Huawei response on the European Commission's Proposal for a Regulation of the European Parliament and of the Council Laying Down the Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts

Huawei welcomes the opportunity to provide feedback on the European Commission's proposal for an Artificial Intelligence Act (hereinafter referred to as the "AI Act"), a crucial piece of legislation which will support the EU in fulfilling its digital ambitions, foster the single market, and consolidate Europe's position as a leader in the digital sphere.

With nearly 197,000 employees and operating in over 170 countries, Huawei – an independent private company fully owned by its employees – is a global player. Since the establishment of our first European R&D centre in Sweden 20 years ago, we have further invested and contributed to Europe's economic growth. Huawei currently employs over 14,000 employees in Europe, of which about 90% have been recruited in Europe/locally, and indirectly supports more than 224, 000 jobs, running two regional offices and 23 R&D sites. So far, Huawei has established 230 technical cooperation projects and has partnered with over 150 universities across Europe. Huawei's European operations generate significant contributions to social and public finance (taxes) in the EU in accordance with relevant national laws and regulations. Huawei's total contribution to the European GDP in 2019 accounted for €16.4 billion, growing by an average of 19.1% per year between 2015 and 2019.

We strongly support the Commission's objective to lay down harmonised rules for AI systems, in line with the guidelines presented by European Commission President Ursula von der Leyen to support the EU in being a global leader in the development of secure, trustworthy and ethical artificial intelligence. We are happy to see that this proposal is putting forward the much-needed legal framework addressing the risks of artificial intelligence. At Huawei, we believe AI developers, deployers and users would greatly benefit from such legal clarity, which in turn would ensure the wider take-up of artificial intelligence across Europe.

We recognise the Commission's success in producing the first ever draft legal framework on artificial intelligence, and we believe the proposal would benefit from further deliberations. We are pleased to participate in the discussion around this innovative proposal by submitting our feedback to the public consultation, and we very much look forward to working with the Commission and co-legislators to attain a fair, clear and practical outcome that works for all.

Our comments are structured along the following points:

1. Definitions concerning AI system
  1.1 Definition of AI system
  1.2 Definition of safety component of a product or system
  1.3 High-risk AI systems

2. Requirements for high-risk AI systems
  2.1 Data governance
  2.2 Post-market monitoring and surveillance
  2.3 Incidents reporting

1. Definitions concerning AI system
1.1 Definition of AI system

> **Article 3 Definitions**
> (1) 'artificial intelligence system' (AI system) means 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.
>
> **ANNEX I ARTIFICIAL INTELLIGENCE TECHNIQUES AND APPROACHES referred to in Article 3, point 1**
> (a) Machine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning;
>
> (b) Logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems;
>
> (c) Statistical approaches, Bayesian estimation, search and optimization methods.

While we recognise the desire to adopt a definition of AI system which is broad and future-proof, we consider that the definition proposed in the AI Act is too broad, and encompasses techniques which are not widely recognised to be related to artificial intelligence in the view of industrial and commercial practices.

Whilst "machine learning approaches" listed under category (a) in Annex I are intrinsically identified with AI, the approaches listed under category (c) are not unequivocally related to AI. For example, the "statistical approaches", "Bayesian estimation", and "search and optimisation methods" have been used for decades in a wide variety of applications. Not every search algorithm, not every optimisation method, and not every statistical calculation is an AI technique.

As such, we recommend that the Commission adopts a less broad definition of AI system in order to avoid unwarranted inclusion of non-AI systems within the scope of the regulation. In this respect, we recommend the removal of item (c) in Annex I.

1.2. Definition of safety component of a product or system

> **Article 3 Definitions**
> (14) 'safety component of a product or system' means a component of a product or of a system which fulfils a safety function for that product or system or the failure or malfunctioning of which endangers the health and safety of persons or property.

> **DIRECTIVE 2006/42/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 May 2006 on machinery, and amending Directive 95/16/EC (recast) (Text with EEA relevance)**
> **Article 2 Definitions**
>
> (c) 'safety component' means a component:
> — which serves to fulfil a safety function,
> — which is independently placed on the market,
> — the failure and/or malfunction of which endangers the safety of persons, and
> — which is not necessary in order for the machinery to function, or for which normal components may be substituted in order for the machinery to function.

