Bundesnetzagentur

SR on AI: final steps

Taras Holoyad (BNetzA, Germany)
AI Standardisation
Taras.Holoyad@bnetza.de

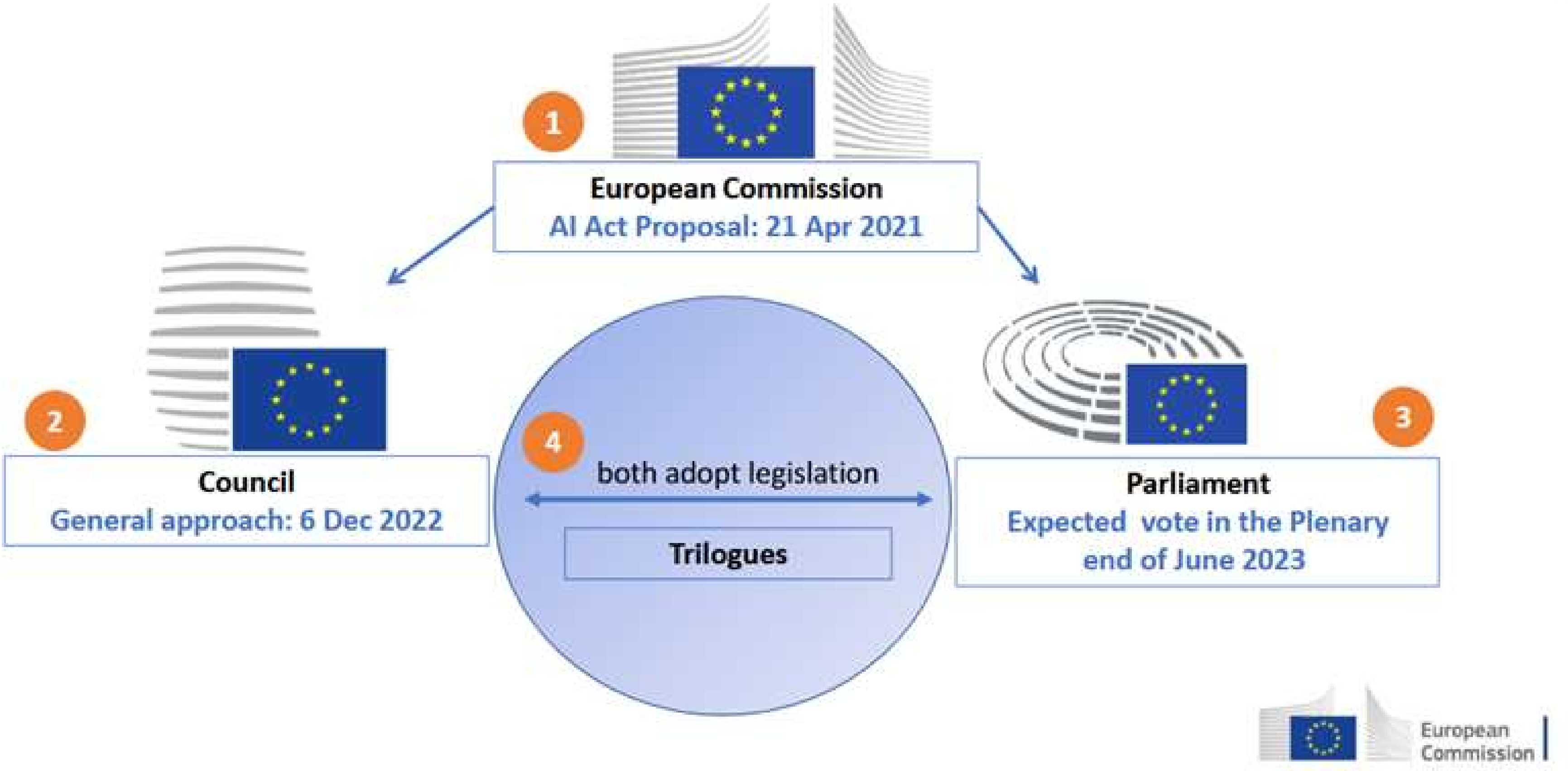
ETSI MTS #89
01.-02.06.2023

Content

- AI Act: State of Play
- CEN-CLC JTC 21: Response to SR on AI
- SR: Joint Work on Cybersecurity
- CEN-CLC JTC 21: Recent/upcoming projects
- Outlook

