Council of the European Union
General Secretariat

PUBLIC

Brussels, 19 September 2022

WK 12224/2022 INIT

LIMITE

TELECOM

WORKING PAPER

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

CONTRIBUTION

From:	General Secretariat of the Council
To:	Working Party on Telecommunications and Information Society
Subject:	Artificial Intelligence Act - DE comments (ST 11124/22)

Delegations will find in the Annex the DE comments on Artificial Intelligence Act (ST 11124/22).

Deadline: ***2 September 2022***

Presidency compromise text for Artificial Intelligence Act (doc.11124/22)

Important: In order to guarantee that your comments appear accurately, please do not modify the table format by adding/removing/adjusting/merging/splitting cells and rows. This would hinder the consolidation of your comments. When adding new provisions, please use the free rows provided for this purpose between the provisions. You can add multiple provisions in one row, if necessary, but do not add or remove rows. For drafting suggestions (2nd column), please copy the relevant sentence or sentences from a given paragraph or point into the second column and add or remove text. Please do not use track changes, but highlight your additions in yellow or use ~~strikethrough~~ to indicate deletions. You do not need to copy entire paragraphs or points to indicate your changes, copying and modifying the relevant sentences is sufficient. For comments on specific provisions, please insert your remarks in the 3rd column in the relevant row. If you wish to make general comments on the entire proposal, please do so in the row containing the title of the proposal (in the 3rd column).

PUBLIC

Presidency second compromise text **Doc. 11124/22**	**Drafting Suggestions**	**Comments**
Proposal for a **REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS**		DEU reserves the right to an in-depth comment regarding biometric identification systems at a later stage, final discussions are still ongoing. Please note that the following views are preliminary as we are still examining the proposal. We reserve the right to make further comments.
(Text with EEA relevance)		

PUBLIC

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,		
Having regard to the Treaty on the Functioning of the European Union, and in particular Articles 16 and 114 thereof,		
Having regard to the proposal from the European Commission,		
After transmission of the draft legislative act to the national parliaments,		
Having regard to the opinion of the European Economic and Social Committee[1],		
Having regard to the opinion of the Committee		

[1] OJ C […], […], p. […].

PUBLIC

of the Regions[2],		
Having regard to the opinion of the European Central Bank[3],		
Acting in accordance with the ordinary legislative procedure,		
Whereas:		
(1) The purpose of this Regulation is to improve the functioning of the internal market by laying down a uniform legal framework in particular for the development, marketing and use of artificial intelligence in conformity with Union values. This Regulation pursues a number of overriding reasons of public interest, such as a high level of protection of health,		

[2] OJ C […], […], p. […].
[3] Reference to ECB opinion

PUBLIC

safety and fundamental rights, and it ensures the free movement of AI-based goods and services cross-border, thus preventing Member States from imposing restrictions on the development, marketing and use of AI systems, unless explicitly authorised by this Regulation.		
(2) Artificial intelligence systems (AI systems) can be easily deployed in multiple sectors of the economy and society, including cross border, and circulate throughout the Union. Certain Member States have already explored the adoption of national rules to ensure that artificial intelligence is safe and is developed and used in compliance with fundamental rights obligations. Differing national rules may lead to fragmentation of the internal market and decrease legal certainty for operators that develop or use AI systems. A consistent and high level of protection throughout the Union should therefore be		

PUBLIC

ensured, while divergences hampering the free circulation of AI systems and related products and services within the internal market should be prevented, by laying down uniform obligations for operators and guaranteeing the uniform protection of overriding reasons of public interest and of rights of persons throughout the internal market based on Article 114 of the Treaty on the Functioning of the European Union (TFEU). To the extent that this Regulation contains specific rules on the protection of individuals with regard to the processing of personal data concerning restrictions of the use of AI systems for 'real-time' ~~remote~~ biometric identification in publicly accessible spaces for the purpose of law enforcement, it is appropriate to base this Regulation, in as far as those specific rules are concerned, on Article 16 of the TFEU. In light of those specific rules and the recourse to Article 16 TFEU, it is appropriate to consult the		

PUBLIC

European Data Protection Board.		
(3) Artificial intelligence is a fast evolving family of technologies that can contribute to a wide array of economic and societal benefits across the entire spectrum of industries and social activities. By improving prediction, optimising operations and resource allocation, and personalising digital solutions available for individuals and organisations, the use of artificial intelligence can provide key competitive advantages to companies and support socially and environmentally beneficial outcomes, for example in healthcare, farming, education and training, infrastructure management, energy, transport and logistics, public services, security, justice, resource and energy efficiency, and climate change mitigation and adaptation.		
(4) At the same time, depending on the		

