ENERGO-PRO Group

Policy on the Use of Artificial Intelligence

2025

ENERGO-PRO

Policy on the Use of Artificial Intelligence

Version: 1.0 | **Effective from:** 1 October 2025 | **Owner:** AI Governance Committee (AIGC)

1. Objective and Scope

1.1. This Policy on the Use of Artificial Intelligence (the "**Policy**") establishes the binding rules for the secure, effective, and responsible use of Artificial Intelligence (the "**AI**") tools within ENERGO – PRO a.s. (the "**Company**") and its affiliates (collectively, the "**Group**"). For the purposes of this Policy, the Group comprises DK Holding Investments, s.r.o., the sole shareholder of the Company, and all of its direct and indirect subsidiaries.

1.2. Our objective is to support innovation and productivity through the adoption of modern technologies while ensuring the highest level of protection for our data, intellectual property, customers, and reputation. Our adoption of AI must be guided not only by innovation but by a firm commitment to operational security, public safety, and the trust placed in us by society.

1.3. We are committed to ensuring that all use of AI aligns with our core ethical principles of integrity, respect, transparency, and ethical conduct. Crucially, human oversight and responsibility shall remain paramount in all our AI-driven processes.

1.4. This Policy applies to all employees, external contractors, consultants, and suppliers who access the Group's information systems or process Group data (collectively, the "**Personnel**"). It applies to all AI Systems used within the Group, regardless of whether they were developed internally, procured from third parties, or accessed as a public service.

2. Definitions

For the purposes of this Policy, the following definitions shall apply:

2.1. **AI System:** An AI system as defined by Article 3(1) of the AI Act (as defined below). Any 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. This definition applies regardless of whether the AI System is a standalone application or an integrated feature within a larger software suite.

Enterprise AI: An approved AI System governed by a contractual agreement (including a Data Processing Addendum as defined below) that guarantees the protection of our data. Such agreements must explicitly prohibit the vendor from using Group data for training its own or any third-party models.

Examples: Microsoft Copilot for M365, DeepL Pro.

Public AI: An approved AI System, typically available on the public internet that offers no contractual guarantees for data protection and may use inputs (Prompts) and outputs (Response) to train or improve its own or third-party models.

Examples: Standard versions of ChatGPT, Google Gemini, Google Translate.

2.2. **Data Classification:** All data is classified into four levels:

Public (Level 1): Any information that is lawfully in the public domain. This includes both information officially published by the Group and information from external public sources.

Examples: Published press releases, academic papers, news articles, public government databases, information on publicly accessible websites.

Internal (Level 2): Non-public information where unauthorised disclosure would present a low risk.

Examples: General team meeting minutes (not containing personal data or trade secrets), internal guides, non-sensitive project drafts.

Confidential (Level 3): Sensitive data, the disclosure of which could cause moderate to severe harm to the Group, its partners, or customers.

Examples: Financial plans, business strategies, unaudited financial results, anonymised contracts.

Strictly Confidential (Level 4): The most sensitive data, protected by law or contract, where unauthorised disclosure could lead to severe legal, financial, or reputational damage.

Examples: Personal data as defined by the GDPR (as defined below) (e.g., employee or customer records), trade secrets, price sensitive information, information protected by a Non-Disclosure Agreement (NDA), know-how, system logins and passwords, proprietary source code, operational data from critical infrastructure (e.g., SCADA systems), detailed grid vulnerability assessments, or schematics of power generation units.

2.3. **Data Processing Addendum (DPA):** A legally binding contract entered into between a data controller and a data processor, pursuant to Article 28 of GDPR. It governs the processing of personal data by the processor on behalf of the controller. It is a mandatory requirement under GDPR whenever a controller engages a processor to handle personal data.

2.4. **Deepfake:** Any AI-generated or AI-manipulated video, audio or image content that resembles existing persons, objects, places, subjects or events and could falsely appear to a reasonable person as authentic or truthful.

