European Parliament

AI Governance Board

Artificial Intelligence in the European Parliament – A foundational Roadmap

EN

PE 783.191/BUR/GT
PE 784.993/BUR/ANN.2

Table of Contents

I. Introduction

Artificial Intelligence (AI) is shaping the way societies work, communicate and take decisions. For the Parliament, AI holds great potential to support Members in exercising their mandate and the administration in delivering services in an innovative and efficient way. AI also offers an opportunity to further strengthen representative democracy by providing new ways and enhancing Parliament's connection with the citizens.

At the same time, AI presents challenges that require careful consideration and management, ranging from ethics, treatment of confidential data and privacy concerns to organisational and environmental impacts. Depending on its development, AI may cause harm to public interests and fundamental rights. It is therefore key that AI is conceived and used fully in line with Union values, and on the basis of thorough risk assessments.

In this context, the AI Act[1] provides the overarching regulatory framework for the responsible deployment of AI in the EU. As the world's first regulation on the matter, the act defines clear requirements for transparency, accountability and human oversight, particularly for high-risk applications.

The AI Act entered into force on 1 August 2024. Some chapters started applying from 2 February and 2 August 2025, respectively. The Regulation will apply in its entirety as from 2 August 2026[2]. It is thus essential that prior to this date Parliament has put in place all necessary foundational measures and mechanisms to comply with the Act.

Data governance and cybersecurity constitute two other regulatory fields that are crucial for the implementation of AI in the Parliament. Both should therefore be duly taken into account in risk assessments on AI tools.

Data is a strategic asset for AI. It should be managed in line with the FAIR principles (findable, accessible, interoperable and reusable) while maintaining the highest standards of confidentiality and personal data protection. AI can contribute to enhancing Parliament cyber-resilience, a potential that should be further explored.

[1] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence

[2] Article 6(1) and the corresponding obligations in the Regulation will apply from 2 August 2027.

II. Framework for the development and use of AI in the Parliament

In March 2024, the Bureau adopted a framework to enable Parliament to develop AI capabilities in a sustainable and ethically responsible manner, encompassing principles, objectives, and governance arrangements.

- **Principles**

The Bureau highlighted the importance of a human centric approach and strong user engagement and established that AI development in Parliament should be guided by the following principles:

- ethical and lawful AI;
- safe and robust AI;
- secure and privacy-compliant AI;
- transparent and explainable AI.

- **Objectives**

The Bureau defined four strategic orientations for AI solutions:

- supporting Members in fulfilling their mandate;
- supporting innovation efforts by the administration and improving efficiency of processes, with a focus on core business and outreach to citizens;
- building a robust competence and governance framework;
- ensuring compliance and control mechanisms to mitigate inherent and residual risks.

- **Governance**

Parliament's AI governance as set by the Bureau aims at ensuring consistency in the development and use of AI across the Institution, with accountability and transparency. The governance should also ensure that risks specific to AI are managed effectively.

In terms of structures, Parliament's AI governance provides for an AI Governance Board, chaired by the Secretary-General and with the participation of all Directors-General. The Governance Board provides direction and takes *inter alia* decisions on sensitive use cases. It is supported by an Inter-DG Steering Group, which coordinates initiatives across services, and by the AI Centre of Competence, which acts as the hub of expertise. For the operationalisation of the overall AI framework, the Bureau requested the development of an AI Roadmap to be approved by the Governance Board.

Following the decision of the Bureau, the governance framework was swiftly implemented by the Secretary-General. Its structures have become operational as from the start of the current legislative term. In the course of 2025, the bodies focussed on the definition of the Roadmap. This has involved carrying technical assessments, proofs of concept and user consultations.

III. AI Roadmap

In line with the principles and objectives set by the Bureau in March 2024, the Roadmap outlined hereunder aims at ensuring that Parliament has all foundational capabilities to implement and use AI solutions. The Roadmap will be implemented by Parliament responsible services under the oversight of the Governance Board. Parliament Vice-Presidents responsible for AI will accompany the implementation of the Roadmap and the Bureau Working Group on Digital Transformation, Cybersecurity and Information Security will be kept informed, thus linking the political and administrative levels.

