in cooperation with industry stakeholders. Amadeus' environmental sustainability strategy is based on three pillars: (1) the environmental efficiency of our operations; (2) the development of IT solutions that help our customers improve their environmental efficiency; and (3) partnering with industry stakeholders in joint sustainability initiatives.

As regards machine learning and artificial intelligence we develop technology solutions that help to improve the operational efficiency of customers, and this improvement is linked in many cases to better environmental performance. The environmental benefits of Amadeus solutions expand to a wide range of stakeholders in the industries our customers are in, including airlines, airports, travelers and cities.

For example, we use advanced algorithms that estimate demand and analyze risk of disruptions to help airlines make fundamental decisions related to airline networks, flight frequencies and equipment, reducing the use of resources (fuel, aircraft, airport infrastructure, etc.) per passenger flown.

Ultimately, we do not lose sight of the sustainability of the process of creating AI tools. Said process comprises usage of sustainable power supplies, and infrastructures as well as e.g. the re-usage of data. This will help to reduce the carbon footprint throughout the entire life cycle of an AI tool, meaning during design, training, development, validation, re-tuning, implementation and its usage.

<u>Requirements for implementing sustainability practices</u>:

- Collect and use only the data essential for each project, minimizing storage needs.
- Optimize model efficiency, for example, by running computations during off-peak hours.

III. GENERAL RULES FOR DEPLOYMENT/USE OF ALL AI TOOLS

Before deploying, and even before procuring, an AI tool, please check **Annex 1: Amadeus AI Prohibited and High-Risk Development and Use List**, in order to ensure that you are not procuring/deploying a Prohibited use case and obtain approval before you are procuring/deploying a High-Risk use case, as the use of these is subject to strict regulatory requirements.

All uses of AI tools procured/ deployed by Amadeus need to be **registered in the Amadeus AI Inventory.** Employees shall log their use case for review and approval of the ***AI Use Case Review Board: LOP - AI Use Case Intake - Power Apps***. *This step is* mandatory.

The registration process enables Amadeus to categorize the AI Use Case based on risk and assign it to the relevant internal review and validation process. Maintaining an up-to-date inventory is essential for compliance.

Additionally, the AI Principles as formulated above should also, to the extent possible, be implemented when we deploy/use AI tools within Amadeus, with an emphasis on fairness and transparency. This translates to the following:

- When deploying AI tools, we must **use them in accordance with the instructions for use** provided by the supplier of the AI tool. This is important because the AI tool might not be accurate in regards purposes that the supplier has not approved it for, and not sticking to the instructions could also breach our contractual or other legal obligations.

- Before deploying an AI tool for purposes related to HR, we should always deliberate about **informing employees/workers' representatives** and the affected employees/workers that they will be subject to the use the tool.

- Before deploying an AI tool for making decisions or assisting in making **decisions related to individuals**, we should always liaise with Legal about informing these individuals about our use of the tool.

- Before deploying an AI tool for any purposes, we should always deliberate with Legal about the necessity to carry out a **data protection impact assessment**.

- We should ensure that **input data are relevant and sufficiently representative** in view of the intended purpose of the AI tool, in order to prevent for example, bias from emerging.

- Individuals need to play a critical role in making decisions about how and when an AI tool is deployed, and whether it is appropriate to continue to use it over time. Human judgment will be key to identifying potential blind spots and biases in AI tools. We should therefore **assign human oversight** for the deployment of AI tools to persons who have the necessary competence, training and authority, as well as the necessary support to carry out this oversight well. Generally, everyone who operates the tool should be able to understand how it should work in order to be able to notice when outputs are unreliable and avoid over-reliance on the outputs.

- Before deploying an AI tool for any purposes, always liaise with Legal on whether and how long we should **keep logs** of the tool, so that we can adequately **monitor** it over time and have a **track record** if something goes wrong.

- AI tools can become inaccurate or otherwise unreliable over time and when applied in different contexts. We should **monitor the operation of the tool**. If we notice risks or incidents regarding the tool that can have impacts on health, safety or fundamental rights or if the tool does not function as expected, always immediately report this to Legal.

