European Union Agency
Ref. Ares(2021)6483454 - 21/10/2021 rity
Vasilissis Sofias Str 1
151 24 Maroussi | Attiki | Greece
Tel: +30 28 14 40 9711
E-mail: info@enisa.europa.eu
www.enisa.europa.eu

BRIEFING NOTE: AI REGULATION AND THE COORDINATED PLAN ON AI 2021 REVIEW

1. EXECUTIVE SUMMARY

On 21 April 2021, the proposal for the first ever **AI Regulation**[1], which addresses the risks of AI and positions Europe to play a leading role globally, together with a **Coordinated Plan**[2] has been published by the European Commission. ENISA welcomes the EC proposal for an AI regulation and the updated EU coordinated action plan for AI and stands ready to support EC actions.

The key objectives of the EC proposal for a Regulation are:

- providing **internal market rules** for AI systems, **aligned with EU product safety legislations**,
- guaranteeing the **safety and fundamental rights** of people and businesses, while **strengthening AI uptake, investment and innovation** across the EU
- focus on concrete high-risk use cases (e.g. risks to **health, safety and/or fundamental rights**) and not on the technology per se.

ENISA has identified the following key areas in which it may assist in the implementation of the proposed AI Regulation:

- putting forward **good practices** and elements for the **risk management system** insofar as cybersecurity is concerned,
- supporting work of the **Artificial Intelligence Board** and National Competent Authorities by providing **advice, opinions, recommendations on cybersecurity aspects** of the Regulation,
- providing cybersecurity requirements needed in **the operation of AI regulatory sandboxes**.

The Coordinated Plan represents a **joint commitment between the Commission and Member States** for **Europe to maximise its AI potential to compete globally** and it includes 4 key actions:

- set **enabling conditions for AI** development and uptake in the EU,
- make the **EU the place where excellence thrives** from the lab to the market,
- ensure that **AI works for people** and is a force for good in society,
- build **strategic leadership** in high-impact sectors.

In support of the Coordinated Plan, **ENISA stands ready to provide**:

- updates to the **AI threat landscape** and **sectorial risk assessments for AI**,

[1] Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence-artificial-intelligence
[2] Coordinated Plan on Artificial Intelligence 2021 review, https://digital-strategy.ec.europa.eu/en/library/coordinated-plan-artificial-intelligence-2021-review

- **qualitative cybersecurity practices for AI and policy recommendations**, which support the Commission in facilitating the uptake of and synergies between national actions,
- advice on **research and innovation priorities** for the application of **AI in cybersecurity**,
- continued **stakeholder engagement** via the AI Working Group.

2. ENISA SUPPORT OF THE REGULATION AND THE COORDINATED PLAN

2.1 THE AI REGULATION

Requirements for high-risk AI systems

The proposal adopts a risk-based approach and imposes regulatory burdens only when an AI system is likely to pose high risks to fundamental rights and safety. Predictable, proportionate and clear obligations are placed on providers and users of those systems to ensure safety and respect of existing legislation protecting fundamental rights throughout the whole AI systems' lifecycle. These obligations include establishment of risk management process, maintenance of accurate technical documentation, and compliance with robustness, accuracy and cybersecurity requirements.

Recommendation: ENISA can provide good practices and elements for the risk management system insofar as cybersecurity is concerned, further to (baseline) security measures, appropriate to the level of risk. ENISA can also contribute to guidelines on technical documentation from the cybersecurity perspective, e.g. description of the security architecture/mechanisms, implemented security and privacy preserving measures and therefore, help mapping consistently AI regulation levels and CSA levels.

Cybersecurity certification for AI

ENISA has noticed that the cybersecurity schemes under development (EUCC, EUCS) are in line with what is proposed in the Regulation in terms of requirements for high-risk AI systems, i.e. testing, documentation, transparency and human oversight, except for AI attacks.

Recommendation: Both EUCC and EUCS are horizontal certification schemes which are designed to be extensible by the definition of protection profiles, therefore ENISA can organize the development of such protection profiles for these schemes, allowing product vendors and cloud service providers to cover the cybersecurity requirements of the AI regulation.

ENISA is likely to be involved in the preparation of certification scheme/s for AI as this is indicated in the current Draft URWP as an area for future certification.