2.5. **Hallucination:** A phenomenon in which an AI model generates outputs that are nonsensical, factually incorrect, or entirely fabricated, despite being presented with confidence and fluency.

2.6. **Prompt:** Any input, such as a question, instruction, or data set, provided by a user to an AI System to elicit an output.

3. Roles, Responsibilities, and Governance

AI Governance Committee (AIGC): A cross-functional team comprising representatives from senior management, Legal, HR, and other key departments. It approves the AI strategy, this Policy, and is responsible for maintaining the Register.

AI Navigator: The primary point of contact for guidance and support on AI-related matters. This role provides proactive advice, supports the AIGC, and assists Personnel with AI-related queries.

AI System Owner: Unless the AI Governance Committee (AIGC) determines otherwise, the AI Navigator shall act as the AI System Owner for each approved AI System. The AI System Owner is responsible for:

1. ensuring the AI System is used solely for its approved purpose and within its authorised parameters;
2. serving as the primary business contact for audits and performance reviews;
3. managing user access in coordination with IT; and
4. reporting any significant performance issues or incidents to the AI Navigator for escalation to the AIGC.

Personnel: Every member of Personnel is responsible for understanding and complying with this Policy.

4. Core Principles of AI Usage

All use of AI within the Group shall comply with the following key principles:

4.1. **Human-in-the-Loop (Mandatory Human Oversight):** AI is a supportive tool, not an autonomous decision-maker. An AI System can assist and support human capabilities, but it does not replace human judgement and accountability. All AI-generated outputs, especially those with potential legal or financial consequences, must be critically reviewed, verified, and approved by a qualified and responsible person before use. The level of scrutiny must be proportionate to the risk of the decision (e.g., verifying a single fact in a report requires less scrutiny than approving an AI-generated network maintenance schedule).

4.2. **Accountability:** The ultimate responsibility for any decision or action based on AI-generated output rests with the person who uses it, not the AI System itself. Personnel must remain vigilant to the possibility that an AI System may produce "hallucinations" and must always verify critical information from an independent and reliable source.

4.3. **Transparency:** Where an AI system is designed to interact directly with natural persons (for instance, via a chatbot), those persons shall be informed that they are interacting with an AI system. Personnel who generate or manipulate image, audio, or video content that purports to be authentic (ranging from AI-generated illustrations for marketing materials to Deepfakes) shall clearly and conspicuously disclose that the content has been artificially generated or manipulated, as further detailed in Section 6.3(iii).

4.4. **Non-Discrimination and Fairness:** AI Systems shall be used in a way that avoids creating or reinforcing unfair bias or discrimination against individuals or groups based on protected characteristics (e.g., age, gender, ethnicity).

4.5. **Security and Privacy by Design:** Data protection and security are fundamental. All AI projects, from procurement to deployment and eventual decommissioning, must integrate privacy and security principles from the outset.

5. Governing Legislation and Policies

5.1. Legal and Regulatory Framework

5.2. The Group's development, procurement, and use of AI Systems are governed by a framework of applicable laws and international standards. All Personnel are required to comply with the latest versions of the following, without limitation:

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (the "**AI Act**").

Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data (the "**Data Act**").

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (the "**NIS 2 Directive**").

Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market (the "**Copyright Directive**").

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the "**GDPR**").

ISO/IEC 42001:2023 – Information technology — Artificial intelligence — Management system.

All applicable national legislation in the jurisdictions where the Group operates, including but not limited to acts governing labour law, intellectual property, and civil liability.

5.3. **Relationship with Other Internal Policies**

5.4. This Policy complements and must be read in conjunction with other binding Group policies. Personnel are also required to ensure their use of AI Systems also complies with all other relevant internal policies, including, but not limited to:

- The Code of Conduct
- Human Rights Policy
- Human Resources Policy
- Security Policy
- Data Protection Policies (Internal and External)
- Contractor and Subcontractor Management Plan

5.5. In the event of any conflict between this Policy and another internal policy, the more restrictive provision shall apply. The matter should be promptly referred to the AI Navigator for clarification by the AIGC.

