engaging NETWORKS

Policy on the Development and Deployment of Artificial Intelligence

Authorised by		**Appointment**	Head of Compliance and Risk	**Date**	**13 Dec 24**
Produced by	Michael Servaes	**Appointment**	Data Protection Officer	**Date**	**14 Oct 24**
Document Classification			**Policy Number**		

Document Version History

Version Number	Reviewed By	Function
1.0		COO
		CEO

Amendment History

Number	Date	Details of amendment

Contents

Policy on the Development and Deployment of Artificial Intelligence

1. Introduction. Engaging Networks (EN) develops and deploys Artificial Intelligence (AI) to provide additional services to its clients and for our own use. This policy outlines the framework for the legal and ethical development and deployment of Artificial Intelligence (AI) within our organization, ensuring compliance with UK, EU, US and other data protection regulations, and the new EU AI Act covering the development and use of AI, Regulation EU 2024/1689, that became law on 01 Aug 2024.

2. Objectives. This policy will:

a. Ensure AI systems are developed and deployed by EN in accordance with the EU AI Act and in a manner that respects individual privacy and data protection rights.

b. Promote transparency, accountability, and fairness in AI operations.

c. Establish a governance structure to oversee AI initiatives and ensure compliance with relevant regulations.

3. Scope.

a. This policy applies to all deployed AI and any new projects and initiatives undertaken by EN, including those developed internally, those developed in collaboration with third parties or those purchased from third parties.

b. The EU AI Act (EU 2024/1689) has global applicability in as much as deployed AI has an effect on the rights of an EU citizen. Where EN develops and deploys AI that may infringe on the rights of (an) EU citizen(s) it must ensure compliance with the requirements of the Act.

4. Definitions. The following definitions will be used in this policy and when referring to AI applications by EN

a. **AI System.** An AI system means a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.

b. **Intended Purpose. I**ntended purpose means the use for which an AI system is intended by the provider, including the specific context and conditions of use, as specified in the information supplied by the provider in the instructions for use, promotional or sales materials and statements, as well as in the technical documentation.

c. **Reasonably Foreseeable Misuse.** This term means the use of an AI system in a way that is not in accordance with its intended purpose, but which may result from reasonably foreseeable human behaviour or interaction with other systems, including other AI systems.

d. **Serious Incident.** A serious incident is an incident or malfunctioning of an AI system that directly or indirectly leads to any of the following:

1) The death of a person, or serious harm to a person's health (unlikely in EN AI).

2) A serious and irreversible disruption of the management or operation of critical infrastructure (again unlikely).

3) The infringement of obligations under Union law intended to protect fundamental rights e.g. data protection rights.

4) Serious harm to property or the environment

e. **Widespread Infringement.** This is an act or omission contrary to Union law protecting the interest of individuals, which:

1) Has harmed or is likely to harm the collective interests of individuals residing in at least two EU Member States other than the Member State in which:

(a) The act or omission originated or took place;

(b) The provider concerned, or, where applicable, its authorised representative is located or established; or

(c) The deployer is established, when the infringement is committed by the deployer;

2) Has caused, causes or is likely to cause harm to the collective interests of individuals and has common features, including the same unlawful practice or the same interest being infringed, and is occurring concurrently, committed by the same operator, in at least three Member States.

f. **General-Purpose AI (GPAI) model.** A GPAI model is one where the AI model is trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable of competently performing a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications, except AI models that are used for research, development or prototyping activities before they are placed on the market.

g. **GPAI System.** An AI system which is based on a general-purpose AI model, and which has the capability to serve a variety of purposes, both for direct use as well as for integration in other AI systems;

h. **Prohibited AI systems**: Prohibited AI systems are those which:

1) Deploy **subliminal, manipulative, or deceptive techniques** to distort behaviour and impair informed decision-making, causing significant harm.

2) **Exploit vulnerabilities** related to age, disability, or socio-economic circumstances to distort behaviour, causing significant harm.

3) **Biometric categorisation systems** inferring sensitive attributes (race, political opinions, trade union membership, religious or philosophical beliefs, sex life, or sexual orientation), except labelling or filtering of lawfully acquired biometric datasets or when law enforcement categorises biometric data.