Recommendation: If ENISA is to receive a request for scheme development alignment with the AI Regulation and the current schemes (under development), as well as specific AI attacks can be taken into account. If a scheme is to be defined in accordance to the CSA, then we'll go for the now "routine" of a request from the EC, an AHWG to support ENISA, etc.

Non-high-risk AI systems

For non-high-risk AI systems only limited transparency and notification obligations are imposed on the AI systems providers. The AI Regulation also contains a framework for codes of conduct, which encourage providers of non-high-risk AI systems to apply voluntarily the mandatory requirements for high-risk AI systems or include other voluntary commitments.

Recommendation: ENISA can advise organizations preparing codes of conducts on cybersecurity and privacy measures which should be included in them.

EU Database (validation of cybersecurity certifications)

ENISA has noticed that while information about cybersecurity certificates issued for an AI system that is registered in the EU database (Article 60 and Annex VIII) must be provided, the AI Regulation doesn't

identify a mechanism for checking validity of this certification. This may lead to a situation that withdrawal or expiry of a cybersecurity certification will result in incorrect information in the EU database.

Recommendation: It is recommended that the ENISA is involved in the practical implementation of the Commission registration system and development of notification and communication mechanisms to ensure alignment and co-operation.

Competent authorities

ENISA observes that an AI notification authority most likely is not the NCCA (the notifying body under the CSA). Conformity assessment bodies may also not necessarily be the same, as cybersecurity certification is demanding substantially different competences and skills than the conformity assessment bodies under the AI Regulation. Different authorities need to cooperate and coordinate with each other when it comes to monitoring and supervision and investigative powers and different applicable penalty systems in the situation of large-scale cross border incidents in a efficient and effective manner.

Recommendation: ENISA recommends that the AI Regulation clarifies what authority will be the lead from national perspective and cross boarder perspective, as well as what are the incident handling, reporting and non-compliance rules that apply and in what prioritised order actions to be taken. ENISA can support this area via recommendations on co-operation and co-ordination procedures related to cybersecurity incidents and on alignment of the different applicable incident handling rules under different Regulations.

Regulatory sandboxes

Innovation aspects of the AI Regulation include creation of regulatory sandboxes as controlled environment that facilitates the development, testing and validation of innovative AI systems. Given that the Regulation allows further processing of personal data for developing certain AI systems in the public interest in these sandboxes, their successful operation depends, among other things, on adequate cyber security and privacy measures.

Recommendation: ENISA can provide the level of cybersecurity requirements needed to allow secure operation of this sandboxes. Additionally, in the foreseen cooperation with EDPS, ENISA could become a partner in a sandbox that is to be established by EDPS (Article 53).

Governance

Compliance with existing law on fundamental rights and safety requirements applicable to AI systems and with the proposed rules will be enforced through a governance system at Member States level (national competent and notification authorities) and through a cooperation mechanism at Union level with the establishment of a European Artificial Intelligence Board, which will be composed of representatives from the Member States and the Commission (namely European Data Protection Supervisor). Despite its long-standing commitment in cyber security issues affecting the smooth adoption of AI, the proposed Regulation foresees ENISA role at the AI Board level only in a consultative manner.

Recommendation: For a smooth functioning of the new AI eco-system at European level, ENISA can provide to the AI Board and the Member States advice, opinions, recommendations on cybersecurity aspects of the Regulation. It also might be worth considering soliciting a permanent status of ENISA at the AI Board.

Amendments to the proposal

Adequate security and data protection are essential elements of trustworthy AI systems, therefore security and data protection by design should be integrated in their design and development. However, these principles are not explicitly mentioned in the AI Regulation.

Recommendation: ENISA proposes addition to the Regulation text as follows:

"*Security by design to be explicitly mentioned. Data protection by design and default are already legal requirements but could also be stated."*

2.2 THE COORDINATED PLAN

Synergies between national actions

When it comes to **support of the** the key action: set **enabling conditions for AI** development and uptake in the EU, **ENISA is currently running a project on stock taking of national and regional AI cybersecurity strategies and polices**.

Recommendation: Outputs of the ENISA project, which include identification of good cybersecurity practices for AI and preparation of policy recommendations, can support the Commission in facilitating the uptake of and synergies between national actions identified in national AI strategies.