AI Act: State of Play

Ordinary legislative procedure



1

European Commission

AI Act Proposal: 21 Apr 2021

2

Council

General approach: 6 Dec 2022

3

Parliament

Expected vote in the Plenary end of June 2023

4

both adopt legislation

Trilogues

European Commission

Source: Dr. Tatjana Evas: Artificial Intelligence Act and Standardisation Work, 7th CEN-CENELEC JTC 21 Plenary , 22.05.2023

AI Act: State of Play

Council & Parliament: Overview of the positions and main changes

- Definition
- High-risk
- Accuracy, robustness & cybersecurity
- Obligations for providers of foundational models
- Common Specifications

Source: Dr. Tatjana Evas: Artificial Intelligence Act and Standardisation Work, 7th CEN-CENELEC JTC 21 Plenary , 22.05.2023

AI Act: State of Play (1/7)

Changes for term “AI system”: definition & removal of Annex 1

European Commission’s old AI Act draft from 04.2021

Definition:
“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.”

Council

- Focus on distinction between AI system and conventional software

Definition:
“means a system that is designed to operate with elements of autonomy and that, **based on machine and/or human-provided data and inputs**, **infers** how to achieve a given **set of objectives** using machine learning and/or **logic- and knowledge** based approaches, and produces system-generated outputs such as content (**generative AI systems**), **predictions**, recommendations or **decisions**, influencing the environments with which the AI system interacts.”

Parliament

- Focus on enlarging the scope

Definition:
“means a **machine-based** system that is designed to operate with varying **levels of autonomy** and that can, for explicit or implicit objectives, generate outputs such as **predictions**, recommendations, or decisions, that influence physical or virtual environments. “

Source: Dr. Tatjana Evas: Artificial Intelligence Act and Standardisation Work, 7th CEN-CENELEC JTC 21 Plenary , 22.05.2023

AI Act: State of Play (2/7)

Changes in requirements for high risk: use cases & filters

Council

- **Added** 2 use cases
  - health/life insurance;
  - digital infrastructure.

- **Deleted** 3 use cases:
  - **deep fake** detection, **crime** analytics & authenticity of travel. documents).

- **Added** a filter for high-risk classification based on
  - '**accessory**' nature of output with power for COM to adopt implementing act.

Parliament

- **Added** 8 use cases
  - health/life insurance;
  - digital infrastructure;
  - emotion recognition (when not prohibited);
  - student monitoring systems;
  - border management systems;
  - prediction of migrations trends/border crossings;
  - AI in elections;
  - recommender systems by very large social media platforms.

- **Added** a filter for high-risk classification based on
  - self-assessment by providers & consultation of national authorities.

Source: Dr. Tatjana Evas: Artificial Intelligence Act and Standardisation Work, 7th CEN-CENELEC JTC 21 Plenary , 22.05.2023

AI Act: State of Play (3/7)

Changes in requirements for high risk: use cases & filters

Council

Position aligned with COM, with minor adjustments

Parliament

Risk Management System:

- "Health or safety of natural persons, their fundamental rights including **equal access and opportunities**, democracy and rule of law or the environment when the high-risk AI system is used in accordance with its **intended purpose** and under conditions of **reasonably foreseeable misuse**".

Data:

- "Additional requirements related to transparency; measures for **detecting**, **preventing** and **mitigating** possible **biases** and conditions for data processing in view of detecting and examining negative biases."

Technical Documentation:

- **"Cybersecurity measures** in place";
- "A description of the **appropriateness** of the **performance metrics** for the specific AI system";
- "Information about **energy consumption** of the AI system during the development and expected energy consumption during use".