PUBLIC

circumstances regarding its specific application and use, artificial intelligence may generate risks and cause harm to public interests and rights that are protected by Union law. Such harm might be material or immaterial.		
(5) A Union legal framework laying down harmonised rules on artificial intelligence is therefore needed to foster the development, use and uptake of artificial intelligence in the internal market that at the same time meets a high level of protection of public interests, such as health and safety and the protection of fundamental rights, as recognised and protected by Union law. To achieve that objective, rules regulating the placing on the market and putting into service of certain AI systems should be laid down, thus ensuring the smooth functioning of the internal market and allowing those systems to benefit from the principle of free movement of goods and services. By laying down those		

PUBLIC

rules, this Regulation supports the objective of the Union of being a global leader in the development of secure, trustworthy and ethical artificial intelligence, as stated by the European Council[4], and it ensures the protection of ethical principles, as specifically requested by the European Parliament[5].		
(5a) The harmonised rules laid down in this Regulation should apply across sectors without prejudice to existing Union law, and in particular without prejudice to Union law on data protection, consumer protection, product safety and employment. This Regulation is intended to regulate AI systems that are to be placed on the market and put into service in the Union and it should complement such existing Union law.	**The harmonised rules laid down in this Regulation should apply across sectors without prejudice to existing Union law, and in particular without prejudice to Union law on data protection including any supplementing provisions of national law, consumer protection, product**	We appreciate these further clarifications concerning the relationship between this Regulation and data protection law, but we suggest to include any supplementing provisions of national law clearlier within the whole Regulation (see Recital 58a, for example Recital 9).

4 European Council, Special meeting of the European Council (1 and 2 October 2020) – Conclusions, EUCO 13/20, 2020, p. 6.

5 European Parliament resolution of 20 October 2020 with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies, 2020/2012(INL).

PUBLIC

	safety and employment.	
(6) The notion of AI system should be clearly defined to ensure legal certainty, while providing the flexibility to accommodate future technological developments. The definition should be based on ~~the~~ key functional characteristics ~~of the software~~ **of artificial intelligence distinguishing it from more classic software systems and programming.** ~~,~~ ~~i~~**I**n particular**, for the purposes of this Regulation AI systems should ~~be intended as~~ have~~ing~~** the ability, **on the basis of machine and/or human-based data and inputs, to infer the way to achieve a given set of human-defined objectives using machine learning and/or logic- and knowledge based approaches ~~through learning, reasoning or modelling~~ and to** ~~for a given set of human-defined objectives, to~~ ~~generate~~ **produce ~~specific~~** outputs ~~**in the form of**~~ ~~such as~~ **such as**		

PUBLIC

content **for generative AI systems (e.g. ~~such as~~ text, video or images)**, **~~as well as~~** predictions, recommendations~~,~~ or decisions**,** ~~which~~ influenc**ing** the environment with which the system interacts, be it in a physical or digital dimension. **A system that uses rules defined solely by natural persons to automatically execute operations should not be considered an AI system.** AI systems can be designed to operate with varying levels of autonomy and be used on a stand-alone basis or as a component of a product, irrespective of whether the system is physically integrated into the product (embedded) or serve the functionality of the product without being integrated therein (non-embedded).		
(6a) Machine learning approaches focus on the development of systems capable of learning from data to solve an application problem without being explicitly		

PUBLIC

programmed with a set of step-by-step instructions from input to output. Learning refers to the computational process of optimizing from data the parameters of the model, which is a mathematical construct generating an output based on input data. The range of problems addressed by machine learning typically involves tasks for which other approaches fail, either because there is no suitable formalisation of the problem, or because the resolution of the problem is intractable with non-learning approaches. Machine learning approaches include for instance supervised, unsupervised and reinforcement learning, using a variety of methods including deep learning, statistical techniques for learning and inference (including Bayesian estimation) and search and optimisation methods.		
(6b) Logic- and knowledge based	**6b) Logic- and knowledge based**	Editorial changes to improve readability

