EUROPEAN
COMMISSION

Brussels, 22.5.2023
C(2023) 3215 final

ANNEXES 1 to 2

ANNEXES

to the

COMMISSION IMPLEMENTING DECISION

on a standardisation request to the European Committee for Standardisation and the European Committee for Electrotechnical Standardisation in support of Union policy on artificial intelligence

ANNEX I

List of new European Standards and European standardisation deliverables to be drafted

Reference information	
1.	European standard(s) and/or European standardisation deliverable(s) on risk management systems for AI systems
2.	European standard(s) and/or European standardisation deliverable(s) on governance and quality of datasets used to build AI systems
3.	European standard(s) and/or European standardisation deliverable(s) on record keeping through logging capabilities by AI systems
4.	European standard(s) and/or European standardisation deliverable(s) on transparency and information provisions for users of AI systems
5.	European standard(s) and/or European standardisation deliverable(s) on human oversight of AI systems
6.	European standard(s) and/or European standardisation deliverable(s) on accuracy specifications for AI systems
7.	European standard(s) and/or European standardisation deliverable(s) on robustness specifications for AI systems
8.	European standard(s) and/or European standardisation deliverable(s) on cybersecurity specifications for AI systems
9.	European standard(s) and/or European standardisation deliverable(s) on quality management systems for providers of AI systems, including post-market monitoring processes
10.	European standard(s) and/or European standardisation deliverable(s) on conformity assessment for AI systems

ANNEX II

Requirements for the European standards and European standardisation deliverables referred to in Article 1

1. Requirements for all European standards and European standardisation deliverables

European standards and European standardisation deliverables shall reflect the generally acknowledged state of the art in order to minimise risks to the health and safety and fundamental rights of persons as guaranteed in the Charter of Fundamental Rights of the European Union as well as in applicable EU law aiming to protect fundamental rights that arise from the design and development of AI systems in view of their intended purpose. State-of-the-art should be understood as a developed stage of technical capability at a given time as regards products, processes and services, based on the relevant consolidated findings of science, technology and experience and which is accepted as good practice in technology. The state of the art does not necessarily imply the latest scientific research still in an experimental stage or with insufficient technological maturity. To the purpose of ensuring that European standards and European standardisation deliverables are in line with Union law on fundamental rights and Union data protection law, CEN and CENELEC shall gather relevant expertise in those areas.

European standards and standardisation deliverables shall take into account, to the extent appropriate and without prejudice to the requirements of this Annex and to the safeguard of EU values and fundamental rights of persons as guaranteed in the Charter of Fundamental Rights of the European Union as well as in applicable EU law aiming to protect fundamental rights, international standardisation efforts. European Standards and European standardisation deliverables produced shall be consistent with the legal framework and international obligations of the Union.

The European standards and European standardiztion deliverables shall provide, to the necessary extent and taking into account the state of the art, technology-based, process-based or methodology-based technical specifications in relation to the design and development of AI systems, including verification, validation and testing procedures, objectively verifiable criteria and implementable methods to assess compliance with such specifications. Supporting specifications, including those on terminology, shall also be identified and provided when necessary to ensure the consistency and ability to implement the European standards and European standardisation deliverables. All the European Standards and European standardisation deliverables prepared on the basis of this request should rely on a common set of terms. Supporting specifications on terminology must build as much as possible on terminology adopted at international level and notably in international standards.

When drafting the European standards and European standardisation deliverables, specific account shall be taken of the risks which are common (horizontal) to the AI systems, including AI systems that continue to learn after being placed on the market or put into service, that the Commission has identified as posing a high-risk in the context of the proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).

Notwithstanding their general horizontal nature, European standards or European standardisation deliverables may provide specifications that concern certain specific AI systems (use cases) or sectors (“vertical specifications”), in consideration of the

intended purpose and/or context of use of those systems. While it is not always possible to develop European standards and European standardisation deliverables that consider each specific intended purpose, European standards and European standardisation deliverables shall cover at the minimum a range of technical solutions and options, which the manufacturer can assess and implement, taking into consideration the intended purpose of their specific system. European standards and European standardisation deliverables shall also possibly include guidance on how such assessment and implementation of solutions and options shall be executed.