IV. ADDITIONAL SPECIFIC RULES FOR USAGE OF GENERATIVE AI TOOLS: THE GENERATIVE AI ACCEPTABLE USE POLICY

The principles above apply generally to our deployment and development of all AI tools. When tools are generative in nature, please also take into account the following.

Generative AI ("GenAI") solutions enable creation of content (e.g., text, audio, video, image). GenAI relies on deep-learning models ("**GenAI Models**") that can generate content outputs from large amounts of data they were trained on in response to user prompts.

Amadeus recognizes GenAI as a promising and exciting technology to streamline work functions, increase efficiency and/or develop internal or external products that our customers love. Whilst encouraging the use of GenAI, it comes with certain risks to confidential and sensitive information, intellectual property and corporate values. This chapter strives to protect these, with the objective of ensuring **legal, ethical and secure** use of GenAI at any time. This paragraph defines acceptable and prohibited uses and outlines employees' obligations related to the use of GenAI Tools (as defined below).

1. Scope

This chapter covers the usage of GenAI Solutions and GenAI Technology (together "**GenAI Tools**") by all Amadeus' employees and contractors on company devices and/or personal devices (when used for work purposes). This applies regardless of whether these tools are publicly available or officially approved/installed for corporate use (enterprise licences).

- **GenAI Solutions** refers to "ready to be used" tools, services or applications such as chatbots (e.g. ChatGPT, Gemini, Microsoft Web Copilot) that leverage GenAI models to perform specific tasks. GenAI Solutions are designed to be user-friendly and require minimal technical knowledge to operate. As such, they can be used by employees across all the departments of the organization for activities such as automating tasks or generating content.

- **GenAI Technology** refers to the underlying technology, services and tools used to develop GenAI applications, products or services. GenAI Technology requires a certain level of technical expertise to be used effectively. It includes platforms and services (e.g. Azure AI services) for developers to build, train and deploy GenAI models.

Differences in acceptable usage between publicly available or approved corporate tools are set out in the **GenAI Acceptable Use Framework** attached to this Policy.

2. Rules

To protect our employees and clients from harm, and to protect the company from reputational damage, employees adhere to the following rules:

2.1. Protect sensitive information

Information is shared with GenAI Tools by user prompts, or a series of instructions or questions for the tool. The use of GenAI Tools increases the risk of inadvertently exposing the company's sensitive information to third parties as the tool may train its model on the data received through prompts and display it in other users' output.

Under Amadeus Information Classification and Asset Management Policy, **sensitive information** means any information that is not classified as [**PUBLIC**], including information classified as [**CONFIDENTIAL**], [**HIGHLY CONFIDENTIAL**] or [**SECRET**]. It also includes personal data or third-party proprietary information.

To maintain the **security** of our data and IT systems and protect the **confidentiality** of our company's sensitive information (including employees' and customers' personal information, proprietary know-how and data), Amadeus users are prohibited from accessing unapproved GenAI Tools when (i) using company systems or networks, (ii) conducting business on behalf of the company (including on personal devices) and/or (iii) using company's data.

- **Do not** input sensitive information or personal data into non-approved Gen AI Tools.
- **Do** remember that access and use of unapproved GenAI Tools from the office environment is only tolerated when using [**PUBLIC**] data.
- **Do** disable the chat history and purge the chat history after each session when using unapproved or publicly available GenAI Tools.
- **Do** contact your manager, or the Legal Department if you are unsure whether the information you are planning to input falls into sensitive information.
- **Do not** use company credentials, email addresses, or telephone numbers as a login to access publicly available GenAI Tools.
- **Do not** use GenAI tools on personal devices to circumvent company policies or safe-guards.
- **Do not** use or install non-approved APIs, plug-ins, connectors, or software related to GenAI tools.
- **Do not** implement or use in any way code generated by non-approved GenAI models on company systems.
- **Do not use Gen AI** to undermine company security.
- **Do** review the Company's Artificial Intelligence security standard and security and privacy policies by clicking here.