PUBLIC

approaches focus on the development of systems with logical reasoning capabilities on knowledge to solve an application problem. Such systems typically involve a knowledge base and an inference engine that generates outputs by reasoning on the knowledge base. The knowledge base, which is usually encoded by human experts, represents entities and logical relationships relevant for the application problem through formalisms based on rules, ontologies, or knowledge graphs. The inference engine acts on the knowledge base and extracts new information through operations such as sorting, searching, matching or chaining. Logic- and knowledge based approaches include for instance knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning, expert systems and search and optimisation	**approaches focus on the development of systems with logical reasoning capabilities on knowledge to solve an application problem. Such systems typically involve a knowledge base and an inference engine that generates outputs by reasoning on the knowledge base. The knowledge base, which is usually encoded by human experts, represents entities and logical relationships relevant for the application problem through formalisms based on rules, ontologies, or knowledge graphs. The inference engine acts on the knowledge base and extracts new information through operations such as sorting, searching, matching or chaining. Logic- and**	and to avoid misunderstandings due to an enumeration of processes, which are already regulated by European or national law.

PUBLIC

methods.	**knowledge based approaches include for instance knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines~~. (symbolic) reasoning, expert systems and search and optimisation methods.~~**	
(6c) In order to ensure uniform conditions for the implementation of this Regulation as regards machine learning approaches and logic- and knowledged based approaches and to take account of ~~The definition of AI system should be complemented by a list of specific techniques and approaches used for its development, which should be kept up-to- date in the light of~~ market and technological developments**, implementing powers should be conferred on the Commission.**~~through the adoption of delegated acts by the Commission~~		

PUBLIC

~~to amend that list.~~		
(7) The notion of biometric data used in this Regulation ~~is in line with and~~ should be interpreted consistently with the notion of biometric data as defined in Article 4(14) of Regulation (EU) 2016/679 of the European Parliament and of the Council[6], Article 3(18) of Regulation (EU) 2018/1725 of the European Parliament and of the Council[7] and Article 3(13) of Directive (EU) 2016/680 of the European Parliament and of the Council[8].		
(8) The notion of ~~remote~~ biometric identification system as used in this Regulation		DEU reserves the right to an in-depth

[6] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

[7] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39)

[8] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (Law Enforcement Directive) (*OJ L 119, 4.5.2016, p. 89).*

PUBLIC

should be defined functionally, as an AI system intended for the identification of natural persons ~~**at a distance**~~ through the comparison of a person's biometric data with the biometric data contained in a reference ~~database~~ **data repository,** irrespectively of the particular technology, processes or types of biometric data used**. Such a definition excludes verification/authentification systems whose sole purpose would be to confirm that a specific natural person is the person he or she claims to be, as well as systems that are used to confirm the identity of a natural person for the sole purpose of having access to a service, a device or premises. This exclusion is justified by the fact that such systems are likely to have a minor impact on fundamental rights of natural persons compared to biometric identification systems which may be used for the processing of the biometric data of a large number of persons.** ~~**and**~~		comment regarding biometric identification systems at a later stage, final discussions are still ongoing.

PUBLIC

~~**without prior knowledge whether the targeted person will be present and can be identified**~~. ~~**Considering their different characteristics and manners in which they are used, as well as the different risks involved, a distinction should be made between 'real-time' and 'post' remote biometric identification systems.**~~ In the case of 'real-time' systems, the capturing of the biometric data, the comparison and the identification occur all instantaneously, near-instantaneously or in any event without a significant delay. In this regard, there should be no scope for circumventing the rules of this Regulation on the 'real-time' use of the AI systems in question by providing for minor delays. 'Real-time' systems involve the use of 'live' or 'near-'live' material, such as video footage, generated by a camera or other device with similar functionality. In the case of 'post' systems, in contrast, the biometric data have		

PUBLIC

already been captured and the comparison and identification occur only after a significant delay. This involves material, such as pictures or video footage generated by closed circuit television cameras or private devices, which has been generated before the use of the system in respect of the natural persons concerned.		
(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 **an undetermined number of natural persons** ~~the public~~, **and irrespective of whether the place in question is privately or publicly owned. and irrepective of the activity for which the place may be used, such as commerce (for instance, shops, restaurants, cafés), services (for instance, banks, professional activities, hospitality), sport (for instance, swimming pools, gyms, stadiums), transport (for instance, bus, metro**		Should the assumption, that „Publicly accessible spaces should not include [...] border control areas", be included in the articles of the AI Act (Art. 3 (39)), not just the recitals?