4) **Social scoring**, i.e., evaluating or classifying individuals or groups based on social behaviour or personal traits, causing detrimental or unfavourable treatment of those people.

5) **Assess the risk of an individual committing criminal offenses** solely based on profiling or personality traits, except when used to augment human assessments based on objective, verifiable facts directly linked to criminal activity.

6) **Compile facial recognition databases** by untargeted scraping of facial images from the internet or CCTV footage.

7) **Infer emotions in workplaces or educational institutions**, except for medical or safety reasons.

8) **Conduct ‘real-time’ remote biometric identification (RBI) in publicly accessible spaces for law enforcement**, except when:

a) Searching for missing persons, abduction victims, and people who have been human trafficked or sexually exploited;

b) Preventing substantial and imminent threat to life, or foreseeable terrorist attack; or

c) Identifying suspects in serious crimes (e.g., murder, rape, armed robbery, narcotic and illegal weapons trafficking, organised crime, and environmental crime, etc.).

i. **Risk.** AI management is based upon risk, i.e the likelihood of something happening. AI systems should be managed under the following 4 risk categories:

1) **Minimal risk:** most AI systems such as spam filters and AI-enabled video games face no obligation under the AI Act, but companies can voluntarily adopt additional codes of conduct.

2) **Specific transparency risk:** systems like chatbots must clearly inform users that they are interacting with a machine, while certain AI-generated content must be labelled as such.

3) **High risk:** high-risk AI systems such as AI-based medical software or AI systems used for recruitment must comply with strict requirements, including risk-mitigation systems, high-quality of data sets, clear user information, human oversight, etc.

4. **Unacceptable risk:** for example, AI systems that allow “social scoring” by governments or companies are considered a clear threat to people's fundamental rights and are therefore banned.

j. **Risk Management System**. The risk-management system is a continuous, iterative process that is planned and run throughout the entire lifecycle of an AI system. That process should be aimed at identifying and mitigating the relevant risks of AI systems on health, safety and fundamental rights. The risk-management system should be regularly reviewed and updated to ensure its continuing effectiveness, as well as justification and documentation of any significant decisions and actions taken. This process should ensure that the provider identifies risks or adverse impacts and implements mitigation measures for the known and reasonably foreseeable risks of AI systems to the health, safety and fundamental rights in light of their intended purpose and reasonably foreseeable misuse, including the possible risks arising from the interaction between the AI system and the environment within which it operates.

5. Governance Structure

a. The EU AI Act (EU 2024/1689) seeks to reduce the risk to the rights of individuals but to provide an environment that allows businesses to develop and deploy AI that delivers benefits without infringing on the individual’s rights. This means that the development and deployment of AI systems must be governed in accordance with the risks that system causes to the rights of the individual. The Head of Risk and Compliance will lead the EN AI Governance Committee and Risk Management System.

b. **AI Governance Committee:** This committee will include the DPO and representatives from legal, IT and the business units. The committee will:

1) Deliver the required level of governance and oversight that ensures that EN development and deployment of AI is in accordance with the principles of “risk management”

2) Review and approve AI projects.

3) Ensure compliance with GDPR and DPA 2018.

4) Monitor AI systems for ethical considerations and potential biases.

5) Review the effects of in place AI to determine if the AI is still performing within regulatory and ethical limits.

6) Lead the investigation of incidents relating to EN deployed AI.

7) The committee will meet (virtually) on a monthly basis, and more frequently should the pace of development require it, or an incident occur.

c. **Data Protection Officer (DPO).** As a member of the AI Governance Committee the DPO will:

1) Oversee data protection strategies and ensure that AI systems comply with data protection laws.

2) Ensure the conduct of and assist on Data Protection Impact Assessments (DPIAs) for all AI projects.

3) Provide guidance on data protection issues related to AI.