To avoid potential data leaks, security incidents and avoid violation of Amadeus contractual obligations with customers or vendors or, in some cases, violation of applicable law:

2.2. Provide transparency

- **Do** clearly attribute any output used for business purposes to the GenAI application that created it through a footnote or other means visible to the reader.
- **Do** maintain an updated record of GenAI use for business purposes and be able to share those records with your manager or other authorized company personnel upon request.

We aim to provide our employees, third parties, and customers with transparency regarding how we use and deploy GenAI to support our work. To protect the company from claims against intellectual property rights infringement or misappropriation of such rights, and ensure transparency, all GenAI generated content must be disclosed, cited and reviewed if used for business purposes (e.g. any purpose related to your work at Amadeus) to enable end-users to determine how to consume the content in an informed manner.

2.3. Be critical of outputs and carefully use them

- **Do** acknowledge that GenAI tools do not reflect human understandings or emotions or creativity and should not be use as a substitute for human judgment.
- **Do not** use any output that contains material that you suspect to be under copyright protection in any materials, internal or externally facing.
- **Do not** rely on or use information that you suspect to be inaccurate, inappropriate or biased (e.g. information that discriminates against individuals on the basis of race, color, religion, sex, national original age, disability, marital status etc.).
- **Do not** use GenAI Tools to create text, audio, or visual content for purposes of committing fraud or to misrepresent an individual's identity.
- **Do** review output provided by GenAI Tools to make sure it meets Company standards for principles of equity, ethics and appropriateness.

Outputs created by GenAI tools may provide fictitious answers sometimes referred to as 'hallucinations', false information or answers. Outputs may also contain copyrighted information, or others' intellectual property. While ownership in many of these cases is unclear, users should err on the side of caution and **remain accountable** for their use of Gen AI Tools and review any biased outputs which may not be aligned with Amadeus' values and our commitment to diversity, equity and inclusion. All employees and contractors are expected to comply with applicable laws, regulations, or company policies regarding the use or development of GenAI content or tools.

2.4. Go through the approval process before procurement/deployment

Use of GenAI Tools on company devices **must** comply with the above-mentioned rules and follow the **GenAI Acceptable Use Policy** available here Use of GenAI tools for business purposes on personal devices to circumvent company policies or safeguards is strictly prohibited.

Employees shall log their use case for review and approval of the **GenAI Use Case Review Board:** LOP - AI Use Case Intake - Power Apps. This step is mandatory.

The AI Use Case Review Board is a transversal forum underneath the AI Office where experts from different functions (LEG, Security, DTS, BDP, Tech etc.) review, approve or decline Generative AI Use Case (based on description of the use case, data inputted and technology). The Board meets on a weekly basis and delivers its decisions within a target of 2 weeks depending on the complexity of the use case.

Please note that approval by the GenAI Use Case does not exempt you from following any other standard Amadeus processes (IT Software governance, CISO, Privacy etc.).

Considering how fast changes relating to GenAI Tools are happening, the GenAI Acceptable Use Framework may not be exhaustive or of all possible use cases. If a use case is not specifically listed, a user should request approval from the Board.

For more information on this process, you can consult this page.

V. GOVERNANCE OF THIS POLICY

1. Who to contact about this Policy

Corporate and Legal Affairs (CLA) is responsible for developing, implementing and overseeing compliance with this AI Policy, including the awareness and dissemination to those who should know of it. For any questions or feedback regarding the Policy, please send an e-mail to AIact@amadeus.com .

2. Understand that we may monitor compliance with the Policy

Amadeus reserves the right to access and monitor the use of GenAI Tools on any company-issued devices or that appears on company managed networks to ensure compliant use of these systems in accordance with Amadeus Acceptable Use Policy.

3. Understand that non-compliance with the Policy can have consequences

Employees who fail to comply with any provision of these rules may be subject to disciplinary actions up to and including termination of employment. Violations by contractors may be considered breach of contract and result in removal from assignment. Any AI-related activities which appear to violate applicable laws will be reported to external law enforcement.