Record-keeping:

"High-risk AI systems shall be **designed** and **developed** with the **logging** capabilities enabling the recording of**energy consumption**, the measurement or calculation of **resource use and environmental impact** of the high-risk AI system during all phases of the system's lifecycle".

Source: Dr. Tatjana Evas: Artificial Intelligence Act and Standardisation Work, 7th CEN-CENELEC JTC 21 Plenary , 22.05.2023

AI Act: State of Play (4/7)

Obligations of providers of high-risk AI systems

Council

Position aligned with COM, with minor adjustments

Parliament

Additional obligations for providers (Art. 16)

- “provide **specifications** for **the input data**, or any other relevant **information** in terms of the **datasets** used, including their limitation and assumptions, taking into account the intended purpose and the foreseeable and reasonably **foreseeable misuses** of the AI system”;
- “Ensure that the high-risk AI system complies with accessibility requirements”.

Additional obligations on exchange of information/ technical documentation

- “required for the fulfilment of the **obligations** set in the **Regulation”**.

Source: Dr. Tatjana Evas: Artificial Intelligence Act and Standardisation Work, 7th CEN-CENELEC JTC 21 Plenary , 22.05.2023

AI Act: State of Play (5/7)

Parliament: Accuracy, robustness & cybersecurity

“Article 15: **Accuracy**, **robustness** and **cybersecurity**

1a.

*To address the technical aspects of how to measure the appropriate levels of **accuracy** and robustness set out in paragraph 1 of this Article, the **AI Office** shall bring together national and international **metrology and benchmarking authorities** and provide non-binding guidance on the matter as set out in Article 56, paragraph 2, point (a).”*

***“Article 56**: “Establishment of the European Artificial Intelligence Office”*

1. *The ‘European Artificial Intelligence Office’ (the ‘AI Office’) is hereby established. The AI Office shall be an independent body of the Union. It shall have legal personality;*

2. *The AI Office shall have a secretariat, and shall be adequately funded and staffed for the purpose of performing its tasks pursuant to this Regulation.“*

Source: Dr. Tatjana Evas: Artificial Intelligence Act and Standardisation Work, 7th CEN-CENELEC JTC 21 Plenary , 22.05.2023

AI Act: State of Play (6/7)

New Content: Foundational Models, General Purpose & Generative AI

Council:

- **"GPAI** to comply with requirements & obligations for **high-risk if AI system can be used in high-risk context** & **providers** of GPAI have to collaborate/**share information** with **downstream** providers".

Parliament:

- **"Foundation models** appear subject to requirements somewhat **inspired by high-risk**, but not aligned to them";

- **"Obligation** for the **provider of the foundational model** to "make use of applicable standards to reduce energy use, resource use and waste, as well as to increase energy efficiency, and the **overall efficiency of the system**.
  - ➢ *This shall be without prejudice to relevant existing Union and national law and this obligation shall not apply before the standards referred to in Article 40 are published. They shall be designed with capabilities enabling the measurement and logging of the consumption of energy and resources, and, where technically feasible, other environmental impact the deployment and use of the systems may have over their entire lifecycle."*

Source: Dr. Tatjana Evas: Artificial Intelligence Act and Standardisation Work, 7th CEN-CENELEC JTC 21 Plenary , 22.05.2023

AI Act: State of Play (7/7)

Common Specifications: **Parliament**

- **Article 41 (Common Specifications)**
  "The Commission **may** develop Common Specifications in case of, i.a.:
  - **Undue delays** in the establishment of an appropriate **standard;**
  - **Lack of compliance** with the requirements of the relevant EU legislation and/or standardisation request;
  - Specific fundamental **rights concerns."**