PUBLIC

and railway stations, airports, means of transport), entertainment (for instance, cinemas, theatres, museums, concert and conference halls) leisure or otherwise (for instance, public roads and squares, parks, forests, playgrounds). A place should be classified as publicly accessible also if, regardless of potential capacity or security restrictions, access is subject to certain predetermined conditions, which can be fulfilled by an undetermined number of persons, such as purchase of a ticket or title of transport, prior registration or having a certain age. By contrast, a place should not be considered publicly accessible if access is limited to specific and defined natural persons through either Union or national law directly related to public safety or security or through the clear manifestation of will by the person having the relevant authority on the place. The factual possibility of access alone		

PUBLIC

(e.g. an unlocked door, an open gate in a fence) does not imply that the place is publicly accessible in the presence of indications or circumstances suggesting the contrary (e.g. signs prohibiting or restricting access). Company and factory premises as well as offices and workplaces that are intended to be accessed only by relevant employees and service providers are places that are not publicly accessible. Publicly accessible spaces should not include prisons or border control areas. Some other areas may be composed of both not publicly accessible and publicly accessible areas, such as the hallway of a private residential building necessary to access a doctor's office or an airport. ~~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~~		

PUBLIC

~~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.		
(10) In order to ensure a level playing field and an effective protection of rights and freedoms of		

PUBLIC

individuals across the Union, the rules established by this Regulation should apply to providers of AI systems in a non-discriminatory manner, irrespective of whether they are established within the Union or in a third country, and to users of AI systems established within the Union.		
(11) In light of their digital nature, certain AI systems should fall within the scope of this Regulation even when they are neither placed on the market, nor put into service, nor used in the Union. This is the case for example of an operator established in the Union that contracts certain services to an operator established outside the Union in relation to an activity to be performed by an AI system that would qualify as high-risk ~~and whose effects impact natural persons located in the Union~~. In those circumstances, the AI system used by the operator outside the Union could process data		

PUBLIC

lawfully collected in and transferred from the Union, and provide to the contracting operator in the Union the output of that AI system resulting from that processing, without that AI system being placed on the market, put into service or used in the Union. To prevent the circumvention of this Regulation and to ensure an effective protection of natural persons located in the Union, this Regulation should also apply to providers and users of AI systems that are established in a third country, to the extent the output produced by those systems is used in the Union. Nonetheless, to take into account existing arrangements and special needs for **future** cooperation with foreign partners with whom information and evidence is exchanged, this Regulation should not apply to public authorities of a third country and international organisations when acting in the framework of international agreements concluded at national or European level for law enforcement and		

PUBLIC

judicial cooperation with the Union or with its Member States. Such agreements have been concluded bilaterally between Member States and third countries or between the European Union, Europol and other EU agencies and third countries and international organisations. **Recipient Member States authorities and Union institutions, offices, bodies and bodies making use of such outputs in the Union remain accountable to ensure their use comply with Union law. When those international agreements are revised or new ones are concluded in the future, the contracting parties should undertake the utmost effort to align those agreements with the requirements of this Regulation.**		
(12) This Regulation should also apply to Union institutions, offices, bodies and agencies when acting as a provider or user of an AI system. **If and insofar** AI systems **are**		

PUBLIC

~~[exclusively]developed~~ **placed on the market or put into service** ~~or used~~ for military **or defence** purposes**, those** should be excluded from the scope of this Regulation **regardless of which type of entity is carrying out those activities, such as whether it is a public or private entity**. **Such exclusion is justified by the specifities of the Member States' and the common Union defence policy subject to public international law, which is therefore the more appropriate legal framework for the regulation of AI systems in the context of the use of lethal force and other AI systems in the context of military and defence activities. Nonetheless, if an AI system ~~developed placed on the market or put into service exclusively~~ for military or defence purposes is used outside those purposes (for example, civilian or humanitarian purposes), such a system would fall within the scope of this Regulation. In that case, the entity using the**		

PUBLIC

system for other than military or defence purposes should ensure compliance of the system with this Regulation, unless the system is already compliant with this Regulation. AI systems placed on the market or put into service for both military or defence and civilian purposes fall within the scope of this Regulation and providers of those systems should ensure compliance with this Regulation. ~~where that use falls under the exclusive remit of the Common Foreign and Security Policy regulated under Title V of the Treaty on the European Union (TEU).~~ **If and insofar ~~When~~ AI systems are ~~exclusively developed~~ placed on the market or put into service ~~or used~~ for national security purposes, they should also be excluded from the scope of the Regulation, regardless of which type of entity is carrying out those activities, such as whether it is a public or private entity.** ~~taking into account~~ **Such**		

