FEEDBACK TO EUROPEAN COMMISSION'S PROPOSED REGULATION ON ARTIFICIAL INTELLIGENCE

I. Hikvision and Artificial Intelligence:

Hangzhou Hikvision Digital Technology Co., Ltd and its affiliates ("**Hikvision**", "**we**") are leading providers of innovative security products in the EU ranging from public security to smart home security solutions. We welcome the opportunity to submit feedback to the European Commission's ("**EC**") proposed regulation on the use of artificial intelligence ("**AI**") in the EU ("**Proposed AI Regulation**").

Hikvision established its European headquarters in 2009 in the Netherlands. Today we employ more than 400 professionals across 20 European countries, and we have 17 Business Units in the EU. In 2019, we launched a Research & Development centre in the UK which develops software modifications to fit specific European customer needs.

We have many successful partnerships in Europe, where we support customers with their security needs. These include the Dun Laoghaire Harbour in Ireland, Milan's Malpensa Airport, IKEA shops in Spain, and light rail transit stations in Frankfurt. We are also a proud sponsor of the Dutch football club Ajax FC. We help them not only secure their stadium, but we also provide them with cutting-edge video and tactical analysis technology to support their games and trainings.

Our products are sold through a network of 600 distribution partners to more than 30,000 installation and integration companies across Europe. Many of these products incorporate AI technologies. We strongly believe that digital transformation, including AI, can be leveraged across a range of industries to protect not only private and public security interests, but also human, animal and ecological well-being as a whole.

AI technologies play an increasingly important role in nearly all aspects of everyday life, from national security, law enforcement, business, healthcare, education, culture, personal, environmental and property protection, and social networking. We are proud that our products make a positive difference for society, safeguarding people, places and assets, and providing important data and business intelligence for customers.

Technological innovation is our driving force and we continuously develop novel technologies using AI, such as facial recognition, biometrics, Big Data and deep learning. As a specialist in commercial video-surveillance we fully appreciate the privacy and fundamental rights' sensitivities and believe that individuals should not have to choose between safety and privacy. The use of AI is becoming more prevalent and as a company engaged in the deployment of products leveraging AI technologies, we witness first-hand the significant benefits such technologies can provide for Europe. In fact, demand for technology-driven innovation in the surveillance industry in Europe is high.

Hikvision believes that such AI technologies have the potential to be a catalyst for economic growth of the EU and supports the EU-wide common approach to regulation as proposed by the EC primarily as this would prevent fragmentation of the European Single Market for these novel technologies and facilitate the uptake of new technologies across the region.

Some of the highly valuable use-cases Hikvision has proposed and deployed in Europe are:

> *AI-powered surveillance technology for traffic management:* Hikvision's Traffic Flow System (with integrated AI technology) can be used by public administrations to efficiently manage traffic, identify congestion points, and improve traffic flows. Traffic congestion increases the amount of pollution produced by automobiles commuting through the city. As administrations look at ways to reduce carbon emissions, fluidifying and rationalizing traffic, the data collected by Hikvision's Traffic Flow System can help them reach this goal.

Access control authentication mechanisms: Hikvision's access control terminals enable companies to control access to and secure an environment, for example, limiting access to warehouse to employees - while also supporting multiple verification methods, for example, ID cards and PIN codes. These terminals can be equipped with facial recognition technology, in which case these systems compare a facial image to templates of images stored on site (by Hikvision's customer). This allows to authenticate an individual, but not to identify a person.

AI-powered in-car video recorders: Hikvision's mobile digital video recorders use AI technology to detect unusual driving behaviours via on-board network cameras. The system increases safety and limits potential incidents as the drivers are alerted in real-time – for instance if a driver was to fall asleep at the wheel.

People counting cameras: Hikvision's people counting cameras equipped with embedded deep learning algorithms enable companies to calculate the number of customers who enter the stores to match the number of staff during busy hours. The cameras can also be used to enforce the customer limits imposed by local authorities.

II. Hikvision's Support of the Proposed AI Regulation:

As also indicated in our submission to the EC's White Paper public consultation, we support the EC's initiative to create a standalone legislative framework for the use of AI in the EU and welcome the opportunity to submit feedback to the Proposed AI Regulation.

Hikvision supports in particular, the following aspects of the Proposed AI Regulation:

- **Risk-Based Regulatory Approach**: We recognise that AI systems can be deployed in many ways and across a variety of sectors, and as such, and with the exception of prohibited AI systems as set out below, we support the EC's approach to regulate AI systems in accordance with a four-tiered risk-based approach depending on how and where they are deployed. This approach allows stakeholders to focus on those AI systems that actually pose a risk to individuals' fundamental rights and freedoms, whilst not hindering technological development of low-risk AI systems and, more generally, the EU's desire to be at the forefront of digital innovation.