Given comparable opportunities AI brings and challenges it poses across all EU institutions, the implementation of the actions defined under the four workstreams of the Roadmap will benefit from ongoing cooperation with other EU institutions and bodies. This concerns in particular the development of ethical guidelines, definition of the infrastructure, legal compliance artefacts and model evaluation.

The Roadmap is structured along four workstreams, each providing for three actions (see table below). Each action includes one or more deliverables. The deliverables will be implemented in their initial iteration by July 2026 and will be continuously updated and enhanced.

Workstreams	**Actions**
Policies	Establishing an AI compliance framework
	Defining data governance policy supporting AI
	Implementing risk prevention and handling mechanisms
Infrastructure	Defining the AI reference infrastructure
	Establishing foundational infrastructure for AI
	Implementing machine learning and model operations
Skills	Developing an AI literacy programme
	Carrying out regular awareness campaigns
	Leveraging the EP AI portal as primary information point on AI
Application	Establishing an AI use case methodology
	Carrying out systematic and regular testing of AI solutions
	Measuring AI deployment and maturity

Workstream I - Policies

AI deployment must always comply with the relevant legal requirements, including the AI Act, data protection rules, information security and cybersecurity requirements, as well as environmental and copyright legislation. AI systems must embody transparency, accountability, fairness, privacy and accessibility, and their outputs must remain under the control of Members and staff. Strong ethical adherence by all actors involved is thus of paramount importance.

Against the above background, this workstream focuses on ensuring that the necessary policies are in place to guarantee the highest standards of regulatory compliance, data treatment and risk handling. The workstream provides for the following three actions:

- Action 1: Establishing an AI compliance framework;
- Action 2: Defining data governance policy supporting AI;
- Action 3: Implementing risk prevention and handling mechanisms.

- ***Action 1 - Establishing an AI compliance framework***

Since entering into force on 1 August 2024, the AI Act's provisions have followed a phased application calendar, with Article 5 on prohibited practices applicable as of 2 February 2025. To meet this requirement, Parliament responsible services have developed a compliance questionnaire and conducted an initial survey to identify any potentially prohibited AI practices. The questionnaire will be regularly updated and include any newly developed or acquired AI system.

The AI Act *compliance framework* should be further developed to address the evolving responsibilities of both AI system deployers and providers in line with the phased application of the AI Act. This framework will be integrated into both technological development and software procurement processes, including software selection or Software as a Service (SaaS) acquisition procedures.

Ethical guidelines for AI are being prepared, aligned with the High-Level Expert Group on AI's *Ethics Guidelines for Trustworthy AI*[3]. The guidelines will ensure that all AI use within Parliament is guided by the principles of human autonomy, prevention of harm, fairness and explicability and that AI systems are designed according to the following seven requirements: (i) human agency and oversight, (ii) technical robustness and safety, (iii) privacy and data governance, (iv) transparency, (v) diversity, non-discrimination and fairness, (vi) societal and environmental well-being, (vii) accountability.

A "Responsible AI Toolkit" is in preparation. It will contain guidelines, tools and frameworks that will help users develop and deploy AI responsibly. The toolkit will address bias identification, data privacy and compliance with changing regulations.

[3] https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

Deliverables

- AI system definition questionnaire
- Prohibited practices questionnaire
- AI Act compliance assessment list for providers
- AI Act compliance assessment list for deployers
- Ethical guidelines
- Model Lifecycle Documentation templates
- AI Model Cards template

- ***Action 2 - Defining data governance policy supporting AI***

Parliament's data landscape is characterised by significant fragmentation. IT systems and applications each maintain their own data pools, leading to isolated data silos that hinder efficient access, understanding and reuse of information.

To achieve better data management, Parliament has adopted a data governance framework. It aims at ensuring that data is easy to find, access, and understand, allowing for straightforward reuse across the Parliament. For personal data, this reuse is strictly conditional on the principles of lawful processing and purpose limitation.