In the fields of human oversight and accuracy, specific requirements for vertical specifications are laid down in Sections 2.5 and 2.6.

The European standards and European standardisation deliverables shall take into account as appropriate work produced by the European Telecommunications Standards Institute (ETSI), notably with regard to:

(a) preparation of the European standards and European standardisation deliverables referred to in point 8 of Annex I and integration of security aspects in the European standards and European standardisation deliverables listed in Annex I other than those referred to in its point 8;

(b) preparation and elaboration of possible vertical specifications;

(c) testing and validation procedures for AI systems.

To this purpose, CEN and CENELEC shall endeavour to establish appropriate modes of cooperation with ETSI.

The European standards and European standardisation deliverables produced shall take into account the interdependencies between the different requirements listed in Section 2, and to the extent possible, reflect them explicitly in the corresponding specifications.

CEN and CENELEC shall ensure that the European standards and European standardisation deliverables produced are, when applicable, consistent with existing and future European and general standards developed in the various relevant sectors, notably those related to products covered by existing Union safety legislation, including Directive 2001/95/EC on general product safety.

CEN and CENELEC shall take into due account that the areas covered by the European Standards and European standardisation deliverables may be the subject of a future standardisation request for harmonised standards in support of the Artificial Intelligence Act.

CEN and CENELEC shall ensure that the European standards and European standardisation deliverables are drafted in such a way so as to reflect an appropriate consideration of the specificities and costs of small and medium-sized enterprises, notably in relation to quality management systems and conformity assessments (Sections 2.9 and 2.10).

2. Requirements for specific European standards and European standardisation deliverables

2.1 Risk management system for AI systems

This (these) European standard(s) or European standardisation deliverable(s) shall set up specifications for a risk management system for AI systems. Risk management shall be intended as a continuous iterative process run throughout the entire lifecycle of the AI system, which is aimed at preventing or minimising the relevant risks to health, safety or fundamental rights.

Specifications shall be drafted in such a way that, for AI systems that are safety components of products, or that are themselves products, the risk management system aspects related to the AI system can, when applicable, be integrated with existing risk management systems established to meet requirements towards risk management systems contained in Union Harmonisation legislation listed in Annex II, Section A of the Artificial Intelligence Act proposal.

Specifications shall be drafted in such a way so as to enable usability by relevant operators and market surveillance authorities.

2.2 Data and data governance

This (these) European standard(s) or European standardisation deliverable(s) shall:

(a) Include specifications for appropriate data governance and data management procedures to be implemented by providers of AI systems (with specific focus on data generation and collection, data preparation operations, design choices, and procedures for detecting and addressing biases and potential for proxy discrimination or any other relevant shortcomings in data); and

(b) Include specifications on quality aspects of datasets used to train, validate and test AI systems (including representativeness, relevance, completeness and correctness).

2.3 Record keeping through logging capabilities

This (these) European standard(s) or European standardisation deliverable(s) shall include specifications for automatic logging of events for AI systems. Those specifications shall enable the traceability of those systems throughout their lifecycle and the monitoring of their operations and shall facilitate the post-market monitoring of the AI systems by providers.

2.4 Transparency and information to the users

This (these) European standard(s) or European standardisation deliverable(s) shall provide specifications related to:

(a) design and development solutions that ensure transparency of the operation of the AI system to enable users to understand the system’s output and use it appropriately; and

(b) instructions for use accompanying AI systems, including instructions on the system’s capabilities and limitations and on maintenance and care measures, taking into particular account:

(i) the need to identify and appropriately distinguish information, that is relevant and comprehensible for different professional user profiles and non professional users; and

(ii) without prejudice to point (i), the need to ensure that identified information is sufficient to enable users to interpret the system's output and use it appropriately in a way that mitigates risks.