PUBLIC

exclusion is justified both by the fact that national security remains the sole responsibility of Member States in accordance with Article 4(2) TEU and by the specific nature and operational needs of national security activities and specific national rules applicable to those activities. Nonetheless, if an AI system placed on the market or put into service for national security purposes is used outside those purposes (for example, for safeguarding public security or for law enforcement), such a system would fall within the scope of this Regulation. In that case, the entity using the system for other than national security purposes should ensure compliance of the system with this Regulation, unless the system is already compliant with this Regulation. AI systems placed on the market or put into service for both national security and other purposes, including law		

PUBLIC

enforcement, fall within the scope of this Regulation and providers of those systems should ensure compliance. In those cases, the fact that an AI system may fall within the scope of this Regulation should not affect the possibility of the national security and defence agencies and entities acting on their behalf to use that AI system for national security, military and defence purposes.		
(12a) This Regulation should be without prejudice to the provisions regarding the liability of intermediary service providers set out in Directive 2000/31/EC of the European Parliament and of the Council [as amended by the Digital Services Act].		
(12~~a~~b) This Regulation should not undermine research and development activity and should respect freedom of science. It is therefore necessary to exclude		

PUBLIC

from its scope AI systems specifically developed and put into service for the sole purpose of scientific research and development and to ensure that the Regulation does not otherwise affect scientific research and development activity on AI systems. As regards product oriented research activity by providers, the provisions of this Regulation should apply insofar as such research leads to or entails placing an AI system on the market or putting it into service. Furthermore, without prejudice to the foregoing regarding AI systems specifically developed and put into service for the sole purpose of scientific research and development, any other AI system that may be used for the conduct of any reaserch and development activity should remain subject to the provisions of this Regulation. Under all circumstances, any research and development activity should be carried out in		

PUBLIC

accordance with recognised ethical standards for scientific research.		
(12aa) In the light of the nature and complexity of the value chain for AI systems, it is essential to clarify the role of actors who may contribute to the development of AI systems. In particular, it is necessary to clarify that general purpose AI systems are AI systems that are intended by the provider to perform generally applicable functions, such as image/speech recognition, and in a plurality of contexts. They may be used as high risk AI systems by themselves or be components of other high risk AI systems. Therefore, due to their peculiar nature and in order to ensure a fair sharing of responsibilities along the AI value chain, such systems should be subject to proportionate and tailored requirements and obligations under this Regulation before their placing on		

PUBLIC

the Union market or putting into service. Therefore, the providers of general purpose AI systems, irrespective of whether they may be used as high-risk AI systems as such by other providers or as components of high-risk AI systems, should cooperate, as appropriate, with final providers to enable their compliance with the relevant obligations under this Regulation and with the competent authorities established under this Regulation.		
(13) In order to ensure a consistent and high level of protection of public interests as regards health, safety and fundamental rights, common normative standards for all high-risk AI systems should be established. Those standards should be consistent with the Charter of fundamental rights of the European Union (the Charter) and should be non-discriminatory and in line with the Union's international trade commitments.		

PUBLIC

(14) In order to introduce a proportionate and effective set of binding rules for AI systems, a clearly defined risk-based approach should be followed. That approach should tailor the type and content of such rules to the intensity and scope of the risks that AI systems can generate. It is therefore necessary to prohibit certain artificial intelligence practices, to lay down requirements for high-risk AI systems and obligations for the relevant operators, and to lay down transparency obligations for certain AI systems.		
(15) Aside from the many beneficial uses of artificial intelligence, that technology can also be misused and provide novel and powerful tools for manipulative, exploitative and social control practices. Such practices are particularly harmful and should be prohibited because they contradict Union values of respect for human		

PUBLIC

dignity, freedom, equality, democracy and the rule of law and Union fundamental rights, including the right to non-discrimination, data protection and privacy and the rights of the child.		
(16) The placing on the market, putting into service or use of certain AI systems ~~intended to distort~~ **materially distorting** human behaviour, whereby physical or psychological harms are likely to occur, should be forbidden. Such AI systems deploy subliminal components ~~individuals~~ **that persons** cannot perceive or **those sysems otherwise** exploit vulnerabilities of ~~children and people~~ **a specific group of persons** due to their age, ~~physical or mental incapacities. They do so with the intention to materially distort~~ **disability within the meaning of Directive (EU) 2019/882, or social or economic situation. Such systems can be placed on the market, put into service**		