6. Acceptable and Prohibited Use

6.1. **The Golden Rule: Match Data to the Appropriate AI System.**

The most critical principle is to ensure that data is only processed by an AI System with a corresponding level of security. A failure to comply with this principle constitutes a serious breach of this Policy.

Data Classification	Public AI	Enterprise AI
Level 1: Public	Permitted	Permitted
Level 2: Internal	Permitted	Permitted
Level 3: Confidential	Permitted with restrictions	Permitted
Level 4: Strictly Confidential	Prohibited	Permitted only with AIGC approval, subject to a mandatory DPIA and IT Security Risk Assessment.

6.2. **Approved AI Systems**

General Rule

Personnel are permitted to use only those AI Systems listed on the official "Register of Approved AI Systems" (the "**Register**"). The use of any AI System not listed in the Register is strictly prohibited.

A list of AI Systems approved as of the effective date of this Policy is attached for reference purposes as Appendix A. The authoritative, live version of the Register is maintained and regularly updated by the AIGC and is available on the Group's M365 SharePoint.

Use of Minimal Risk AI Systems

Notwithstanding the preceding clause, Personnel are permitted to use an AI System not listed in the Register, provided that such a system qualifies as a "Minimal Risk AI System" pursuant to the classification in Section 8 of this Policy. The person who intends to use the system shall be solely responsible for its proper assessment and classification as a Minimal Risk AI System.

A person who makes use of this exception shall notify the AI Navigator of the use of such an AI System without undue delay by email. The use of any such system must, at all times, be in full compliance with this Policy and all other Group policies, including but not limited to those concerning data protection (GDPR), information security, and IT security.

Use of Public AI Systems for Level 3 (Confidential) Data

The processing of Level 3 (Confidential) Data using Public AI Systems is strictly prohibited, except where all of the following conditions are met:

(i) The Public AI System used must be approved for this purpose in the Register and used in accordance with the conditions specified therein. As of the latest revision of this Policy, the required methods are:

- **For Adobe Acrobat AI Assistant:** Approved for use without requiring additional privacy settings. Its privacy-by-design architecture ensures user data is isolated and is not used for model training.
- **For ChatGPT:** The 'Temporary Chat' feature must be used.
- **For Google Gemini:** The 'Gemini Apps Activity' setting must be turned off.
- **For NotebookLM:** Approved for use without requiring additional privacy settings. Its privacy-by-design architecture ensures user data is isolated and is not used for model training.

(ii) The Public AI System's terms of use guarantee that user inputs (prompts) and system outputs (responses) shall not be used for the purposes of training or improving the provider's or third-party AI models.

(iii) All inputs and outputs from the session shall not be retained in the user's permanent conversation history and must be subject to automatic deletion by the provider. Users must acknowledge the provider's retention period for security and operational purposes, which is currently:

- Up to 30 days for ChatGPT 'Temporary Chat'.
- Up to 72 hours (3 days) for Google Gemini with 'Activity' turned off.

It is the user's responsibility to select the correct feature and understand the applicable data retention period prior to submitting any Level 3 (Confidential) Data into the Public AI System.

6.3. **Prohibited Activities**

The use of AI for the following purposes is strictly prohibited:

(i) Any activity that contravenes applicable law, particularly the prohibited practices defined in Article 5 of the AI Act, or violates the Group's Code of Conduct or any other applicable internal policy.

(ii) Inputting any Level 4 Data into any Public AI System or inputting any Level 3 Data into any Public AI System without complying with the restrictions set out in Section 6.2.

(iii) The creation or dissemination of Deepfakes and other AI-generated synthetic media for a malicious, fraudulent or deceptive purpose—or in any manner intended, or reasonably likely, to mislead any person into believing the content is authentic—is prohibited.