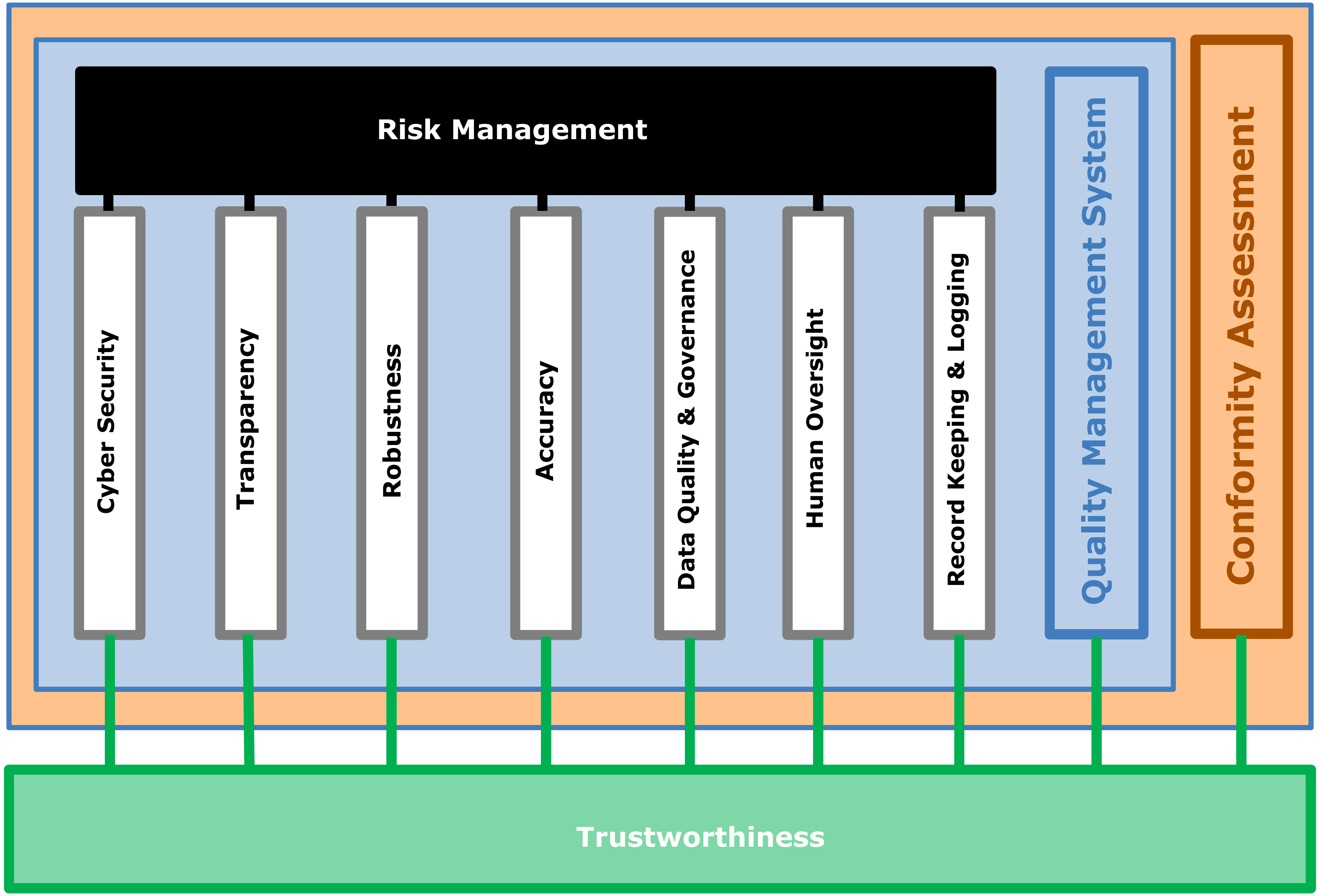
"The Commission **shall** develop Common Specifications

- For the methodology to fulfil the reporting and **documentation** requirement on the **consumption of energy** and **resources** during development, training and deployment of high risk AI systems."