PUBLIC

or used with the objective to or the effect of materially distorting the behaviour of a person and in a manner that causes or is **reasonably** likely to cause **physical or phycological** harm to that or another person~~. The intention~~ **or groups of persons, including harms that may be accumulated over time. The intention to distort the behaviour** may not be presumed if the distortion ~~of human behaviour~~ results from factors external to the AI system which are outside of the control of the provider or the user~~.~~ ~~Research for legitimate purposes in relation to such AI systems should~~, **meaning factors that may** not be ~~stifled~~ **reasonably foreseen and mitigated** by the ~~prohibition, if such research does not amount to use~~ **provider or the user** of the AI system ~~in human-machine relations that exposes natural persons to~~ **. In any case, it is not necessary for the provider or the user to have the intention to cause the physical or pshycological** harm ~~and such research is carried~~		

PUBLIC

~~out in accordance with recognised ethical standards~~**, as long as such harm results from the manipulative or exploitative AI-enabled practices. The prohibitions** for ~~scientific research~~ **such AI practices are ~~is~~ complementary to the provisions contained in Directive ~~[Unfair Commercial Practice Directive~~ 2005/29/EC~~, as amended by Directive (EU) 2019/216]~~, notably that unfair commercial practices leading to economic or financial harms to consumers are prohibited under all circumstances, irrespective of whether they are put in place through AI systems or otherwise**.		
(17) AI systems providing social scoring of natural persons ~~for general purpose~~ by public authorities or **by private actors** ~~on their behalf~~ may lead to discriminatory outcomes and the exclusion of certain groups. They may violate the right to dignity and non-discrimination and		

PUBLIC

the values of equality and justice. Such AI systems evaluate or classify ~~the trustworthiness of~~ natural persons based on their social behaviour in multiple contexts or known or predicted personal or personality characteristics. The social score obtained from such AI systems may lead to the detrimental or unfavourable treatment of natural persons or whole groups thereof in social contexts, which are unrelated to the context in which the data was originally generated or collected or to a detrimental treatment that is disproportionate or unjustified to the gravity of their social behaviour. ~~Such~~ AI systems **entailing such unacceptable scoring practices** should be therefore prohibited. **This prohibition should not affect lawful evaluation practices of natural persons done for one or more specific purpose in compliance with the law**.		
(18) The use of AI systems for 'real-time'		

PUBLIC

~~remote~~ biometric identification of natural persons in publicly accessible spaces for the purpose of law enforcement is considered particularly intrusive in the rights and freedoms of the concerned persons, to the extent that it may affect the private life of a large part of the population, evoke a feeling of constant surveillance and indirectly dissuade the exercise of the freedom of assembly and other fundamental rights. In addition, the immediacy of the impact and the limited opportunities for further checks or corrections in relation to the use of such systems operating in 'real-time' carry heightened risks for the rights and freedoms of the persons that are concerned by law enforcement activities.		
(19) The use of those systems for the purpose of law enforcement should therefore be prohibited, except in ~~three~~ exhaustively listed and narrowly defined situations, where the use	(…) **In addition, this Regulation should preserve the ability for law enforcement, migration or asylum**	

PUBLIC

is strictly necessary to achieve a substantial public interest, the importance of which outweighs the risks. Those situations involve the search for potential victims of crime, including missing children; certain threats to the life or physical safety of natural persons or of a terrorist attack; and the detection, localisation, identification or prosecution of perpetrators or suspects of the criminal offences referred to in Council Framework Decision 2002/584/JHA[9] if those criminal offences are punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least three years and as they are defined in the law of that Member State. Such threshold for the custodial sentence or detention order in accordance with national law contributes to ensure that the offence should be serious enough to potentially justify the use of 'real-time'	**authorities to carry out identity checks in the presence of the person that is concerned, in accordance with the conditions set up in national law and Union law for such checks. (…)**	Clarification: Union law also provides for relevant requirements.

[9] Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (OJ L 190, 18.7.2002, p. 1).

PUBLIC

~~remote~~ biometric identification systems. Moreover, of the 32 criminal offences listed in the Council Framework Decision 2002/584/JHA, some are in practice likely to be more relevant than others, in that the recourse to 'real-time' ~~remote~~ biometric identification will foreseeably be necessary and proportionate to highly varying degrees for the practical pursuit of the detection, localisation, identification or prosecution of a perpetrator or suspect of the different criminal offences listed and having regard to the likely differences in the seriousness, probability and scale of the harm or possible negative consequences. **In addition, this Regulation should preserve the ability for law enforcement, migration or asylum authorities to carry out identity checks in the presence of the person that is concerned, in accordance with the conditions set up in national law for such checks. In particular, law enforcement, migration or asylum**		