As a next step, data policy should be developed, including operational rules, best practices, methodologies and procedures for ensuring and maintaining the appropriate level of data management. One of the key objectives of such a policy framework is to provide high quality of data to be used for AI tools.

An additional initiative is the ongoing set-up of Parliament data platform. It aims at designing and building a set of capabilities and services for corporate-level data production, integration and utilisation. It will support two key objectives: (i) sound data management by maximising the value of data assets, and (ii) support data-driven decision-making and digital services, including AI, by providing high-quality, accessible and semantified data for analytics, reporting and AI-based applications.

Next to using existing data management practices, building AI-ready data will require leveraging data engineering and data management. These must expand to include new techniques to address emerging AI use cases and AI techniques, in particular data labelling and annotation, feature engineering, prompt engineering and privacy enhancing technologies (PETs).

Deliverables

- General AI data policies
- AI data quality framework
- Data drift detection alerts (automated notifications and logs)

- ***Action 3 - Implementing risk prevention and handling mechanisms***

A comprehensive risk prevention and handling framework is necessary to apply AI in Parliament in a way which is compliant with the AI Act while ensuring additional risk mitigation mechanisms. This framework will elaborate on and complement the risk categories as defined in the AI Act, while supporting Parliament to prioritise the most significant risks that may arise when AI is used in the Institution. The framework will cover specific legal and broader ethical concerns.

In terms of data protection risks, the framework will focus on potential violations of Regulation (EU) 2018/1725. These include unlawful or non-transparent processing of personal data, infringement of data subjects' rights, lack of appropriate safeguards. With reference to ethical concerns, the framework will address issues such as model profiling and model bias, and automated decision-making.

The framework will map the identified risks with practical, business-aligned mitigation strategies, including policy changes, technical safeguards, human oversight and escalation protocols. A review of the framework will be conducted after one year. However, if major evolutions in AI raise new risks that require new mitigation actions, the review will take place sooner.

This risk exercise will be conducted in close cooperation with all involved stakeholders, in particular the Risk, Crisis and Business Continuity Unit within the Central Services and the Data Protection Unit. In parallel, Parliament responsible services will continue to work closely with the European Data Protection Supervisor (EDPS) through the designated EP AI Correspondent, with the AI Office and other relevant European Union bodies to systematically track and remediate risks associated with AI.

Deliverable
• AI risk identification and mitigation plan

Workstream II - Infrastructure

AI infrastructure comprises the hardware and software needed to create and deploy AI solutions. AI infrastructure is key to enable developers to effectively create and deploy AI and machine learning (ML) applications like for instance chatbots.

Parliament AI infrastructure is highly fragmented, leading to inefficiencies and ultimately risks. This workstream will therefore focus on the standardisation of AI architecture, enabling a smooth and coherent deploy of AI solutions in the Parliament. This foundational work will be key for establishing infrastructure for generative AI as well as successfully implementing machine learning and model operations. Accordingly, the workstream provides for the following three actions:

- Action 1: Defining the AI reference infrastructure;
- Action 2: Establishing foundational infrastructure for AI;
- Action 3: Implementing machine learning and model operations.

- ***Action 1 - Defining the AI reference architecture***

AI architecture includes different layers, such as AI applications, the AI capability platform, the AI framework, etc.

In order to maximise the efficiency of AI infrastructure and coherence, it is proposed to standardise the AI architecture. This includes defining the concept of AI architecture, describing the layers contained in the AI architecture, the hierarchical relationships or interfaces between these layers, as well as the basic functions, input and output information of each layer within the AI architecture.

Deliverables
• AI reference architecture diagram • Technology stack recommendations

- ***Action 2 - Establishing foundational infrastructure for AI***

For generative AI to reach its full potential throughout Parliament, a strong infrastructural foundation, a platform, must be put in place. This platform should be flexible, secure and scalable enough to allow for experimentation, foster rapid deployment of the models and encourage responsible development and application. This foundation should be used to enable all generative AI efforts.

The foundational infrastructure for generative AI will enable the Parliament to keep pace with machine learning advancements. It will be composed of modular components that allow for both the scaling of open-source and commercial model use, and dedicated governance.