Source: Dr. Tatjana Evas: Artificial Intelligence Act and Standardisation Work, 7th CEN-CENELEC JTC 21 Plenary , 22.05.2023

CEN-CLC JTC 21: Response to SR on AR

Architecture of CEN-CENELEC JTC 21 „Artificial Intelligence“:



Source: Draft response to Standardization Request, 7th CEN-CENELEC JTC 21 Plenary , 22.05.2023

SR: Joint Work on Cybersecurity (1/2)

Joint European work on cyber security

Coordinator for envisaged **joint work**
between CEN-CLC JTC 21, JTC 13, ENISA & ETSI:

- **Annegrit Seyerlein-Klug** (annegrit.seyerleinklug@th-brandenburg.de)

Joint Ad-hoc Group:

- prepare a proposal to develop cybersecurity standards for AI systems
- led by CEN-CENELEC JTC 21 under the CEN directives
- Members are
  - ➢ J-AHG Convenor from JTC 21 WGs; JTC 13 WGs;
  - ➢ J-AHG Vice-convenor from JTC 21 WGs; JTC 13 WGs;
  - ➢ Editors from JTC 21; JTC 13;
  - ➢ Experts from JTC 21; JTC 13; ETSI (TC CYBER, ISG SAI?) & ENISA.

Source: Draft ToR for AHG/Task Group on cybersecurity for AI systems, 7th CEN-CENELEC JTC 21 Plenary , 22.05.2023

SR: Joint Work on Cybersecurity (2/2)

Joint European work on cyber security

Envisaged topics:

- Information security AI management systems;
- Security threat analysis;
- Security requirements (Systems, products, services, people);
- Security conformity assessment methods;
- Security evaluation and testing methods;
- Security cryptography tools
  (homomorphic encryption, Identity based encryption, ...);
- Privacy risks identification and mitigation;
- Privacy by default requirements;
- Safety aspects and requirements for cybersecurity;
- Fundamental rights aspects for cybersecurity.

Source: Draft ToR for AHG/Task Group on cybersecurity for AI systems, 7th CEN-CENELEC JTC 21 Plenary , 22.05.2023

Recent Work Items in CEN-CENELEC JTC 21 “Artificial Intelligence”

Recent/upcoming projects in **committee**,
mostly parallel development with ISO/IEC JTC1/SC42:

- AI Risk Management;
- AI Checklist for Risk Management;
- Logging;
- Trustworthiness characterization;
- Accuracy of NLP systems;
- Data Governance and Data Quality for Artificial Intelligence;
- AI-enhanced nudge;
- Ethics;
- Robustness.

Adoption of

- ISO/IEC 12791 - Treatment of unwanted bias in classification and regression machine learning tasks;
- ISO/IEC 8183 - Information technology – Data life cycle framework.

