Joint Declaration of the European Police Chiefs

as approved by the European Police Chiefs
during their informal meeting in Berlin on 24 May 2022

On 21 April 2021, the European Commission published a draft regulation designed to govern artificial intelligence *(Artificial Intelligence Act - "AI Act")*.

We, the European Police Chiefs, generally welcome the Commission's initiative for regulation, because rarely has a new technology been associated with as many opportunities and risks as artificial intelligence. However, in line with the objectives of the draft regulation, we would like to emphasise that the rules formulated could seriously affect police work and address the following particularly critical aspects:

1) AI is absolutely essential for police work

Given the fact that the number of crimes committed in digital space is increasing and that these offences already involve significant quantities of data - in the multi-digit terabyte range in individual investigations - the use of AI-supported tools and machine learning is indispensable for the successful fight against crime and the enforcement of the law. AI is an essential part of a high number of digital forensics and analysis tools, including commercial ones, which are currently used by law enforcement authorities to analyse ever-increasing volumes of data and extract digital evidence. Only through the use of AI will it be possible to respond to the ever-increasing data quantities to be analysed in an effective and efficient manner. Without the help of advanced technologies, we will not be able to stay abreast of the progressing digital transformation, to adequately analyse the rapidly increasing data volumes - frequently under particular time pressure - and to initiate necessary police measures to enforce the law and avert danger. For law enforcement to bring criminals to justice, mitigate crimes and adequately protect victims in the digital age, the use of AI-supported tools is not a choice but a necessity.

2) No disclosure of particularly sensitive data

The discharge of a significant proportion of police tasks involves the processing of particularly sensitive data, the disclosure of which is subject to certain restrictions and cannot be authorised on the basis of the decision-making powers of the police authorities alone.
Therefore, when rules regarding access to test and training data by third parties are laid down, it must be ensured that adequate consideration is given to the sensitivity of police data, for instance by excluding unrestricted remote access.

3) No blanket classification as high-risk

The risk-based approach advocated by the European Commission, which aims at counteracting the unregulated and uncontrolled development and application of this technology, is plausible. This must not, however, lead to a situation where entire areas of application affecting the security authorities are generally classified as high-risk and thus subjected to significant restrictions by default. The use of a fingerprint quality check algorithm created by machine learning, for instance, must not result in a blanket high-risk classification of the entire process. In fact, most of the AI applications used for law enforcement work in the European Union do not pose a high risk of harm to the health and safety and the fundamental rights and freedom of persons.

This is because, AI applications such as speech and text recognition (text classification, machine translation), information extraction (named entity recognition), object detection or image classification, are aimed at automating data pre-processing and processing tasks, so as to relieve human analysts from repetitive tasks and from exposure to gruesome materials, and allow them to focus on more cognitive tasks. These AI systems are used to support the work of criminal analysts faced with a dramatic increase in the number and size of structured and unstructured datasets, but they do not involve automatic decision-making.

The rules need to enable the specific evaluation on a case-by-case basis and the assessment of risk in the concrete individual case. In this context, it has to be borne in mind that the systems employed by security authorities are exclusively used in line with the relevant police powers and legal provisions and that they are already subject to rigorous control. These systems do not replace but only support investigative activities. The results achieved by the use of AI are always evaluated and checked by humans, i.e. specially trained and skilled police officers. Moreover, many AI-supported tools are applied to data that has been seized in the context of a criminal investigation, meaning there is no real-time dimension or indiscriminate analysis of data.

For this reason, we wish to formulate the following expectations of the future regulation of AI:

- The regulation must provide for exceptions applying to law enforcement authorities, which take sufficient account of the peculiarities and specific requirements of police tasks within the already existing legal framework as well as the realities of investigations in the digital age.

- The regulation must not lead to a situation where the police cannot use AI at all or only with considerable effort or delay. Therefore, suitable expedited procedures are needed to ensure that police tasks are performed effectively and without delay while ensuring the necessary checks and balances.

- The regulation must include relevant terms, definitions and phrases (e.g. mandatory, transparent, plausible, explicable), clearly define them in a legally reliable manner and must not be in conflict with existing tasks of the security authorities.

- The regulation and the definition of AI systems it contains must not lead to a situation where already established IT procedures, which thus far have not been generally considered as AI, fall within the scope of the regulation and may therefore no longer be used.

- The regulation must enable the concrete evaluation and assessment of risks in specific cases and must not make general provisions for a blanket classification of police systems involving AI as high-risk.

- The regulation must not contradict already established legislation with relevance for the police, particularly the existing data protection and data processing provisions, or result in a collision of pertinent legal norms.

- The regulation should also recognise the criminal use of AI and the need to empower law enforcement to investigate those “cyber-enabled” crimes.

We as the police welcome the European Commission's initiative to regulate AI. However, in order for the police to continue to effectively carry out the tasks assigned to it by law in the areas of crime control and law enforcement to offer protection to and provide security for all citizens living in the EU, it is essential that the rules to be adopted take into account the specific objectives and existing legal control

mechanisms regarding the use of AI by security authorities. At the same time, separate case-by-case assessments or exceptions should be provided for when it comes to these systems and cases of application. This is the only way to maintain the security authorities' capacity to act in the future in a digital environment which is characterised by the ever-increasing volumes of information including personal data.

Berlin, May 24th 2022