However, generative AI is not the only type of artificial intelligence. Depending on the identified use cases, Parliament will also need to consider a wider portfolio of AI technologies. Each specific type of technology (e.g. predictive analytics, computer vision and autonomous systems) will be assessed and specific governance processes will be developed. Different AI systems pose different risks and will require different approaches.

Deliverables
• GenAI reference architecture blueprint • Model sourcing strategy document • Prompt engineering and management framework

- ***Action 3 - Implementing machine learning and model operations***

To transition from experimentation to execution, Parliament must operationalise how it builds, deploys and manages AI models. The International Organisation for Standardisation has published a new standard[4] on AI Management Systems. It will be assessed how to implement the relevant parts of the standard.

Machine learning operations and Model operations (MLOps and ModelOps) capability will be necessary to allow machine learning to be a repeatable, scalable and a reliable capability for the organisation as opposed to a one-time occurrence. This larger capability will lay the foundation for managing the complete machine learning model lifecycle. It should cover training, deployment and ongoing monitoring. It should also include governance, traceability and tracking.

Implementing machine learning and model operations throughout Parliament will enable a single cooperation setup for data scientists, engineers, and business teams. This will reduce production time and improve model performance in real-world use.

Deliverables (potential generated artefacts)
• MLOps reference architecture diagram • Model monitoring framework

Workstream III - Skills

The successful use of AI in the Parliament requires more than technology. It depends on people, skills and a shared culture of responsible use. To this end, AI literacy will be key. Accordingly, Article 4 of the AI Act establishes that: "*Providers and deployers of AI systems shall take measures to ensure, to their best extent, a sufficient level of AI literacy of their staff and other persons dealing with the operation and use of AI systems on their behalf, taking into account their technical knowledge, experience, education and training and the context the AI systems are to be used in, and considering the persons or groups of persons on whom the AI systems are to be used.*"

For Members, their assistants and EP staff, AI literacy is crucial to make informed decisions about adopting and overseeing AI tools in parliamentary and administrative work. Developing AI skills across the institution will ensure that the Parliament has both the broad awareness and the specialised expertise to guide AI use responsibly and strategically.

To follow up on the above, the following actions will be implemented to leverage AI literacy, including through awareness and knowledge management:

- Action 1: Developing an AI literacy programme;
- Action 2: Carrying out regular awareness campaigns;

[4] ISO/IEC 42001:2023.

 Action 3: Leveraging the EP AI portal as primary information point on AI .

- ***Action 1 - Developing an AI literacy programme***

At a basic level, AI literacy means being able to recognise where AI is applied, to understand concepts such as machine learning and data analysis and to critically assess the opportunities and risks of these technologies. A more advanced level of AI literacy is required for those directly involved in designing, managing or evaluating AI systems. This deeper expertise includes knowledge of the core principles of AI, the risks and business impacts of AI systems, their technologies and applications, as well as the analytical and algorithmic methods on which they rely. It also requires a strong grasp of data management and data literacy, combined with a clear understanding of the ethical dimensions of AI.

To launch and develop Parliament's AI literacy programme, the responsible Parliament services have already created on-boarding material and launched several AI training courses. The training offer will undergo continuous review and adaptation to the audiences, which include general users, managers, IT professionals and Members. Specific courses will also be created for the use of AI applications by policy DGs.

Deliverables
• Foundational AI learning track • Tailored workshops and specific training sessions • Custom trainings for EP-specific AI tools (e.g. EP GenAI Hub)

- ***Action 2 - Carrying out regular awareness campaigns***

AI awareness is crucial to foster responsible use of AI tools and inform the users about new developments and opportunities, but also about risks. Internal communication materials including videos, posters, emails and workshops will introduce what AI is (and isn't), where it's being used and what's coming next.

Members and staff will also be regularly surveyed on their AI awareness and AI adoption to track overall literacy scores and perceived risks. The results of the surveys will inform training offer and the development of awareness campaigns.

Deliverables
• Periodic AI-focused events • AI awareness and readiness surveys

- ***Action 3 - Leveraging the EP AI portal as primary information point on AI***

An EP AI portal has been established and made accessible to any user with a valid Parliament account. Its primary purpose is to provide a structured way to communicate about AI and raise awareness.