We believe it is important that the assessment of a "safety component" refers back to Union harmonised legislation in Annex 2 in order to ensure the consistency with relevant regulatory requirements.

Taking a reference to the definition of safety component in the Machinery Directive, it emphasises the impact on human safety. It is recommended that the definition of "safety component" in AI Act should be designed to address the negative impact on human health and safety consistently, and not be extended to "property".

1.3 High-risk AI systems

> **ANNEX III HIGH-RISK AI SYSTEMS REFERRED TO IN ARTICLE 6(2)**
> High-risk AI systems pursuant to Article 6(2) are the AI systems listed in any of the following areas:
>
> 2. Management and operation of critical infrastructure: (a) AI systems intended to be used as safety components in the management and operation of road traffic and the supply of water, gas, heating and electricity.

In order to provide the needed legal certainty and ensure its implementation, it is suggested that the list of high-risk products or components of AI systems used in road traffic be clarified.

2. Requirements for high-risk AI systems
2.1 Data governance

> **CHAPTER 2**

> **REQUIREMENTS FOR HIGH-RISK AI SYSTEMS**
>
> **Article 10 Data and data governance**
> 3. Training, validation and testing data sets shall be relevant, representative, free of errors and complete. They shall have the appropriate statistical properties, including, where applicable, as regards the persons or groups of persons on which the high-risk AI system is intended to be used. These characteristics of the data sets may be met at the level of individual data sets or a combination thereof.

Data governance is an important aspect of the development and application of artificial intelligence systems, under which Article 10(3) requires the data sets to be "relevant, representative, free of errors and complete". However, the meaning of "completeness" may be obscure, since data sets are dynamic and new data can be continuously generated. Therefore, it's suggested that the "completeness" required of data sets be clarified and interpreted.

2.2 Post-market monitoring and surveillance

> **Article 29 Obligations of users of high-risk AI systems**
> 4. Users shall monitor the operation of the high-risk AI system on the basis of the instructions of use. When they have reasons to consider that the use in accordance with the instructions of use may result in the AI system presenting a risk within the meaning of Article 65(1) they shall inform the provider or distributor and suspend the use of the system. They shall also inform the provider or distributor when they have identified any serious incident or any malfunctioning within the meaning of Article 62 and interrupt the use of the AI system. In case the user is not able to reach the provider, Article 62 shall apply mutatis mutandis.
> For users that are credit institutions regulated by Directive 2013/36/EU, the monitoring obligation set out in the first subparagraph shall be deemed to be fulfilled by complying with the rules on internal governance arrangements, processes and mechanisms pursuant to Article 74 of that Directive.
>
> 6. Users of high-risk AI systems shall use the information provided under Article 13 to comply with their obligation to carry out a data protection impact assessment under Article 35 of Regulation (EU) 2016/679 or Article 27 of Directive (EU) 2016/680, where applicable.
>
> **Article 61 Post-market monitoring by providers and post-market monitoring plan for high-risk AI systems**
> 2. The post-market monitoring system shall actively and systematically collect, document and analyse relevant data provided by users or collected through other sources on the performance of high-risk AI systems throughout their lifetime, and allow the provider to

evaluate the continuous compliance of AI systems with the requirements set out in Title III, Chapter 2.

Article 65 Procedure for dealing with AI systems presenting a risk at national level
1. AI systems presenting a risk shall be understood as a product presenting a risk defined in Article 3, point 19 of Regulation (EU) 2019/1020 insofar as risks to the health or safety or to the protection of fundamental rights of persons are concerned.
2. Where the market surveillance authority of a Member State has sufficient reasons to consider that an AI system presents a risk as referred to in paragraph 1, they shall carry out an evaluation of the AI system concerned in respect of its compliance with all the requirements and obligations laid down in this Regulation. When risks to the protection of fundamental rights are present, the market surveillance authority shall also inform the relevant national public authorities or bodies referred to in Article 64(3). The relevant operators shall cooperate as necessary with the market surveillance authorities and the other national public authorities or bodies referred to in Article 64(3).

Where, in the course of that evaluation, the market surveillance authority finds that the AI system does not comply with the requirements and obligations laid down in this Regulation, it shall without delay require the relevant operator to take all appropriate corrective actions to bring the AI system into compliance, to withdraw the AI system from the market, or to recall it within a reasonable period, commensurate with the nature of the risk, as it may prescribe.