The creation and use of AI-generated or AI-manipulated images, audio, video or comparable outputs is otherwise permitted for legitimate illustrative, educational, design, training or other business purposes, provided that:

a. the content is clearly disclosed to the intended audience as AI-generated / AI-manipulated (for example by an on-asset label, caption, watermark, metadata notice, slide footnote or other accompanying information visible at the point of use); and

b. the content is not presented as a factual record of real-world persons, objects, places, subjects or events.

(iv) The creation and use of realistic human-like avatars for the purpose of impersonating or deceptively interacting with employees, customers, or the public.

(v) Making final, automated decisions about individuals (e.g., in recruitment, performance reviews, or termination) without meaningful human oversight and review.

(vi) Any attempt to circumvent the security measures or usage limitations of an approved AI System.

6.4. **Encouraged Activities**

We welcome and encourage the use of approved AI Systems. The following list is illustrative, not exhaustive, providing examples of beneficial applications:

(i) Assisting with the drafting of e-mails, reports, or presentations.

(ii) Translating documents (subject to data classification rules).

(iii) Summarising documents and analysing data to identify new insights.

(iv) Brainstorming and creating conceptual drafts.

(v) Automating repetitive tasks (e.g., generating spreadsheet formulas).

(vi) Initial drafting of technical reports on energy market trends based on public data, with all facts and figures subsequently verified by a subject-matter expert.

For any potential use case not specified above, Personnel must exercise due caution and ensure the proposed use fully complies with the core principles of this Policy and all other applicable legal and internal regulations. Sound professional judgement must be exercised at all times. If there is any uncertainty regarding the permissibility or compliance of a proposed use, consultation with the AI Navigator is mandatory before proceeding.

7. Procurement and Approval of AI Systems

7.1. Every new AI System must undergo the following approval process before it can be used:

(i) **Request Submission:** A person shall submit a request using the official form (see Appendix B).

(ii) **Initial Assessment:** The AI Navigator shall review the request against basic criteria.

(iii) **Risk Assessment:** The AIGC shall conduct a detailed risk assessment (see Section 8).

(iv) **Decision:** The AIGC shall approve, reject, or approve the AI System with specified limitations.

(v) **Registration:** The approved AI System shall be recorded in the Register.

8. Risk Assessment and System Classification

8.1. Each AI System shall be classified according to the four-tier risk model of the AI Act:

Unacceptable Risk: AI Systems that are prohibited by law and this Policy (e.g., social scoring).

High Risk: An AI System that meets the criteria set out in Article 6 of the AI Act, including but not limited to AI Systems that could significantly affect the health, safety, or fundamental rights

of individuals (e.g., an AI System used in the management of critical infrastructure, or an AI System used for filtering job applications). Such systems are subject to stricter rules, including mandatory registration, rigorous testing, and continuous monitoring.

Limited Risk: This category covers AI Systems that pose specific risks of manipulation or deception and are therefore subject to specific transparency obligations. These obligations vary based on the type of AI System and its use:

- **Direct Interaction Systems (e.g., Chatbots):** When using systems designed for direct interaction with individuals, such as chatbots for internal HR support or external customer service, users must be clearly informed that they are communicating with an AI.
- **Synthetic Media (Images, Audio, Video):** AI Systems used to generate or manipulate realistic images, audio, or video content (e.g., Deepfakes) must have their outputs clearly labelled as "AI-generated" or "artificially manipulated," unless the content is obviously artistic or creative and not intended to represent reality.
- **General-Purpose AI (GPAI) for Text Generation:** The underlying models of tools like ChatGPT, Gemini, and Copilot are considered General-Purpose AI (GPAI) and are subject to transparency requirements from their providers. For our purposes as users (deployers), when these tools are used for assistive functions such as summarising text, drafting e-mails, or brainstorming, the generated text does not need to be labelled as AI-generated, provided that it is subject to meaningful human review and editorial control before use. In these cases, the AI functions as an assistant, and the final responsibility for the content rests entirely with the Personnel.