PUBLIC

authorities should be able to use information systems, in accordance with Union or national law, to identify a person who, during an identity check, either refuses to be identified or is unable to state or prove his or her identity, without being required by this Regulation to obtain prior authorisation. This could be, for example, a person involved a crime, unwilling, or unable due to an accident or a medical condition, to disclose their identity to law enforcement authorities.		
(20) In order to ensure that those systems are used in a responsible and proportionate manner, it is also important to establish that, in each of those three exhaustively listed and narrowly defined situations, certain elements should be taken into account, in particular as regards the nature of the situation giving rise to the request and the consequences of the use for the rights and freedoms of all persons concerned and the		

PUBLIC

safeguards and conditions provided for with the use. In addition, the use of 'real-time' ~~remote~~ biometric identification systems in publicly accessible spaces for the purpose of law enforcement should be subject to appropriate limits in time and space, having regard in particular to the evidence or indications regarding the threats, the victims or perpetrator. The reference database of persons should be appropriate for each use case in each of the three situations mentioned above.		
(21) Each use of a 'real-time' ~~remote~~ biometric identification system in publicly accessible spaces for the purpose of law enforcement should be subject to an express and specific authorisation by a judicial authority or by an independent administrative authority of a Member State. Such authorisation should in principle be obtained prior to the use, except in duly justified situations of urgency, that is,		

PUBLIC

situations where the need to use the systems in question is such as to make it effectively and objectively impossible to obtain an authorisation before commencing the use. In such situations of urgency, the use should be restricted to the absolute minimum necessary and be subject to appropriate safeguards and conditions, as determined in national law and specified in the context of each individual urgent use case by the law enforcement authority itself. In addition, the law enforcement authority should in such situations seek to obtain an authorisation as soon as possible, whilst providing the reasons for not having been able to request it earlier.		
(22) Furthermore, it is appropriate to provide, within the exhaustive framework set by this Regulation that such use in the territory of a Member State in accordance with this Regulation should only be possible where and in as far as the Member State in question has		

PUBLIC

decided to expressly provide for the possibility to authorise such use in its detailed rules of national law. Consequently, Member States remain free under this Regulation not to provide for such a possibility at all or to only provide for such a possibility in respect of some of the objectives capable of justifying authorised use identified in this Regulation.		
(23) The use of AI systems for 'real-time' ~~remote~~ biometric identification of natural persons in publicly accessible spaces for the purpose of law enforcement necessarily involves the processing of biometric data. The rules of this Regulation that prohibit, subject to certain exceptions, such use, which are based on Article 16 TFEU, should apply as *lex specialis* in respect of the rules on the processing of biometric data contained in Article 10 of Directive (EU) 2016/680, thus regulating such use and the processing of biometric data		

PUBLIC

involved in an exhaustive manner. Therefore, such use and processing should only be possible in as far as it is compatible with the framework set by this Regulation, without there being scope, outside that framework, for the competent authorities, where they act for purpose of law enforcement, to use such systems and process such data in connection thereto on the grounds listed in Article 10 of Directive (EU) 2016/680. In this context, this Regulation is not intended to provide the legal basis for the processing of personal data under Article 8 of Directive 2016/680. However, the use of 'real-time' ~~remote~~ biometric identification systems in publicly accessible spaces for purposes other than law enforcement, including by competent authorities, should not be covered by the specific framework regarding such use for the purpose of law enforcement set by this Regulation. Such use for purposes other than law enforcement should therefore not be		

PUBLIC

subject to the requirement of an authorisation under this Regulation and the applicable detailed rules of national law that may give effect to it.		
(24) Any processing of biometric data and other personal data involved in the use of AI systems for biometric identification, other than in connection to the use of 'real-time' ~~remote~~ biometric identification systems in publicly accessible spaces for the purpose of law enforcement as regulated by this Regulation, ~~including where those systems are used by competent authorities in publicly accessible spaces for other purposes than law enforcement,~~ should continue to comply with all requirements resulting from ~~Article 9(1) of Regulation (EU) 2016/679, Article 10(1) of Regulation (EU) 2018/1725~~ and Article 10 of Directive (EU) 2016/680~~., as applicable.~~ **For purposes other than law enforcement, Article 9(1) of**		