We welcome the post-market monitoring of AI systems, so as to promptly address the risks that may arise from the evolution of data statistical characteristics and continuous learning in the applications. We appreciate that the AI Act specifies corresponding requirements on the providers, the users, and market regulators. Different actors in the market work together in order to better address the impact of AI systems on safety and fundamental rights.

In general, we suggest that to the AI Act reflect the role of sector-specific regulators - and also of users and providers - set in their specific sectors (in particular where AI is used for various use cases, purposes and in different sectors).

To effectively implement existing laws and for consistency with sector-specific obligations, we suggest that the AI Act adopt existing EU legislative and regulatory framework, and include current sector-specific regulators as (possibly even main) regulatory authorities for AI in their specific domains. For example, relevant information relating to risks (e.g., as specified in Article 29(6) and Article 29(4)) could be provided by the users to the sector-specific regulators or their third-party representatives to enable them to analyse market monitoring information in order to periodically release and update known and foreseeable AI risks and concerns for each sector and to guide the users and providers to continuously improve their capability to tackle and prevent such specific risks.

2.3 Incidents reporting

Article 29 Obligations of users of high-risk AI systems
4. Users shall monitor the operation of the high-risk AI system on the basis of the instructions of use. When they have reasons to consider that the use in accordance with the instructions of use may result in the AI system presenting a risk within the meaning of Article 65(1) they shall inform the provider or distributor and suspend the use of the system. They shall also inform the provider or distributor when they have identified any serious incident or any malfunctioning within the meaning of Article 62 and interrupt the use of the AI system. In case the user is not able to reach the provider, Article 62 shall apply mutatis mutandis.
For users that are credit institutions regulated by Directive 2013/36/EU, the monitoring obligation set out in the first subparagraph shall be deemed to be fulfilled by complying with the rules on internal governance arrangements, processes and mechanisms pursuant to Article 74 of that Directive.

Article 62 Reporting of serious incidents and of malfunctioning
1. Providers of high-risk AI systems placed on the Union market shall report any serious incident or any malfunctioning of those systems which constitutes a breach of obligations under Union law intended to protect fundamental rights to the market surveillance authorities of the Member States where that incident or breach occurred.

Such notification shall be made immediately after the provider has established a causal link between the AI system and the incident or malfunctioning or the reasonable likelihood of such a link, and, in any event, not later than 15 days after the providers becomes aware of the serious incident or of the malfunctioning.

We welcome the requirement to report serious incidents and malfunctioning in the operation of AI systems, which will facilitate timely identification, addressing, and correction of the impact of AI systems on society. To this end, for the second sentence in Article 29 (4), we suggest the following revision: "They shall also inform the market surveillance authorities of the Member States, the provider or distributor…" Such notification could enable the market surveillance authority to inform other providers and users and, thereby, enhance their capability for a timely response to and correction of serious incidents and malfunctioning.

2.4 Information sharing

Chapter 3 Enforcement
Article 64 Access to data and documentation

> 2. Where necessary to assess the conformity of the high-risk AI system with the requirements set out in Title III, Chapter 2 and upon a reasoned request, the market surveillance authorities shall be granted access to the source code of the AI system.

Article 64(2) states that "Where necessary to assess the conformity of the high-risk AI system with the requirements set out in Title III, Chapter 2 and upon a reasoned request, the market surveillance authorities shall be granted access to the source code of the AI system." In this respect, it would be important that the AI Act or other legislations provide more guidance on how such disclosure of sensitive information will work to maintain confidentiality and meet the proportionality principle. Otherwise it may amount to a general obligation to disclose the source code for all high-risk AI systems.

In general, ensuring consistency with the overall EU legislative framework is key ranging from compliance with all data and record-keeping provisions of the GDPR, to the possibility for market surveillance authorities to request access to the source code of AI applications, where alignment with the spirit and the letter of the Trade Secrets Directive needs to be ensured.

3. Standards and organisations
3.1 Harmonised standards and common specifications

> **Article 40 Harmonised standards**
> High-risk AI systems which are in conformity with harmonised standards or parts thereof the references of which have been published in the Official Journal of the European Union shall be presumed to be in conformity with the requirements set out in Chapter 2 of this Title, to the extent those standards cover those requirements.
>
> **Article 41 Common specifications**
> 1. Where harmonised standards referred to in Article 40 do not exist or where the Commission considers that the relevant harmonised standards are insufficient or that there is a need to address specific safety or fundamental right concerns, the Commission may, by means of implementing acts, adopt common specifications in respect of the requirements set out in Chapter 2 of this Title. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 74(2).