- **Conformity Assessments**: We agree with the EC's choice to subject high-risk AI systems[1] to a mandatory conformity assessment[2] procedure prior to being marketed in the EU – as is the case for many physical, tangible products under applicable EU product legislation. From a transparency perspective this will enable AI system users[3] and individuals to easily identify products which comply with applicable EU legislation and in turn, should enhance trust.

[1] For reference, the Proposed AI Regulation considers an AI system to be high-risk where (i) "*the AI system is intended to be used as a safety component of a product, or is itself a product covered by Union harmonisation legislation listed in Annex II*", e.g. medical device, and (ii) "*the product whose safety component is the AI system, or the AI system itself as a product, is required to undergo a third-party conformity assessment with a view to the placing on the market or putting into service of that product pursuant to the Union harmonisation legislation listed in Annex II*". In addition, AI systems referred to in Annex III are also considered high-risk. See Proposed AI Regulation, Art. 6.

[2] For reference, a "conformity assessment" is defined in the Proposed AI Regulation as: "*the process of verifying whether the requirements set out in Title III, Chapter 2 of this Regulation* [i.e. the requirements imposed on high-risk AI systems] *relating to an AI system have been fulfilled*".

[3] For reference, an AI system "user" is defined in the Proposed AI Regulation as: "*any natural or legal person, public authority, agency or other body using an AI system under its authority, except where the AI system is used in the course of a personal non-professional activity*".

- **Voluntary Codes of Conduct**: We support the approach proposed by the EC to not impose mandatory statutory requirements on the development and deployments of lower-risk AI systems and instead to offer AI system providers[4] the opportunity to voluntarily adhere to the above conformity assessments or codes of conduct to demonstrate compliance and potentially put such providers at a competitive advantage.

III. Hikvision's Suggestions for the Proposed AI Regulation:

As indicated above, Hikvision strongly supports the introduction of the Proposed AI Regulation. There are however, certain aspects of the Proposed AI Regulation which we consider would benefit from further consideration:

- **Scope of 'AI System' Definition**: The scope of the definition of an AI system[5] is in our view, too broad. *First*, the EC maintains the right to update the list of AI techniques in Annex I to the Proposed AI Regulation[6] but it is not clarified on the basis of which criteria or parameters this would be done. *Second*, an adequate determination of the techniques in Annex I is key for the definition of an 'AI system', because if they are not adequately determined, this will likely result in systems which are not in reality AI but which would nonetheless be captured by the definition. For example, thermostats (which adapt the temperature to a pre-determined temperature level) and cruise control on cars (which adapt a car's speed to the speed limit determined by the driver) are able to generate output and interact with their environment but do not necessarily function on the basis of one of the techniques listed in Annex I and as such would not be captured by the Proposed AI Regulation. *Third*, the definition is also dependent on the determination that a given system is 'able to' generate output – whereas in practice it may not systematically be clear *which* system is generating the output. For example, where a particular solution or product incorporates different types of software to function, it may not be clear which software is actually generating the output and falls within the definition of an 'AI system'.

  Lastly, the definition an 'AI system' should only capture AI systems which (negatively) impact individuals' fundamental rights and freedoms so as to limit the scope of application of the Proposed AI Regulation to such systems. The objective of the Proposed AI Regulation is to ensure that AI systems placed on the EU market are safe and respect EU fundamental rights' principles and values – however '*without unduly constraining or hindering technological development or otherwise disproportionately increasing the cost of placing AI solutions on the market*'[7]. In other words, the intention of the regulation is not (and should not be) to regulate AI systems which have little or no (negative) impact on individual fundamental rights – in particular as this may unduly hinder innovation. There are numerous applications of such AI systems for example, systems which are solely used to monitor and preserve wildlife and do not process personal data or otherwise have an effect on individuals. Furthermore, such

[4] For reference, an AI system "provider" is defined in the Proposed AI Regulation as: "*a natural or legal person, public authority, agency or other body that develops an AI system or that has an AI system developed with a view to placing it on the market or putting it into service under its own name or trademark, whether for payment or free of charge*".

[5] For reference, we include the definition of an AI system in the Proposed AI Regulation here: *"'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*" (Art. 3(1) Proposed AI Regulation).

[6] For reference, Annex I provides the following: "*(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*".

[7] See Proposed AI Regulation, Explanatory Memorandum, p. 1-3.

products and systems, when placed on the EU market, have to comply with general EU product safety regulations and would already be regulated.

The definition of an AI system is the most fundamental concept in the Proposed AI Regulation since it determines the scope of application and this should be specified further to enhance legal certainty.