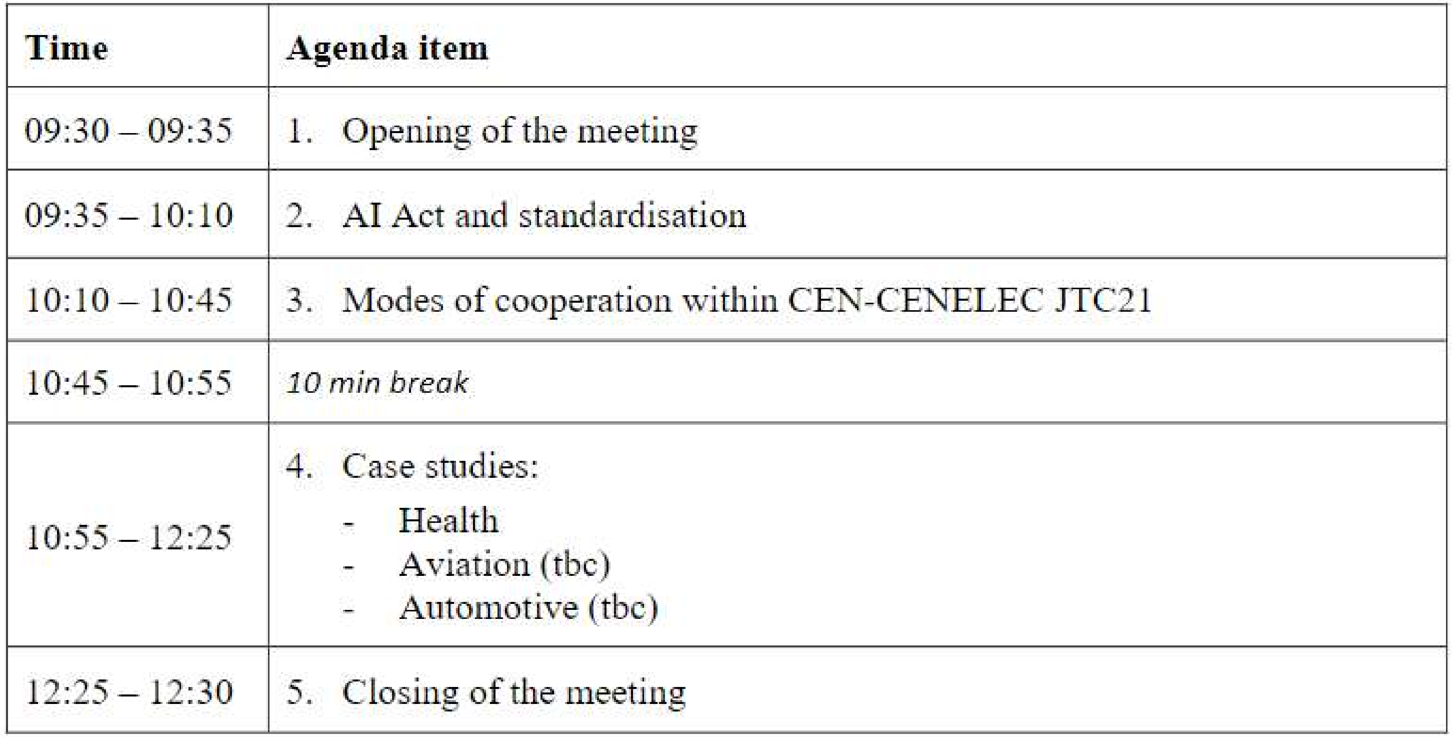
Source: 7th CEN-CENELEC JTC 21 Plenary , 22.05.2023

Outlook (1/2)

European Commission: Online Workshop on AI standardisation

Headline: “Exploring the interplay between horizontal and vertical standardisation deliverables”

Date: 7 June 2023, 9:30 – 12:30



Time	**Agenda item**
09:30 – 09:35	1. Opening of the meeting
09:35 – 10:10	2. AI Act and standardisation
10:10 – 10:45	3. Modes of cooperation within CEN-CENELEC JTC21
10:45 – 10:55	*10 min break*
10:55 – 12:25	4. Case studies: - Health - Aviation (tbc) - Automotive (tbc)
12:25 – 12:30	5. Closing of the meeting

Source: CEN-CENELEC JTC 21: Draft agenda for EC workshop on AI standardization, 25.05.2023.

Outlook (2/2)

Development of deliverables

- Timeline - deliverables by 30 April 2025
- Involvement of SMEs in CEN-CENELEC JTC 21
- Late engagement in ISO/IEC 42001 (Management system):
  - no opportunity to adopt our suggested changes to align with Art. 17
- No time to increase technical depth of essential AI QMS aspects,
  - e.g., post market monitoring
- Planned: homegrown / JTC21-led standards
  where ISO/IEC standards not aligned with AI Act, i.a.,
  - AI Risks - Check List for AI Risks Management;
  - Artificial Intelligence trustworthiness characterisation.

Source: Dr. Tatjana Evas: Artificial Intelligence Act and Standardisation Work, 7th CEN-CENELEC JTC 21 Plenary , 22.05.2023

Thank you for your attention!

Taras Holoyad (BNetzA, Germany)
AI Standardisation
Taras.Holoyad@bnetza.de

ETSI MTS #89
01.-02.06.2023