If monitoring systems and processes detect a possible policy violation or if a user reports a possible policy violation, the suspect event should be processed using appropriate security incident response processes.

All employees are encouraged to report instances of non-compliance with this Policy through the Speak Up reporting channel. Employees who report misconduct or concerns in good faith will not be retaliated against. For more information, see Speak-up Policy.

4. Changes to the Policy

Amadeus will review the Policy as relevant to ensure it remains up to date considering the pace of evolution of AI technology and the regulatory environment.

Any changes to this Policy will be communicated to Amadeus employees and contractors via standard means of corporate communication (email, NEO, Yammer etc.).

ANNEX 1: AI Prohibited and High-Risk Development and Deployment/Use List

The following practices and use cases are always prohibited or restricted, both with regard to development and deployment. If you are in doubt about whether a practice or use case falls within the scope below, please contact AIact@amadeus.com

PROHIBITED PRACTICES

The following practices are strictly prohibited (under the EU AI Act and can result in fines of up to 7% of the total worldwide annual turnover of Amadeus. No one within Amadeus may therefore engage in these practices under any circumstances, including through AI Tools which have been approved:

a. **Subliminal, manipulative and/or deceptive techniques** with the risk of significant harm. For example, using an AI tool to manipulate people´s opinion (by creating fake news) in order to influence the outcome of elections.

b. Exploitation of **vulnerabilities of persons** in a manner that is reasonable likely cause significant harm. For example, creating a voice-assisted doll encouraging dangerous behavior in children or challenges in the guise of a game.

c. **Biometric categorization** to infer sensitive personal traits. For example, using AI to categorize passengers by their facial images to infer their race.

d. **Classification or scoring** of people based on behavior or personality characteristics leading to detrimental treatment. For example, forbidding a person to attend university due to low social credit from minor infractions.

e. Real-time remote **biometric identification in publicly accessible spaces** for law enforcement purposes, except in limited cases. For example, cross- checking faces captured by live cameras in a town square against a terrorist database.

f. **Predictive policing** based solely on profiling or assessment of personality traits. For example, using AI tools to identify persons, based on their facial image, located in publicly accessible spaces, commonly frequented by pick pocketers, for alerting policemen.

g. Untargeted **scraping of facial recognition databases**. For example, using an AI tool to scrape of facial images from the internet, social media platforms or CCTV footage.

h. **Inferring emotions** in workplaces and education. For example, using AI tools to assess employees' moods during work hours based on vocal tone, speech patterns, and micro-expressions.

HIGH-RISK PRACTICES

The following use cases are a sub-set of high-risk AI practices as potentially relevant to Amadeus. They are generally heavily regulated pursuant to the AI Act and should therefore never be developed and/or deployed without prior approval of Legal, as fines for not complying with the requirements can result in fines of up to 3% of the total worldwide annual turnover of Amadeus:

- Tools (intended to be) used for the following purposes:

    1. **Biometrics:** remote biometric identification of individuals, biometric categorisation of individuals and/or emotion recognition of individuals (including facial recognition).
    2. **Safety of critical infrastructure:** to directly protect physical integrity or health and safety of individuals and property in relation to the management and operation of critical digital infrastructure (e.g., data centres, IXPs, cloud computing services), or in the supply of water, gas, heating, or electricity;
    3. **Recruitment and HR**: decision-making in the area of recruitment and HR (e.g., selection, evaluation, assessment, promotion, termination, task allocation and monitoring of employees and/or other workers and/or applicants);
    4. **Credit(worthiness)**: evaluating creditworthiness of individuals or establishing their credit score (with the exception of financial fraud detection);
    5. **Immigrant identification**: detecting, recognising or identifying individuals (with the exception of verification of travel documents) in the context of migration, asylum or **border control management**.

PRACTICES SUBJECT TO TRANSPARENCY OBLIGATIONS:

The following use cases are regulated in the form of specific transparency obligations and should therefore never be developed without prior advice from Legal:

- tools that are designed to interact directly with individuals;
- tools which generate content, including audio, image, video, or text