AI Threat Landscape

In December 2020 ENISA published the Threat Landscape for Artificial Intelligence report[3], which has been identified in the Coordinated Plan as one of the activities supporting trust in AI systems. Since the technology evolves and new threats emerge all the time, risk assessment and security controls should take into account and reflect the evolving threat landscape.

Recommendation: ENISA could update its AI threat landscape as described in the Coordinated Plan. This year ENISA is working on identifying security controls for Machine Learning algorithms. Subject to the need, ENISA could continue identification of pertinent and proportionate security controls.

Research and innovation

The key action: make the EU the place where excellence thrives from the lab to the market focuses on: building and mobilising research capabilities, identifying measures to boost AI research and innovation excellence and on improving European competitiveness.

Recommendation: ENISA is working this year on the research and innovation priorities for the application of AI in cybersecurity and can provide recommendations and advice in this area.

[3] https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges

ANNEX I - SUMMARY OF ENISA RECOMMENDATIONS

Subject	Recommendation
AI REGULATION PROPOSAL	
Requirements for high-risk AI systems	ENISA can provide good practices and elements for the risk management system insofar as cybersecurity is concerned, further to (baseline) security measures, appropriate to the level of risk. ENISA can contribute to guidelines on technical documentation from the cybersecurity perspective, e.g. description of the security architecture/mechanisms, implemented security and privacy preserving measures and therefore, help mapping consistently AI regulation levels and CSA levels.
Cybersecurity certification for AI	Both EUCC and EUCS are horizontal certification schemes which are designed to be extensible by the definition of protection profiles, therefore ENISA can organize the development of such protection profiles for these schemes, allowing product vendors and cloud service providers to cover the cybersecurity requirements of the AI regulation. If ENISA is to receive a request for scheme development alignment with the AI Regulation and the current schemes (under development), as well as specific AI attacks can be taken into account. If a scheme is to be defined in accordance to the CSA, then we'll go for the now "routine" of a request from the EC, an AHWG to support ENISA, etc.
Non-high-risk AI systems	ENISA can advise organizations preparing codes of conducts on cybersecurity and privacy measures which should be included in them.
EU Database (validation of cybersecurity certifications)	It is recommended that the ENISA is involved in the practical implementation of the Commission registration system and development of notification and communication mechanisms to ensure alignment and co-operation.
Competent authorities	ENISA recommends that the AI Regulation clarifies what authority will be the lead from national perspective and cross boarder perspective, as well as what are the incident handling, reporting and non-compliance rules that apply and in what prioritised order actions to be taken. ENISA can support this area via recommendations on co-operation and co-ordination procedures related to cybersecurity incidents and on alignment

	of the different applicable incident handling rules under different Regulations.
Regulatory sandboxes	ENISA can provide the level of cybersecurity requirements needed to allow secure operation of this sandboxes. Additionally, in the foreseen cooperation with EDPS, ENISA could become a partner in a sandbox that is to be established by EDPS (Article 53).
Governance	For a smooth functioning of the new AI eco-system at European level, ENISA can provide to the AI Board and the Member States advice, opinions, recommendations on cybersecurity aspects of the Regulation. It also might be worth considering soliciting a permanent status of ENISA at the AI Board.
Amendments to the proposal	ENISA proposes addition to the Regulation text as follows: "Security by design to be explicitly mentioned. Data protection by design and default are already legal requirements but could also be stated."
	AI COORDINATED PLAN
Synergies between national actions	Outputs of the ENISA project, which include identification of good cybersecurity practices for AI and preparation of policy recommendations, can support the Commission in facilitating the uptake of and synergies between national actions identified in national AI strategies.
AI Threat Landscape	ENISA could update its AI threat landscape as described in the Coordinated Plan. This year ENISA is working on identifying security controls for Machine Learning algorithms. Subject to the need, ENISA could continue identification of pertinent and proportionate security controls.
Research and innovation	ENISA is working this year on the research and innovation priorities for the application of AI in cybersecurity and can provide recommendations and advice in this area.

