Group Policy Artificial Intelligence (AI)

Group Policy No.	Version	Valid as of
022	01	22 October 2025

Group Policy Owner	Approved by	Hierarchy of rules
Chief Information Officer	Executive Board (*Vorstand*) TUI AG	Group Policy

Who needs to comply with this Group Policy

To put it simply: Everyone at TUI Group.

More specifically: All **directors, officers and employees** of TUI AG and of all companies majority-owned, directly or indirectly, by TUI AG, whether domestic or foreign, and of any other shareholdings, where management control directly or indirectly lies with TUI AG ("**Managed Group Companies**") need to comply with this Group Policy. Directors, officers and employees of companies where management control does not lie with TUI AG ("**Non-Managed Group Companies**") need to comply with this Group Policy if it has been implemented in their respective company.

In addition, employees seconded by **third-party** service providers of TUI Group, **consultants**, whether or not in full or part-time, seasonal, temporary or permanent capacity and all other persons engaged to conduct business on behalf of a TUI Group company need to comply with this Group Policy.

Each of the above mentioned persons is also referred to in this Group Policy as "**you**".

1. Purpose

Artificial intelligence (AI) offers huge potential to support and enhance TUI's business. Applications include, for example, virtual chat agents, personalised content and recommendation engines, video and image enhancement and speech recognition. However, the science behind AI is very complicated, the technology is

developing, and the outputs may not always be reliable or well understood. AI is not truly 'intelligent' at this point in time, it does not know whether source data is true and correct, it does not necessarily recognise potentially offensive or unacceptable output. AI solutions must be used in a considered, transparent, responsible and secure way. TUI recognises the importance of building an environment where every colleague feels informed and confident in embracing the opportunities AI brings. This policy sets out the legal and ethical considerations you must follow when using AI applications in TUI's business.

2. Understanding AI

AI is the science of making intelligent machines and computers. 'Machine learning' is the most relevant branch of AI where computers use mathematical problem-solving processes known as algorithms combined to form complex networks which can process and analyse data.

'Generative AI' refers to learning models that can take raw data and generate statistically probable outputs when prompted, which appear as considered, educated responses. Generative AI platforms are generally trained on data lakes (centralised repositories that ingest and store large volumes of data in their original form) and question snippets (search result generated extracts which contain relevant content from a website that matches the user's search query). Such AI training involves billions of parameters that are constructed by software processing huge archives of images and text. Examples of generative AI include ChatGPT, Microsoft Copilot or Midjourney.

AI platforms identify patterns and relationships, which they then use to create rules and then make judgments and predictions when responding to a prompt. At a high level, generative models encode a simplified representation of their training data and draw from it to create a new work that is similar, but not identical, to the original data.

3. Permitted Applications, AI Risk and Ways of Working

It is important to note that **although AI is a particular technology application you should approach it no differently from any other business service**. AI software and tools must be assessed and used in accordance with relevant TUI Group and local policies, guidance, business processes and risk considerations (for example, IT security, legal, data privacy and procurement). **Appropriate due diligence (background investigation) and risk assessment must be undertaken as relevant to the role and scope of the AI application in the business**.

An AI application may only be used in TUI's business if it is:

a) an authorised third-party application licensed for business use by TUI in accordance with the TUI Group Procurement Policy; or
b) developed internally by TUI and complies with TUI's AI Lab requirements of accountability and governance set out in section 4.1 below (Transparency: Governance, Accountability and Labelling); or

c) a third-party AI tool into which no confidential information or personal data is input or processed and which is either a generative chatbot such as ChatGPT (appropriately licensed to you for relevant use) or an AI tool being tested or trialled for potential use in TUI's business with the AI Lab informed.

Please be aware that **certain applications of AI systems are deemed 'high risk'**. These include **AI applications used in employment and workers management, in particular for the recruitment and selection of persons** (to place targeted job advertisements, analyse and filter job applications, and evaluate candidates), for making decisions affecting terms of employment, promotion and termination of employment, for allocating tasks on the basis of individual behaviour, personal traits or characteristics and for monitoring or evaluation of employees. You must ensure any such 'high risk' use of AI applications only falls within categories a) and b) above and is appropriately authorised, monitored and recorded. It is not always apparent or obvious that certain use of AI falls within this category so each use must be carefully considered.

Specific AI risks and rules may change over a short space of time so if you are in any doubt as to any of the guidance set out in this policy please consult the relevant teams (Legal, Data Privacy or IT Security) referenced in the sections below.