We consider that harmonised standards developed by European SDOs and published in the OJEU are an essential cornerstone of the product regulatory framework in the EU. We are pleased that the Commission recognises the importance of harmonised standards, and sees these as central to its proposed product regulation framework in the context of AI systems.

In order to ensure that the harmonised standards (Article 40) are available when the regulation comes into force, standardisation requests to the SDOs shall be issued in a timely manner. With

reference to the EU's High Level Expert Group on Artificial Intelligence, the development of standards involves stakeholders such as industry representatives to provide industry expertise and experience on AI governance.

We are looking forward to the appropriate processes to be clarified and initiated when the case through collaborations with relevant standardisation bodies and a timeline are provided. All economic and societal actors in the AI supply chain can benefit also from more clarity regarding the specific situations when common specifications in Article 41 are required. This would also enable all economic actors to prepare the industrial processes accordingly in a timely manner.

With regards to 41(1), to the extent that relevant harmonised standards do not exist, or where they do exist but might be deemed to be insufficient, we recommend that the Commission issue mandates to European SDOs on a case-by-case basis to create or amend such harmonised standards, rather than creating common specifications itself via implementing acts. This is especially pertinent in cases where the standards address highly technical subjects, and would benefit from the experience and knowledge available in European SDOs.

3.2 Organisations

TITLE VI Governance, Chapter I Europe artificial intelligence board
Article 56 Establishment of the European Artificial Intelligence Board
1. A 'European Artificial Intelligence Board' (the 'Board') is established.

In Articles 56, 57 and 58 of the AI Act, the Commission sets out its plans for the establishment of a European Artificial Intelligence Board. We note that AI is a highly technical and specialised field, which involves a highly diverse and complex ecosystem and supply chain. While AI is still in its infancy, although widely adopted and deployed, it is important to ensure the balance between regulation and a high level of innovation and that we learn from ongoing experiences on the ground and adapt the rules for its regulation.

For the above reasons, we believe that the Commission will benefit from the expertise and experience of the industry in defining the governance of AI. We would recommend that the Commission formally allow the active participation of the industry in the Board's Expert Group when the group is created.

4. Others
4.1. Codes of conduct

TITLE IX Codes of conduct

> **Article 69 Codes of conduct**
> 1. The Commission and the Member States shall encourage and facilitate the drawing up of codes of conduct intended to foster the voluntary application to AI systems other than high-risk AI systems of the requirements set out in Title III, Chapter 2 on the basis of technical specifications and solutions that are appropriate means of ensuring compliance with such requirements in light of the intended purpose of the systems.

We are supportive of the Commission's view (Article 69) that the drawing up of voluntary codes of conduct by the industry should be encouraged for AI systems other than high-risk AI systems.

4.2 Digital skills

To reap the benefit of artificial intelligence, we believe it is necessary to have the industry working together with governments, local communities and other partners to improve the digital skills of individuals and society as a whole, and help SMEs enhance digital capabilities. We would advise the Commission to continue its excellent efforts in promoting the advancement of digital skills, as demonstrated by initiatives like the Digital Education Action Plan, the Digital skills and jobs coalition and many others.

A solid, future-proof education policy that fits the digital age and is fully inclusive is needed. We recommend that policy makers consider the following: focus on educating the future workforce, upskilling the current workforce, training the educators, and providing inclusive digital education. Huawei is active in the digital skills and education fields through activities aiming at building a digital talent ecosystem and developing digital inclusion and empowerment initiatives with measurable outcomes. Our initiatives include the ICT academy[1], TECH4ALL[2], and Seeds for the Future[3].

---

[1] A school-enterprise cooperation project training more than 45 ,000 students globally every year, including in Spain, Poland and Portugal.

[2] A project to develop digital inclusion and empowerment initiatives by leveraging cooperation with local governments, communities and organisations to bridge the technology talent gap. The project provides training in digital skills to equip people with the skills needed for employment.

[3] Huawei's flagship global CSR programme which helps enhance knowledge transfer, promote a greater understanding and interest in the telecommunications sector and participation in the digital community.