Minimal Risk: This category applies to AI Systems that present a negligible risk to the rights, freedoms, or safety of individuals. A system shall be classified as Minimal Risk only if it meets all of the following conditions:

- It does not make decisions or determinations that affect the legal rights of natural persons;
- It does not process sensitive personal data; and
- Its potential failure or erroneous output would have no material safety impact.

An AI System may be reclassified into a higher risk category (Limited or High Risk) if its intended purpose is modified to include the processing of personal, biometric, or safety-critical data. Although not specifically regulated by the AI Act, the use of any Minimal Risk AI System must adhere to the general principles set out in this Policy.

Examples of Minimal Risk AI Systems: AI-powered spam filters, Weather-forecasting models, Inventory management systems using simple AI for demand forecasting, Grammar- and spell-checking assistants embedded in word-processing or email clients, Machine-translation tools (e.g. website auto-translate) used for quick comprehension (translating publicly available text poses negligible risk only when no sensitive data are involved)

9. Data Protection, Intellectual Property, and Security

Privacy by Design: The principle of data protection by design and by default shall be integrated into every AI project from the outset.

DPIA: A Data Protection Impact Assessment (see Appendix C) is mandatory for any AI system that is likely to result in a high risk to the rights and freedoms of natural persons.

Intellectual Property of AI-Generated Content: Personnel must be aware that the legal status of AI-generated content is complex and evolving. Unless explicitly stated otherwise in the terms of an approved AI System, outputs generated by AI may not be subject to copyright protection or may be subject to third-party rights. All content created using AI in the course of employment is considered the work product of the Group, but Personnel should not assume the Group holds exclusive copyright. The use of AI-generated content in public-facing materials or commercial products requires prior consultation with the AI Navigator.

Protection of Confidential Information and Intellectual Property: Personnel must exercise extreme caution to protect the Group's sensitive information. This includes, but is not limited to, trade secrets, price sensitive information, know-how, information protected by NDAs, copyrights, and industrial property rights. As stipulated in Section 6, such information must never be input into a Public AI System.

Security: All AI Systems must comply with our established cybersecurity standards.

10. Monitoring, Reporting, and Metrics

We shall monitor the performance, accuracy, and security of our AI Systems.

For High Risk AI Systems, regular performance reports to the AIGC are mandatory.

We shall measure not only technical parameters but also the business value generated (e.g., time saved, process improvements).

11. Incident Response and Change Management

Incidents: Any incident involving an AI System (e.g., a data breach, an erroneous output with significant impact, a suspected case of discrimination) must be reported immediately to the AI Navigator.

Changes: Any significant change to an AI System (e.g., a new version, a change in its intended use) requires a new risk assessment by the AIGC. A significant change includes, but is not limited to: a change in the system's intended purpose, the deployment of a new major version of its underlying model, or a substantial alteration of its data inputs or outputs.

12. Personnel Training and AI Literacy

Mandatory Training: All Personnel are required to undergo initial training on the use of AI, covering this Policy, data security, risk awareness (including discrimination and hallucinations), and the proper use of approved AI Systems. Additional training will be conducted on an as-needed basis, for instance, following significant updates to legal regulations or our AI Systems.

Advanced Training: Provided to Personnel who work intensively with AI, focusing on effective prompting and advanced features of approved AI Systems.

AI Portal: An internal SharePoint site serving as the central resource hub for all AI-related matters. It contains the Register, user guides, training materials, policy documents, and contact information.

13. Third-Party and Vendor Management

Prior to the procurement of any Enterprise AI System, the vendor shall be subject to a thorough due diligence process. This assessment shall evaluate the vendor's security posture, compliance certifications, reputation, and transparency regarding its AI models.

Non-negotiable Requirement: We must have a signed Data Processing Addendum (DPA) with any vendor whose AI System will process our non-public data (Levels 2-4). This DPA must prohibit the vendor from using our data to train its models.

14. Policy Review and Audit

This Policy is a living document. The AIGC shall review and update it at least annually, or more frequently in response to significant technological or legislative changes. Internal Audit shall periodically verify compliance with this Policy.