4. Principles

There are six key principles to consider when using AI in TUI's business which are explained in more detail in the following pages:

- **Transparency: Governance, Accountability and Labelling**
- **Data Privacy and Confidential Information Protection**
- **Fairness: No unfair bias or discrimination**
- **Human Agency and Decision Making**
- **Respect for Intellectual Property Rights and Responsibility**
- **Safety, Security and Robustness**

Compliance with all principles must be accounted for on an ongoing basis. Monitoring, feedback and evaluation are key components of the successful use of AI in TUI's business.

4.1. Transparency: Governance, Accountability and Labelling

The key to ensuring compliance with the AI principles is transparency through **proper management of relevant AI projects**. All projects or initiatives involving the introduction or development of AI in TUI's business must identify a stakeholder within TUI with relevant accountability for the AI project. It is such stakeholder's responsibility to:

- **submit the application project or initiative to the AI Lab** for review, guidance and steering;
- **implement a governance programme** to oversee the AI project lifecycle either themselves or by the appointment of a responsible programme manager; and
- **keep TUI's portfolio management updated**, according to the current lifecycle of the application, project or initiative.

The programme manager or stakeholder must implement a successful governance programme which will:

- **define the roles and responsibilities of people working on the AI project** to ensure compliance with TUI Group Policies and due processes;
- **incorporate the feedback and steering from the AI Lab review** (as above); and
- improve AI's performance and trustworthiness and reduce risk throughout the AI lifecycle through **regular monitoring, re-assessment and review**.

Accountability includes the requirement that the use of AI tools must be appropriately authorised and licensed under a written contract. The contractual terms with service providers must include appropriate com-pliance with these AI principles as relevant. For any legal queries please email techlaw@tui.com.

All interactive AI systems, such as chatbots or AI assistants, must comply with labelling requirements that allow users to make informed decisions. Users (employees or customers) must be made aware when they are interacting with an AI application so they can decide whether they want to continue using it. It must be made clear to users when they are interacting with an AI chatbot or other AI generated response system unless it is obvious from the point of view of the user that this is the case. **Unless it has been reviewed by a human** any AI generated or manipulated text which is published with the purpose of informing the public on matters of public interest shall disclose that the text has been artificially generated or manipulated (See also section 4.4 below (Human Agency and Decision Making)).

AI can be legitimately used to enhance the quality and appeal of photos, videos and other content. However, AI must only be used to generate or manipulate images, videos or audio that appreciably resemble existing persons, objects, places, entities or events and would falsely appear to a person to be authentic or truthful (known as '**deepfakes**') if such content is **clearly labelled distinguishably disclosing its AI origin**. AI applications such as image, video and text enhancement must be used appropriately and responsibly and in accordance with relevant advertising standards. You must not mislead customers.

4.2. Data Privacy and Confidential Information Protection

You must ensure that confidential information and personal data is properly protected at all times and kept secret. Confidential information and personal data should not be used with AI tools unless you are sure it is kept confidential and secure. It is your responsibility to ensure that generative AI tools involving the input and output of confidential information and personal data are kept appropriately safe and secure and may be accessed by only the people for whom the confidential information or personal data is intended. **You**

must be careful to only use TUI authorised AI applications to process confidential information and personal data (for example the Microsoft Copilot with the 'Enterprise Data Protection' green shield symbol ticked) as set out in Section 3 (Permitted Applications, AI Risk and Ways of Working)**.** You must only use your TUI business accounts, and not personal accounts or any unauthorised AI applications, to process confidential information or personal data.

AI applications that process personal data must comply with the **Group Policy Data Privacy, Group Manual Data Privacy** and data protection laws. If processing personal data you must consider data protection obligations from the outset. You should take a risk-based approach to data privacy compliance. This means assessing risks to the rights and freedoms of data subjects that may arise when using AI and implementing appropriate and proportionate technical and organisational measures to mitigate these risks. **It is important to engage your Data Protection Officer as early as possible when considering AI applications**. Please email dataprivacy@tui.com.

4.3. Fairness: No Unfair Bias or Discrimination

The data sources used by generative AI models may contain elements of unfair bias, discrimination or false information. The algorithms involved may inadvertently produce biased or discriminatory output, as data sets will often contain cultural biases of the groups that created the majority of the content.

AI applications must be assessed for inclusivity and avoidance of discrimination (for example, voice recognition, facial recognition and generative AI for minority groups) by stakeholders and users as relevant. AI generated content must be monitored by stakeholders and users as relevant to eradicate or minimise unfair bias and to avoid stereotyping or discrimination. If bias or discrimination is, or becomes, apparent, use of the tool must be suspended and referred to the AI Lab for assessment.