- **Extraterritorial Scope:** We support the EC's proposal to regulate AI systems which could have an impact on individuals in the EU irrespective of the AI system provider's and user's establishment inside or outside the EU[8]. However, we believe that the extraterritorial scope is overly inclusive[9]. Art. 2(1)(c) of the Proposed AI Regulation provides that providers outside the EU are subject to the Regulation where their AI system's output[10] is 'used' in the EU – without qualifying this further. Providers are unable to exercise control over and are unable to ascertain and anticipate where their AI system's output will be used after they have placed the product on the market. In other words, a provider is unable control that the output of their AI system is not used in the EU (unless, for example, the provider is targeting the EU market in one way or another and can therefore reasonable expect that AI system's output will be used in the EU, and provided that such 'reasonable expectation' would be considered sufficient to meet this threshold). Without this type of clarification, 'providers' should be omitted from the Art. 2(1)(c) territorial application condition.

- **Scope of 'Provider' definition:** We welcome the EC's decision to define a significant amount of concepts in the Proposed AI Regulation. However, as is the case for the definition of an 'AI system', the definition of 'provider' would benefit from further clarification – in particular in situations where multiple stakeholders are involved in the development, provision and/or putting into service of an AI system and/or the product the AI system is incorporated in, and it may not be clear who the provider is.

- **Prohibited AI Systems**: Whilst we acknowledge the EC's intention in seeking to protect individuals' rights and freedoms by prohibiting certain specific AI system practices[11], we

[8] For reference, the Proposed AI Regulation's Explanatory Memorandum puts forward the following elements as the objectives to the Proposed AI Regulation regulatory framework: *"(i) ensure that AI systems placed on the Union market and used are safe and respect existing law on fundamental rights and Union values; (ii) ensure legal certainty to facilitate investment and innovation in AI; (iii) enhance governance and effective enforcement of existing law on fundamental rights and safety requirements applicable to AI systems; (iv) facilitate the development of a single market for lawful, safe and trustworthy AI applications and prevent market fragmentation*".

[9] For reference, we include the extraterritorial scope of application in Art. 2(1) of the Proposed AI Regulation here: "*This Regulation applies to (a) providers placing on the market or putting into service AI systems in the Union, irrespective of whether those providers are established within the Union or in a third country; (b) users of AI systems located within the Union; (c) providers and users of AI systems that are located in a third country, where the output produced by the system is used in the Union*" (emphasis added).

[10] For reference, AI system "output" is interpreted under the Proposed AI Regulation as "*content, predictions, recommendations or decisions which influence the environment with which the system interacts, be it in a physical or digital dimension*". See Proposed AI Regulation, Recital (6).

[11] For reference, the Proposed AI Regulation prohibits the following AI systems, Art. 5(1): *"(a) the placing on the market, putting into service or use of an AI system that deploys subliminal techniques beyond a person's consciousness in order to materially distort a person's behaviour in a manner that causes or is likely to cause that person or another person physical or psychological harm; (b) the placing on the market, putting into service or use of an AI system that exploits any of the vulnerabilities of a specific group of persons due to their age, physical or mental disability, in order to materially distort the behaviour of a person pertaining to that group in a manner that causes or is likely to cause that person or another person physical or psychological harm; (c) the placing on the market, putting into service or use of AI systems by public authorities or on their behalf for the evaluation or classification of the trustworthiness of natural persons over a certain period of time based on their social behaviour or known or predicted personal or personality characteristics, with the social score leading to either or both of the following: (i) detrimental or unfavourable treatment of certain natural persons or whole groups thereof in social contexts which are unrelated to the contexts in which the data was originally generated or collected; (ii) detrimental or unfavourable treatment of certain natural persons or whole groups thereof that is unjustified or*

consider that as proposed, the exemptions are too narrow and could result in unintended consequences and potentially prevent the use of certain AI systems which could be beneficial to society as a whole. In particular, we believe that the exemptions to the use of real-time remote biometric identification systems in public spaces[12] for law enforcement, are too narrow. The Proposed AI Regulation only permits use of AI systems for these purposes where such use is 'strictly necessary' for a limited number of objectives[13] which do not cover all law enforcement activity, such as the search of missing children, terrorist attacks and human trafficking. Further, each individual use of an AI system for this purpose must in principle be subject to prior judicial or administrative authorisation – which could inhibit the use of such AI systems. When used properly, AI technology has proven to be very valuable in law enforcement and can lead to more efficient and effective enforcement without having a disproportionate impact on individual rights. As such, we believe these exemptions should be expanded to the extent appropriate.

In addition, the concept of a 'publicly accessible space' should be narrowed in the Proposed AI Regulation. Currently, the regulation assumes that remote biometric identification in virtually all spaces accessible to the public (with or without entry restrictions) is 'particularly intrusive' to individual rights and freedoms, whereas in a large number of applications of remote biometric identification, individuals (should) have a reasonable expectation of being monitored and/or identified, for example for safety purposes in airports and other public transport. In turn, not all such monitoring would be particularly intrusive and should not be captured by the prohibition.

