HIKVISION COMMENTS TO PUBLIC CONSULTATION ON THE EUROPEAN DATA PROTECTION BOARD'S DRAFT GUIDELINES ON THE CONCEPTS OF CONTROLLER AND PROCESSOR IN THE GDPR

I. Introduction:

Hangzhou Hikvision Digital Technology Co., Ltd is a leading provider of innovative IoT products in the European Union, ranging from public security to smart home solutions.

Today, Hikvision employs more than 40,000 dedicated professionals worldwide, and we are present in 59 countries and regions. Our products are being used in more than 150 countries and regions worldwide. In 2019, we reached EUR 7.6bn in global annual revenue.

Hikvision established its European headquarters in 2009 in Hoofddorp, near Amsterdam (the Netherlands). In Europe, we employ more than 400 professionals across 20 countries. We have launched a R&D centre in the UK in 2019 that can make software modifications to fit specific European customer needs and usage habits.

Hikvision takes data security and privacy very seriously. We develop and produce all our products with Security-by-Design and Privacy-by-Default in mind. Obligations under the EU General Data Protection Regulation ("**GDPR**") have a direct impact on our activities, both as a manufacturer of devices and solutions that will eventually process data, including sensitive data, and as a marketer providing solutions to users who will be in the position of data controller and/or processor.

As a responsible company operating in the European Union, we welcome the opportunity to respond to the public consultation on the European Data Protection Board's ("**EDPB**") draft Guidelines 07/2020 on the concepts of controller and processor under the GDPR ("**Guidelines**").

II. Support for the Guidelines:

As a leading provider of innovative technologies in the European Union, we believe that the correct designation of a party as either a controller, joint controller or processor is critical, to understand the obligations that each party has both from a regulatory perspective under the GDPR (including, in relation to the protection of individuals' rights) and contractually. The designation also determines the liability of a particular party under the GDPR. Whilst these are not new concepts under the GDPR, they are still concepts which are often not fully understood and applied. As such, Hikvision welcomes the publication of the Guidelines which provide practical guidance, both for our company as a manufacturer and for our customers, on the controller/processor distinction.

Hikvision supports in particular, the following aspects of the Guidelines:

- **Consistency in controller/joint controller and processor concepts across the European Economic Area ("EEA")**: Hikvision supports the recognition by the EDPB that the aforementioned concepts and the criteria for defining such concepts "*must be sufficiently clear and consistent*" throughout the EEA. The overall intention of the GDPR was to create a harmonised approach to data protection compliance across the EU and a lack of consistency in particular, in relation to core concepts makes it particularly challenging for multi-jurisdictional organisations such as Hikvision. As such, Hikvision strongly supports such a consistent approach.

- **Sufficient guarantees required from processors to controllers on security measures where processing personal data**: Hikvision supports the acknowledgement by the EDPB in the Guidelines of the importance of vendor information security and the recommendation that controllers carry out a risk assessment when engaging processors and throughout the contractual relationship, requiring processors to "*provide sufficient guarantees to implement*

appropriate technical and organisational measures so that the processing meets the requirements of the GDPR". As is the case with most multi-jurisdictional organisations, we also act as a processor when providing certain services to end-users, and welcome the reference to controllers providing processors with "*a clear and detailed description of the security measures to be implemented*" and "*minimum security objectives to be achieved*". This will enable service providers such as Hikvision to be able to respond to a concrete set of security objectives proposed by the controller and identify from the outset of contractual negotiations what security measures need to be implemented in relation to the processing activities under the data processing agreement.

- **Detailed controller instructions in relation to data processing by processors**: Hikvision welcomes the requirement in the Guidelines for controllers to provide detailed instructions in relation to the personal data processing, including "*permissible and unacceptable handling of personal data*" and "*ways of securing data*". We further support the provision of more detailed controller instructions, which will help ensure as processors it is clear from the point of entry into the data processing agreement what processing activities are requested by the controller in order to avoid processing outside of the remit of the controller's instructions and in turn breaching obligations under the GDPR.