2.5 Human oversight

This (these) European standard(s) or European standardisation deliverable(s) shall specify measures and procedures for human oversight of AI systems that are:

(a) identified and, when technically feasible, built into the AI system by the provider before it is placed on the market or put into service; and

(b) identified by the provider before placing the AI system on the market or putting it into service and which are appropriate to be implemented by the user.

These shall include measures enabling users to understand, monitor, interpret, assess and influence relevant aspects of the operation of the AI system.

This (these) European standard(s) or European standardisation deliverable(s) shall also establish, where justified, appropriate oversight measures that are specific to certain AI systems in consideration of their intended purpose. With respect to AI systems intended for remote biometric identification of persons, human oversight measures shall, inter alia, to provide for the possibility that no action or decision is taken by the user on the basis of the identification resulting from the system unless this has been separately verified and confirmed by at least two natural persons.

2.6 Accuracy specifications for AI systems

For the purpose of this (these) European standard(s) or European standardisation deliverable(s), "accuracy" shall be understood as referring to the capability of the AI system to perform the task for which it has been designed. This should not be confused with the narrower definition of statistical accuracy, which is one of several possible metrics for evaluating the performance of AI systems.

This (these) European standard(s) or European standardisation deliverable(s) shall lay down specifications for ensuring an appropriate level of accuracy of AI systems and for enabling providers to declare the relevant accuracy metrics and levels.

This (these) European standard(s) or European standardisation deliverable(s) shall also establish, where justified, a set of appropriate and relevant tools and metrics to measure accuracy against suitably defined levels, that are specific to certain AI systems in consideration of their intended purpose.

2.7 Robustness specifications for AI systems

This (these) European standard(s) or European standardisation deliverable(s) shall lay down specifications for the robustness of AI systems, taking into consideration relevant sources of errors, faults and inconsistencies, and the interactions of the AI system with the environment.

2.8 Cybersecurity specifications for AI systems

This (these) European standard(s) or European standardisation deliverable(s) shall provide suitable organisational and technical solutions, to ensure that AI systems are resilient against attempts to alter their use, behaviour, or performance or to compromise their security properties by malicious third parties exploiting the AI systems' vulnerabilities. Organisational and technical solutions shall therefore include, where appropriate, measures to prevent and control cyberattacks trying to manipulate AI specific assets, such as training data sets (e.g. data poisoning) or trained models (e.g. adversarial examples), or trying to exploit vulnerabilities in an AI system's digital assets or the underlying ICT infrastructure. These technical solutions shall be appropriate to the relevant circumstances and risks.

This (these) European standard(s) or European standardisation deliverable(s) shall take due account of the essential requirements for products with digital elements as listed in Sections 1 and 2 of Annex I to the proposal for a Regulation of the European Parliament and the Council on horizontal cybersecurity requirements for products with digital elements[1].

2.9 Quality management system for providers of AI systems, including post-market monitoring process

This (these) European standard(s) or European standardisation deliverable(s) shall lay down specifications for a quality management system to be implemented within their organisations by providers of AI systems. Such quality management systems shall ensure inter alia continous compliance of an AI system with the aspects described under points 2.2, 2.3, 2.4, 2.5, 2.6, 2.7 and 2.8. Appropriate consideration shall be given to the implementation of quality management system measures by small and medium-sized enterprises and organisations.

Specifications shall be drafted such that the quality management system aspects related to the AI system may be integrated into the overall management system of the provider, in particular with existing quality management systems established to meet requirements towards quality management systems contained in Union Harmonisation legislation listed in Annex II, Section A of the Artificial Intelligence Act proposal.

2.10 Conformity assessment for AI systems

This (these) European standard(s) or European standardisation deliverable(s) shall provide procedures and processes for conformity assessment activities related to AI systems and quality management systems of AI providers.

This (these) European standard(s) or European standardisation deliverable(s) shall also provide criteria for assessing the competence of persons tasked with the conformity assessment activities.

This (these) European standard(s) or European standardisation deliverable(s) shall consider both the scenarios whereby the conformity assessment is carried out by the

[1] COM (2022) 454 final of 15 September 2022.

provider itself or with the involvement of a professional external third-party organisation.