The portal will be further developed and will centralise knowledge, standards and resources to ensure responsible, consistent and transparent AI use throughout Parliament. It will provide information about the implementation of AI solutions and risks. It will also feature information about use cases and highlight new opportunities.

Deliverable
• EP AI Portal

Workstream IV - Application

This workstream focuses on defining and embedding standard processes and acquiring the right tools to support the application of AI across its entire lifecycle. The goal is to move from fragmented, uncoordinated and experimental AI-based activities and projects to scalable, production-grade and responsible AI capabilities. This involves setting up continuous integration and delivery pipelines for AI models, automating deployment and rollback processes, and defining clear operational support structures. Such a structured approach will facilitate the transition from development to production and make AI deployments predictable, responsible and efficient.

It is important to note that these processes should be integrated into existing workflows (e.g. procurement, software selection) to ensure alignment, reduce duplication and facilitate adoption across the Parliament. Accordingly, the existing IT planning processes should be also used for planning AI ideas. Particular attention should be given to existing tools or software that are being modified to include AI features.

The workstream provides for the following actions:

- Action 1: Establishing an AI use case methodology;
- Action 2: Carrying out systematic and regular testing of AI solutions;
- Action 3: Measuring AI deployment and maturity.

- ***Action 1 - Establishing an AI use case methodology***

Successful AI implementation relies on well-managed use case identification, evaluation and follow-up, as well as on information sharing and stakeholder engagement. To achieve this, a clear and systematic methodology for evaluation AI use cases is essential. This process includes (i) use case identification and ideation, and (ii) evaluation and assessment.

By implementing a robust AI use case methodology for gathering, evaluating and prioritising AI use cases, Parliament will be able to focus on high-impact projects, maximising the return on investment and gaining a competitive edge in leveraging AI.

To respond to the fast AI development and assess the viability of proposed use cases, the possibility for a prototyping phase has been already foreseen in the IT Plan workflow. This approach should be used, for instance, when the underlying technology is still maturing, or when agility is required to assess feasibility, complexity and cost.

Deliverable
• AI use case evaluation template

- ***Action 2 - Carrying out systematic and regular testing of AI solutions***

Testing is fundamental to guarantee the safe and compliant usage of AI solutions. As a first step, a testing methodology will be developed that takes the specific risks, challenges and opportunities typical for AI solutions into account. Testing priorities will be fixed according to the estimated risk of the proposed solution. The testing methodology should flag up identified risks and propose mitigation strategies.

The AI governance structures will be leveraged to ensure that AI-based solutions are fed into the testing assessment cycle as well as for the evaluation and acceptance of potential residual risks remaining after the application of the mitigation strategies.

Deliverable
• Adaptation of testing methodology for AI-based solutions

- ***Action 3 - Measuring AI deployment and maturity***

The application of AI solutions must be continuously assessed to identify any gaps that could prevent its effective adoption, deployment and use. These gaps may include technical infrastructure, expertise, as well as awareness and literacy. In order to measure AI capability in the Parliament, two tools will be put in place: (i) an AI value monitoring system, and (ii) an AI maturity assessment.

The value monitoring system will aim at identifying the extent to which deployed AI systems deliver the expected outcomes in terms of financial savings, time efficiency and quality improvements. It will include the definition of performance indicators and targets, measuring processes such as surveys, usage statistics collection, AI training course attendance statistics, cost control systems, continuous model benchmarking, sample checks in deliverable quality, etc. The system will help ensure transparency about how AI tools are working and the impact they have on the work of the Institution.

The maturity assessment will be based on established maturity measurement methodologies and include a set of metrics, surveys and the scorecard. Maturity assessments will be carried out on an annual basis to measure progress. The results of the assessments will feed into the further improvements and adaptation of the roadmap and enhanced implementation of AI-related objectives, policies and actions.

Deliverables
● AI value metrics ● “Use case to value” mapping templates ● Automated KPI tracking pipelines

Annex I: Implementation timeline