- **Requirements for High-Risk AI Systems:** Whilst we support the imposition of certain requirements[14] on the use of high-risk AI systems and we understand the ultimate goal i.e., to protect individual rights and freedoms, we consider that some of the requirements are overly burdensome and potentially duplicate requirements that already exist in current EU legislation, such as the obligation to implement a risk and quality management system, the data and data

disproportionate to their social behaviour or its gravity; (d) the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement, unless and in as far as such use is strictly necessary for one of the following objectives: (i) the targeted search for specific potential victims of crime, including missing children; (ii) the prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or of a terrorist attack; (iii) the detection, localisation, identification or prosecution of a perpetrator or suspect of a criminal offence referred to in Article 2(2) of Council/JHA62 Framework Decision 2002/584/ and punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least three years, as determined by the law of that Member State."

[12] For reference, "public spaces" are interpreted as follows in the Proposed AI Regulation, Recital 9: "*For the purposes of this Regulation the notion of publicly accessible space should be understood as referring to any physical place that is accessible to the public irrespective of whether the place in question is privately or publicly owned. Therefore, the notion does not cover places that are private in nature and normally not freely accessible for third parties, including law enforcement authorities, unless those parties have been specifically invited or authorised, such as homes, private clubs, offices, warehouses and factories. Online spaces are not covered either, as they are not physical spaces. However, the mere fact that certain conditions for accessing a particular space may apply, such as admission tickets or age restrictions, does not mean that the space is not publicly accessible within the meaning of this Regulation. Consequently, in addition to public spaces such as streets, relevant parts of government buildings and most transport infrastructure, spaces such as cinemas, theatres, shops and shopping centres are normally also publicly accessible. Whether a given space is accessible to the public should however be determined on a case-by- case basis, having regard to the specificities of the individual situation at hand.*" In turn, airports, for instance, are likely covered.

[13] Please refer to our footnote above for the list of objectives.

[14] For reference, the high-risk requirements under the Proposed AI Regulation can be summarized as follows: implementation of a risk and quality management system, data and data governance requirements, preparation of technical documentation and instructions of use, recordkeeping and automatic logging requirements, transparency requirements, human oversight requirements, accuracy, robustness and cybersecurity requirements, conformity assessment procedure requirements, registration requirements, take corrective action and/or notify, inform and cooperate with competent authorities in case of non-compliance, affix the CE marking, and otherwise demonstrate conformity of the AI system with the Regulation's requirements upon request of a competent authority. See Proposed AI Regulation, Title III.

governance requirements, preparation of technical documentation and instructions of use, recordkeeping and automatic logging requirements, and the establishment of a post-market monitoring system. In each case, we recommend that each requirement be assessed to ensure it is necessary to achieve the ultimate purpose of the Proposed AI Regulation i.e. to safeguard individual rights and freedoms and ensure the safety of AI systems but *also* to facilitate the development of a single market for AI systems and not hinder innovation. For instance, the data governance requirement in the Proposed AI Regulation[15] imposes an overly high standard on training, validation and testing data which are used to train AI models. Data sets are inherently imperfect and are unlikely to be able to meet this high standard. In practice, the various requirements under the Proposed AI Regulation often depend on the AI system's intended use[16] and as such would lead to overly burdensome customization and configuration of AI systems before they are being placed on the market – i.e. depending on the needs of the customer and the product's intended use. Companies will then also be required to develop, for example, customized instructions of use, software updates, and technical documentation for each of these customized products. Furthermore, it should be noted that the financial impact for high-risk AI system providers to comply with the Proposed AI Regulation is estimated at EUR 30,000 per AI system, which is significant and may have an impact on AI innovation[17].

- **Responsibility of Providers vs. Users:** As drafted, the user of an AI system becomes a provider of an AI system in instances where the user does not comply with the instructions of use prepared by the provider. Whilst we agree with this approach we are concerned that preparing exhaustive instructions of use that anticipate each and every use case by a user, is not realistic for a provider.

[15] See Proposed AI Regulation, Art. 10: "*High-risk AI systems which make use of techniques involving the training of models with data shall be developed on the basis of training, validation and testing data sets that meet the quality criteria referred to in paragraphs 2 to 5.* […]".

[16] This is also expressly recognized in the Proposed AI Regulation – see Art. 8(2): "*The intended purpose of the high-risk AI system […] shall be taken into account when ensuring compliance with those [high risk AI system] requirements.*"

[17] Study commissioned by the EU Commission, Study to Support an Impact Assessment of Regulatory Requirements for Artificial Intelligence in Europe, available at: https://op.europa.eu/en/publication-detail/-/publication/55538b70-a638-11eb-9585-01aa75ed71a1/language-en/format-PDF/source-204305195.