6. Development and Deployment Guidelines.

a. **Data Minimization.** This principle is a carry over from data protection and requires that EN/the project will only connect such data as is required to ensure that the AI can function effectively; that data should be "retired" when it is no longer required.

b. **Anonymisation and Pseudonymisation**. Any AI system deployed by EN must use data that is Anonymised, or if that cannot be achieved it must be Pseudonymised. This requirement comes directly from data protection regulations and is a method of reducing bias.

c. **Transparency.**

1) Every individual has the right to be informed of the purpose for which their data is being collected and used. This is, of course, of greater importance if the data is being processed using AI and reflects the rights included in UKGDPR/GDPR Art 6, 18 and particularly Art 21, the right to object to automated processing of their data.

2) Where AI is used to make decisions about the individual there must be a clear statement included in the Privacy Statement that covers not just the data used but also a statement of how the decision is made.

3) Clients have the right to request information about how their data is used in AI decision-making processes. The organization will provide clear and concise explanations in response to such requests.

d. **Fairness and Accountability.**

1) Where EN deploys AI, it is incumbent on it to demonstrate to users, or to enable clients to demonstrate to their users, how the AI operates to reinforce fairness and to avoid discrimination. We will do this through clear statements in our Privacy Policy and through frequent audits that will be directed by and report to the EN AI Governance Committee.

2) EN is required to demonstrate that the AI it deploys is fair and accountable and any decision meets these criteria. To do this where the AI makes decisions regarding individuals, we will deploy a capability for

individuals to appeal decisions about them either to EN directly or in support of appeals made to clients deploying EN provided AI.

7. Training and Awareness

a. EN has a strong record in delivering training to its employees to cover data protection and information security. In line with that training all employees and contractors involved in AI development and use will undergo mandatory training on GDPR requirements, ethical AI principles, and this AI policy. The training will cover topics such as data privacy, fairness, transparency, and accountability.

b. Regular updates and refresher training will be provided to ensure ongoing awareness and compliance. The organization will foster a culture of responsible AI use and encourage open dialogue on ethical considerations.

8. Incident Reporting and Response

a. Any incidents or breaches related to EN deployed AI systems and client data is to be promptly reported to the AI governance committee through established reporting channels. In this instance the term incident includes where bias or discrimination have been identified in the decision making.

b. With the DPO and in line with paragraph 5.b.6) the AI Governance Committee will investigate the incident, assess the impact, and take appropriate actions to mitigate risks and ensure compliance with GDPR requirements. This may involve suspending or modifying AI systems, notifying relevant authorities, and implementing corrective measures.

c. Clients affected by any incidents will be notified in accordance with GDPR breach notification requirements. EN will provide clear information about the nature of the incident, its potential consequences, and the steps taken to address it.

9. Third-Party Vendors and Partnerships

a. From time to time EN may engage with third-party vendors or partners for AI development or deployment. Where this occurs EN will ensure that the third parties adhere to the principles and requirements outlined in this policy and the development and deployment will be conducted under the governance of the AI Governance Committee.

b. Contracts and agreements with third parties for the development and/or deployment of AI are to include provisions related to data privacy, security, and compliance with GDPR and other applicable regulations.

10. Continuous Improvement and Innovation

a. EN as an organization encourages continuous improvement and innovation in AI technologies while upholding the principles of responsible and ethical AI use and this policy should be an enabler of that innovation and development within the law.

b. EN is also a “learning organization” and employees are encouraged to stay updated with the latest developments in AI and GDPR regulations and to share knowledge and best practices within the organization. As a part of this culture of learning EN will actively participate in industry forums, collaborations, and research initiatives to contribute to the advancement of responsible AI practices.

11. Policy Violations and Consequences

a. The EU AI Act brings with it criminal sanctions for the worst transgressor and as such violations of this AI policy may result prosecution for EN or responsible individuals. Internally, violations may result in disciplinary action, up to and including termination of employment or contract.

b. EN reserves the right to report any illegal activities related to AI misuse to the appropriate authorities.

12. Review and Update.

a. This AI policy will be regularly reviewed and updated, at least annually, to ensure alignment with evolving AI and data privacy regulations, industry best practices, and organizational requirements. The AI governance committee will be responsible for conducting the review and proposing updates as necessary.