ANNEX II – SUMMARY OF AI REGULATION AND THE COORDINATED PLAN

2.3 AI Regulation

2.3.1 General Provisions

Title I define the subject matter of the regulation and the scope of application of the new rules that cover the placing on the market, putting into service and use of AI systems. It also sets out the definitions used throughout the instrument:

- **Internal market rules** for EU and non-EU providers of AI systems, **aligned with EU product safety legislations**
- No regulation of the technology as such, but of concrete **high-risk use cases**
- Exclusions for AI developed **exclusively for military purposes** and used by **public authorities in a third country** or by **international organisations**

Definition of AI (as neutral as possible in order to cover techniques which are not yet known/developed, aims to cover all AI, including traditional symbolic AI, Machine learning, as well as hybrid systems):
"a software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with"[4]

2.3.2 Prohibited AI practices

The list of prohibited practices in Title II comprises all those AI systems which use is considered unacceptable as contravening Union values, for instance by violating fundamental rights:

- **Subliminal manipulation** resulting in physical / psychological harm
- **Exploitation of vulnerabilities** resulting in physical/psychological harm
- **'Social scoring'** by public authorities
- **'Real-time' remote biometric identification for law enforcement purposes in publicly accessible spaces** (with certain exceptions)

2.3.3 Hi-risk AI systems

The Regulation follows a risk-based approach, differentiating between uses of AI that create a) an unacceptable risk (mentioned above), b) a high risk, and c) low or minimal risk. Chapter 1 of Title III sets the classification rules and identifies two main categories of high-risk AI systems:

- **Safety components of regulated products** (e.g. medical devices, machinery) which are **subject to third-party assessment** under the relevant sectorial legislation
- **Other stand-alone AI systems** in the areas defined in Annex III, e.g. biometric identification and categorisation of natural persons and many other.

2.3.4 High-risk AI system requirements

Chapter 2 of Title III contains specific rules and legal requirements for AI systems that create a high risk to the health and safety or fundamental rights of natural persons. They are identified as:

- **Risk management system** - establishment and continuous iterative risk management process,
- **Data and data governance** - Using High-quality training, validation and testing data,
- **Technical documentation** - drawing up and maintain accurate and complete technical documentation,
- **Record keeping** - capabilities enabling the automatic recording of events ('logs') while the high-risk AI systems is operating,

[4] This definition is based on the OECD definition

- **Transparency and provision of information to users** - design and development of high-risk AI systems in such a way to ensure that their operation is sufficiently transparent to enable users to interpret the system's output and use it appropriately,
- **Human oversight** - design and development of high-risk AI systems which include appropriate human-machine interface tools, that they can be effectively overseen by natural persons during the period in which the AI system is in use,
- **Robustness, accuracy and cybersecurity** - design and developme of high-risk AI systems in such a way that they achieve, in the light of their intended purpose, an appropriate level of accuracy, robustness and cybersecurity, and perform consistently in those respects throughout their lifecycle.

2.3.5 Obligations of AI systems operators

Chapter 3 of Title III includes a clear set of horizontal obligations on providers of high-risk AI systems. Proportionate obligations are also placed on users and other participants across the AI value chain.

- **Providers obligations include:**
  - establishing and implementing quality management system,
  - up to date technical documentation,
  - conformity assessment and re-assessment (in case of substantial modification),
  - registering an AI system in the EU database,
  - affixing CE marking and sign declaration of conformity,
  - conducting post-market monitoring,
  - collaborating with market surveillance authorities.
- **Users obligations include:**
  - operating AI system in accordance with instructions of use,
  - ensuring human oversight when using an AI system,
  - monitoring operation for possible risks,
  - informing the provider or distributor about any serious incident or malfunctioning,
  - complying with existing legal obligations (e.g. under GDPR).

2.3.6 Non-high-risk AI systems

While non-high-risk AI systems don't have to comply with the requirements listed above, transparency and notification obligations described in Title IV apply to some of them, specifically when humans are:

- **interacting with an AI system** unless this is evident,
- **exposed to emotional recognition** or **biometric categorisation** systems,
- **exposed to deep fakes** (generated or manipulated images, audio or video).

The regulation also creates a framework for **codes of conduct**, which aim to encourage providers of non-high-risk AI systems to apply voluntarily the mandatory requirements for high-risk AI systems. Providers of non-high-risk AI systems may create and implement the codes of conduct themselves.