AI systems must provide a similar quality of service for all relevant demographic groups.

4.4. Human Agency and Decision Making

TUI does not seek to replace human intelligence, judgement or creativity with AI. **AI should support and enhance employees' capabilities in their roles.** Since new technological innovations may involve changes to the processes and procedures associated with particular job roles, TUI is committed to supporting our workers through this transition by investing in initiatives to promote skills training around AI.

AI tools can provide accurate and detailed data collection, analysis and prediction. However, data sources and outputs may contain errors or false information and cannot necessarily be trusted. All **AI generated information and data should be verified by a responsible person if it is to be relied upon for any significant decision making, justification or publication** with the purpose of informing the public on matters of public interest. AI tools must not solely be used to make significant decisions concerning individuals.

4.5. Respect for Intellectual Property Rights and Responsibility

The development, use, and deployment of AI technologies requires special attention to, and responsibility for, managing intellectual property rights (known as "IPR" being the legal rights protecting creations of the mind, including copyrights, patents, trademarks, and trade secrets). **Employees, contractors, and partners must ensure that all use of TUI and third-party AI tools, whether for generating, modifying, or analysing content is conducted in a manner that respects TUI's and any third party's IPR.** It is important to keep in mind that AI generated material (images, video, codes, data models and text) may replicate and incorporate IPR.

Users are responsible for verifying that any data or material used in conjunction with AI tools is lawfully obtained and does not infringe third-party rights, such as copyright, trademarks, patents, or trade secrets (e.g., training models on copyrighted material without permission). If AI generated content is supplied by a third party the supplier's contract terms should contain relevant indemnification for potential intellectual property rights infringement by AI generated output or provisions that allow for self-reporting by the AI itself of its outputs to flag for potential intellectual property rights infringement.

Any content generated by AI tools for publication or commercialisation must be carefully considered for IPR ownership, license terms and legal compliance before use. TUI retains ownership of any AI-assisted work produced in the course of employment or contractual duties. If you have any questions please contact ip@tui.com

Third-party suppliers must not be allowed to train their AI systems on TUI datasets that contain copyrighted, confidential, or proprietary information without appropriate agreed written licence terms and restrictions in place. For any licence queries please email techlaw@tui.com

Where applicable, authorship or contribution of human creators must be distinguished from AI-generated elements. Appropriate IP labels (for example copyright) should be used for human generated and AI generated material. If you have any questions please contact ip@tui.com

AI applications must not be used for any anti-competitive activity. For example, AI applications must not be used for practices such as information or pricing collusion between competitors or for abusing a dominant market position by leveraging power or pricing to exclude competition.

4.6. Safety, Security and Robustness

AI systems must be actively protected against adversarial attacks to minimise security risks and maintain confidence in system outcomes.

All AI systems, applications or services must meet the requirements stipulated in the document '*Information Security Standard: Secure use of AI*' which can be found at Secure Use of AI. This standard incorporates the requirement to carry out a risk assessment prior to production 'go-live', when significant changes occur to the system, application or service and at a regular interval. This is to enable any significant

information security risks identified to follow an appropriate risk treatment plan. For any IT security questions please contact the Head of Information Security Governance, Risk and Compliance.

The Group Manual – IT Security states a range of controls that must be in place for IT systems, these controls also apply to AI systems and can be found at Group Manual IT Security.

Contracts with third-party organisations providing AI systems, applications or services to TUI should incorporate the standard Information Security Schedule which sets out the minimum requirements TUI expects of IT suppliers.

5. Responsibilities

5.1. Responsibility for content

The *Chief Information Officer* is responsible for the content of this Group Policy ("**Group Policy Owner**"). Questions and/or comments relating to its content shall be addressed to the Group Policy Owner.

5.2. Responsibility for local implementation

The management of each Managed Group Company is responsible for the effective local implementation of this Group Policy within three months after a respective request by Group Policy Management. This includes usually at least (i) a review of compliance with local law in areas of application outside of Germany, (ii) a formal decision of the management to enact the Group Policy for the respective Managed Group Company, (iii) a transformation of the requirements and processes of the Group Policy in the local organisation, and (iv) an adequate communication within the local organisation.

The management informs Group Policy Management if the Group Policy needs to be changed locally due to mandatory law and/or if the local implementation takes more than three months.

In the case of Non-Managed Group Companies, the respective management decides whether this Group Policy shall be implemented.

This Group Policy is directly applicable to TUI AG.

Record of revisions

Version	As of	Changes/comments