15. Sanctions for Non-Compliance

A breach of this Policy shall be considered a serious breach of employment duties and may be subject to disciplinary action in accordance with internal regulations and applicable law, up to and including termination of employment or contract.

16. Appendices (Available on the AI Portal)

- **Appendix A:** Register of Approved AI Systems
- **Appendix B:** Request Form for the Approval of a New AI System
- **Appendix C:** Template for a Data Protection Impact Assessment (DPIA)
- **Appendix D:** Contact Details

Appendix A: Register of Approved AI Systems

Last Updated: 1 October 2025 | **Maintained by:** AI Navigator

This register provides a definitive list of AI Systems that have been assessed and approved for use within the Group. Any AI System not present on this list is considered prohibited unless explicit approval has been granted by the AI Governance Committee (AIGC).

AI System Name	Category	Risk Classification	Examples of Approved Use Cases	Max. Data Classification Permitted	Status
Adobe Acrobat AI Assistant	Public AI	Limited Risk	AI Assistant quickly analyses your documents to extract key insights, identify patterns, and answer complex questions, with all responses directly linked to sources within the text.	Level 3 (Confidential) with restrictions	**Approved**
Celsia AI Assistant	Enterprise AI	Limited Risk	Filtering relevant information from internal Group documents, producing concise summaries, and answering ESG-related questions.	Level 4 (Strictly Confidential)	**Approved**
ChatGPT (Free/Plus versions)	Public AI	Limited Risk	Drafting emails, summarizing documents, brainstorming ideas, or translating text.	Level 3 (Confidential) with restrictions	**Approved**
DeepL Pro	Enterprise AI	Limited Risk	Translation of documents, including those containing Strictly Confidential.	Level 4 (Strictly Confidential)	**Approved**
Google Gemini	Public AI	Limited Risk	Drafting emails, summarizing documents, brainstorming ideas, or translating text.	Level 3 (Confidential) with restrictions	**Approved**
Google Translate	Public AI	Limited Risk	Translation of non-sensitive, public information only.	Level 2 (Internal)	**Approved**

Microsoft Copilot for M365	Enterprise AI	Limited Risk	Drafting emails, summarising documents and meetings, data analysis within Microsoft 365 applications.	Level 4 (Strictly Confidential)	**Approved**
NotebookLM	Public AI	Limited Risk	Transform specific project documents, research, and meeting notes into an interactive expert you can query for summaries, factual answers, and new insights grounded only in your private sources.	Level 3 (Confidential)	**Approved**

Appendix B: Request Form for the Approval of a New AI System

Please complete this form in its entirety and submit it to the AI Navigator for any new AI System you wish to use for Group purposes.

Section 1: Requester Information

- **Full Name:**
- **Department:**
- **Job Title:**
- **Date of Request:**

Section 2: AI System Details

- **Name of AI System:**
- **Vendor/Provider:**
- **Link to System's Website:**
- **Link to Privacy Policy / Terms of Service:**

Section 3: Intended Use

- **Business Purpose:** (Please describe the business problem you are trying to solve and how this AI System will help. What is the primary objective?)
- **Specific Tasks:** (List the specific tasks you intend to perform with this AI System, e.g., "Translate legal contracts," "Generate marketing copy," "Analyse customer feedback.")

Section 4: Data Usage

- **What is the highest level of data classification you intend to process with this AI System?** (Refer to Section 2.2 of the AI Policy)
    - [ ] Level 1: Public
    - [ ] Level 2: Internal
    - [ ] Level 3: Confidential
    - [ ] Level 4: Strictly Confidential
- **Will the AI System process any Personal Data as defined by the GDPR?**
    - [ ] Yes

- [ ] No

- **Will the AI System be used to make decisions that have a significant effect on individuals (e.g., recruitment, performance evaluation)?**
  - [ ] Yes
  - [ ] No

Section 5: Initial Risk Assessment

- **Does the vendor provide a Data Processing Addendum (DPA) that explicitly prohibits the use of our data for their or any third-party model training?**
  - [ ] Yes
  - [ ] No
  - [ ] I do not know
- **To your knowledge, are there any known security vulnerabilities or ethical concerns associated with this AI System?** (Please provide details if yes.)