2.3.7 Supporting Innovation

One of the objectives of the Regulation (Title V) is creation of a legal framework that is innovation-friendly, future-proof and resilient to disruption:

- **Regulatory sandboxes** - controlled environment to test innovative technologies under supervision and in cooperation with national authorities or the European Data Protection Supervisor.
- **Support for SMEs/start-ups** include **priority access to regulatory sandboxes** and measures to reduce the regulatory burden on SMEs and start-ups.

2.3.8 Governance

The Regulation (Titles VI, VII AND VII) sets up the governance systems at Union and national level.

- **National Competent Authorities (NCA)** - At national level, Member States will have to designate one or more national competent authorities and, among them, the national supervisory authority
    - responsible for the application and implementation of the Regulation,
    - oversight of conformity assessment bodies
    - market surveillance activities ex Regulation (EU) 2019/1020
- **Artificial Intelligence Board** (representatives from NCAs and EDPA)
    - facilitate a smooth, effective and harmonised implementation of this Regulation
    - collect and share best practices & expertise (harmonized standards, technical specifications and guidance documents),
    - provide advice, opinions, recommendations on AI issues.

2.4 The Coordinated Plan on AI 2021 Review

2.4.1 Set Enabling Conditions for AI Development and Uptake in the EU

In order to support the development and take-up of AI and to achieve the objectives of this Coordinated Plan, appropriate governance and coordination framework must be established. **All Member States made substantial efforts to develop national strategies on AI.** The next step is to ensure that these efforts bring concrete results and lead to synergies at EU level. Commission actions in this area include:

- establishing 3 AI horizontal expert groups and **sectoral expert groups focused on specific AI policy areas** including **emerging security risks,**
- **steering discussions** on: standardization activities, the socioeconomic impact of AI, financing opportunities, measures to support start-ups, support for public-sector AI uptake, **AI and cybersecurity**, and AI and mobile connectivity,
- adopting 2020 the European Strategy for Data and proposing **Data Governance Act** (measures to **increase trust in data sharing** and aims at making more quality data available for AI applications),
- plans to adopt a **proposal for a Data Act** to stimulate the use of privately-held data by government (B2G),
- launching an **Industrial Alliance on Microelectronics** and investing in research and innovation for the computing needs of low-power edge AI.

2.4.2 Make the EU the Place where Excellence Thrives from the Lab to the Market

The development and deployment of AI technologies, in addition to data and computational infrastructure, also require horizontal actions, which cover a whole AI lifecycle:

- **Collaborate** with stakeholders through, e.g. the European Partnership on AI, Data and Robotics and expert groups,
- Build and mobilize **research capacities,**
- **Provide tools** for developers to **test and experiment** (TEFs), and for **AI uptake by SMEs and public administrations** (EDIH),
- Fund and scaling innovative ideas and solutions.

2.4.3 Ensure that AI Works for People and is a Force for Good in Society

The successful development and uptake of AI contribute to EU's economic growth and global competitiveness and bring enormous benefits to our society and the environment. However, some AI systems can **challenge rights protected by EU law**, **trigger safety and security concerns**, and **affect labour markets**. To address this challenge, the Commission identified the following areas:

- nurture talent and improve the supply of skills,
- develop a policy framework to ensure trust in AI systems,
- promote the EU vision on sustainable and trustworthy AI in the world.

Consultations with wide spectrum of stakeholders during development of policy actions to facilitate trust in AI included **establishing in 2020 by ENISA an Ad-Hoc Working Group on Artificial Intelligence Cybersecurity**, to address specific AI-related cybersecurity risks

EU Cybersecurity Strategy for the Digital Decade has been adopted in 2020. The Commission plans to further **strengthen cooperation with EU agencies and other relevant EU bodies working on AI**, including with **ENISA** and to establish **national, regional or sectoral Security Operation Centres (SOCs)**, which will be powered by AI and will constitute a **'cybersecurity shield' for the EU**

2.4.4 Build Strategic Leadership in High-Impact Sectors

The Coordinated Plan puts forward several **sectoral action areas**. The key proposal for building strategic leadership are:

- bring AI into play for climate and environment,
- use the next generation of AI to improve health,
- maintain Europe's lead: Strategy for Robotics in the world of AI,
- make the public sector a trailblazer for using AI,
- apply AI to law enforcement, migration and asylum,
- make mobility smarter, safer and more sustainable through AI,
- support AI for sustainable agriculture.