- **Movement from 'pro-forma' restatement of Article 28 GDPR provisions**: Hikvision supports the recognition by the EDPB in the Guidelines that data processing agreements should not merely restate the Article 28 GDPR provisions but "*should include more specific, concrete information as to how the requirements will be met and which level of security is required for the personal data processing that is the object of the processing agreement*". We submit this provides processors with a greater level of awareness as to what processing requirements they are required to comply with, including security obligations, under the data processing agreements and in turn ensures its processing is carried out in compliance with the GDPR.

- **Greater clarity on circumstances where parties are considered joint controllers**: Hikvision strongly supports the helpful clarification in the Guidelines, building on Court of Justice of the European Union case law, on determining where both parties are joint controllers in relation to data processing. For example, we welcome the recognition that where both parties are "*inextricably linked*" and take "*converging decisions*" that "*complement each other and are necessary for the processing to take place in such manner that they have a tangible impact on the determination of the purposes and means of the processing*" both parties are joint controllers. Further, we welcome the helpful reference in the Guidelines to additional provisions that should be included in the joint controller agreement that provide further clarity and build on the provisions provided for in the GDPR, for example, inclusion of a legal basis for processing, security measures and the responsibility for carrying out data protection impact assessments.

III. Requests for Clarification

As referred to above, Hikvision strongly supports the publication of the Guidelines. There are however, certain areas of the Guidelines which we consider would benefit from further clarification:

- **Sufficient guarantees required from processors to controllers on security measures where processing personal data**: Hikvision submits the Guidelines would benefit from practical examples on how processors can provide sufficient guarantees to controllers in relation to appropriate organisational and technical security measures where processing personal data under data processing agreements. The Guidelines refer to an exchange of relevant information such as privacy policies, data processing records, external audits and information security policies. Given processors range from large multinational service providers to smaller

businesses, we suggest it would be helpful for further clarification on what 'guarantees' will be sufficient to satisfy the controller's risk assessment.

- **Amendments to processing provisions must be approved**: Hikvision recognises that as a matter of good practice modifications to data processing agreements by the processor should be notified and in turn approved by the controller. We note the reference in the guidelines to "*the mere publication of these modifications on the processor's website is not compliant with Article 28*". We would welcome further clarity on suggested notification measures, where for example, the processor is an online service platform with several individual customers or an app service provider with end-users across the EEA. We submit practical examples on what notification measures would be appropriate in this context would be useful.

- **Provision of additional information in the data processing agreement in order for the controller to be fully informed on the details of processing by the processor**: Hikvision recognises the importance of good data governance in relation to its personal data processing activities and those carried out on its behalf by its processors. We welcome the recognition in the Guidelines that the data processing agreement should "*include details on the flow of information between the processor and the controller*" in order for the controller to be "*fully informed as to the details of the processing*". We suggest it would be helpful if the Guidelines provide further clarification on the level of information that should be provided in the contract on the flow of information between the processor and the controller in order for the controller to be fully informed on the details of the processing and how the processing activity will be carried out by the processor.

IV. Conclusion

The Guidelines as drafted seek to further clarify the designation of parties as controllers, joint controllers or processors under the GDPR and in turn are crucial in determining the division of responsibilities for data processing, compliance with obligations under the GDPR and corresponding liabilities for non-compliance. Hikvision fully supports the position in the Guidelines that "*it is therefore of paramount importance that the precise meaning of these concepts and the criteria for their correct use are sufficiently clear and shared throughout the European Union and the EEA*". For example, we have carried out an assessment of our processing activities in the EEA and identified where we act as a controller and processor in order to ensure compliance with the GDPR with regard to the provision of our video surveillance products and solutions to customers and end-users. We would welcome the aforementioned additional clarifications which would serve to provide further practical guidance for processors on how to comply with the GDPR, in light of the additional compliance obligations imposed by the Guidelines.

With the increasing digitalisation of the society and growth in demand for internet-based solutions and Internet of Things (IoT) devices processing large amounts of personal data in multiple use-cases, Hikvision believes that any further clarification that helps streamline the application of the GDPR across the Member States of the European Union will greatly benefit the European Single Market. We therefore very much support the EDPB's efforts to provide further guidance on the application of the GDPR in the European Union.