For Internal Use by AIGC Only

- **Request ID:**
- **Date Received:**
- **AI Navigator Assessment:** Complete / Incomplete
- **AIGC Decision:** Approved / Rejected / Approved with Limitations
- **Date of Decision:**
- **Justification / Limitations:**

Appendix C: Template for a Data Protection Impact Assessment (DPIA) for an AI System

This template must be completed for any AI System classified as **High Risk** or any AI System processing **Level 4 (Strictly Confidential)** data, particularly where personal data is processed on a large scale or the processing is likely to result in a high risk to the rights and freedoms of natural persons.

DPIA Reference: [Unique ID]

AI System Name: [Name of the AI System]

AI System Owner: [Name]

Date of Assessment: [Date]

Part 1: Description of the Processing

- **Nature and Scope of Processing:** Describe the AI System's functionality, the nature of the data it will process, the volume of data, and the categories of data subjects involved.
- **Purpose of Processing:** What are the intended outcomes and benefits for the Group, customers, or employees?
- **Context of Processing:** Describe the relationship with data subjects and their reasonable expectations. Detail the sources of data and any data flows to third parties.

Part 2: Assessment of Necessity and Proportionality

- **Lawful Basis:** What is the lawful basis for processing personal data under GDPR Article 6?
- **Purpose Limitation:** Are the data processed strictly for the specified, explicit, and legitimate purposes?
- **Data Minimisation:** Is the data being processed adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed?

Part 3: Risk Assessment

- **Risks to the Rights and Freedoms of Data Subjects:** Identify potential risks, such as:
    - Unauthorised access or data breach.
    - Inaccurate outputs leading to incorrect decisions.
    - Discriminatory bias in outputs (e.g., in recruitment or credit scoring).
    - Lack of transparency or explainability in AI-driven decisions.
    - Re-identification of anonymised or pseudonymised data.

- **Likelihood and Severity:** For each identified risk, assess its likelihood (Low/Medium/High) and potential severity of impact.

Part 4: Measures Envisaged to Mitigate Risks

- **Technical Measures:** Describe the security controls in place (e.g., encryption, access controls, pseudonymisation).
- **Organisational Measures:** Describe the procedural controls (e.g., human oversight, regular audits, staff training, vendor DPA).
- **Bias Mitigation:** Describe the steps taken to test for and mitigate algorithmic bias.
- **Transparency Measures:** How will data subjects be informed about the use of the AI System and their rights?

Part 5: Consultation and Approval

- **Consultation with DPO:** Record the advice provided by the Data Protection Officer.
- **AIGC Decision:**
    - [ ] Proceed with processing.
    - [ ] Proceed with processing subject to the implementation of additional measures.
    - [ ] Do not proceed with processing.
    - [ ] Consult with the Supervisory Authority.

Sign-off:

- **AI System Owner:** _____
- **Data Protection Officer:** _____
- **AIGC Chair:** _____

Appendix D: Contact Details

For any enquiries regarding this Policy or the use of AI within the Group, please contact the relevant individuals.

Primary Point of Contact

- **AI Navigator**
  - **Name:** Tomáš Brandejský
  - **Email:** t.brandejsky@energo-pro.com
  - **Responsibilities:** First-line support for Personnel, coordinating training, and managing the AI System approval process.

Governance and Escalation

- **AI Governance Committee (AIGC)**
  - **Chairperson:** Jakub Fajfr
  - **General Counsel:** Christian Blatchford
  - **Data Protection Officer (DPO):** Marina Radeva
  - **Head of HR:** Nikola Šugra
  - **Email:** AIGC@energo-pro.com
  - **Responsibilities:** Strategic oversight, approving and regularly updating the Register of Approved AI Systems, AI Policy approval, risk management, and final approval for High Risk AI Systems.