PUBLIC

Regulation (EU) 2016/679 and Article 10(1) of Regulation (EU) 2018/1725 prohibit the processing of biometric data for the purpose of uniquely identifying a natural person, unless one of the situations in the respective second paragraphs of those two articles applies.		
(25) In accordance with Article 6a of Protocol No 21 on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, as annexed to the TEU and to the TFEU, Ireland is not bound by the rules laid down in Article 5(1), point (d), (2)**,** ~~and~~ (3) **and (4)** of this Regulation adopted on the basis of Article 16 of the TFEU which relate to the processing of personal data by the Member States when carrying out activities falling within the scope of Chapter 4 or Chapter 5 of Title V of Part Three of the TFEU, where Ireland is not bound by the rules governing the forms of		

PUBLIC

judicial cooperation in criminal matters or police cooperation which require compliance with the provisions laid down on the basis of Article 16 of the TFEU.		
(26) In accordance with Articles 2 and 2a of Protocol No 22 on the position of Denmark, annexed to the TEU and TFEU, Denmark is not bound by rules laid down in Article 5(1), point (d), (2) ~~and ,~~ (3) **and (4)** of this Regulation adopted on the basis of Article 16 of the TFEU, or subject to their application, which relate to the processing of personal data by the Member States when carrying out activities falling within the scope of Chapter 4 or Chapter 5 of Title V of Part Three of the TFEU.		
(27) High-risk AI systems should only be placed on the Union market or put into service if they comply with certain mandatory requirements. Those requirements should ensure	AI systems identified as high-risk should be limited to those that have a significant harmful impact on the health, safety and	In line with the inclusion of AI systems posing high risks to the environment in Annex III, 2.b) (new), the scope of

PUBLIC

that high-risk AI systems available in the Union or whose output is otherwise used in the Union do not pose unacceptable risks to important Union public interests as recognised and protected by Union law. AI systems identified as high-risk should be limited to those that have a significant harmful impact on the health, safety and fundamental rights of persons in the Union and such limitation minimises any potential restriction to international trade, if any.	fundamental rights of persons in the Union, as well as on the environment, and such limitation minimises any potential restriction to international trade, if any.	relevant harmful impacts should be extended to include significant harmful impact on the environment.
(28) AI systems could produce adverse outcomes to health and safety of persons, in particular when such systems operate as components of products. Consistently with the objectives of Union harmonisation legislation to facilitate the free movement of products in the internal market and to ensure that only safe and otherwise compliant products find their way into the market, it is important that the safety risks that may be generated by a product as a whole	(…) The fundamental right to a high level of environmental protection enshrined in the Charter and implemented in Union policies should also be considered when assessing the severity of the harm that an AI system can cause~~, including in relation to the health and safety of persons~~.	The phase "including in relation to the health and safety of persons" does not improve the clarity of the sentence. Environment protection serves the goal of remaining in a "safe operating space for humanity" within the planetary boundaries.

PUBLIC

due to its digital components, including AI systems, are duly prevented and mitigated. For instance, increasingly autonomous robots, whether in the context of manufacturing or personal assistance and care should be able to safely operate and performs their functions in complex environments. Similarly, in the health sector where the stakes for life and health are particularly high, increasingly sophisticated diagnostics systems and systems supporting human decisions should be reliable and accurate. The extent of the adverse impact caused by the AI system on the fundamental rights protected by the Charter is of particular relevance when classifying an AI system as high-risk. Those rights include the right to human dignity, respect for private and family life, protection of personal data, freedom of expression and information, freedom of assembly and of association, and non-discrimination, consumer protection, workers'		

PUBLIC

rights, rights of persons with disabilities, right to an effective remedy and to a fair trial, right of defence and the presumption of innocence, right to good administration. In addition to those rights, it is important to highlight that children have specific rights as enshrined in Article 24 of the EU Charter and in the United Nations Convention on the Rights of the Child (further elaborated in the UNCRC General Comment No. 25 as regards the digital environment), both of which require consideration of the children's vulnerabilities and provision of such protection and care as necessary for their well-being. The fundamental right to a high level of environmental protection enshrined in the Charter and implemented in Union policies should also be considered when assessing the severity of the harm that an AI system can cause, including in relation to the health and safety of persons.		

PUBLIC

(29) As regards high-risk AI systems that are safety components of products or systems, or which are themselves products or systems falling within the scope of Regulation (EC) No 300/2008 of the European Parliament and of the Council[10], Regulation (EU) No 167/2013 of the European Parliament and of the Council[11],		

[10] Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002 (OJ L 97, 9.4.2008, p. 72).

[11] Regulation (EU) No 167/2013 of the European Parliament and of the Council of 5 February 2013 on the approval and market surveillance of agricultural and forestry vehicles (OJ L 60, 2.3.2013, p. 1).

PUBLIC

Regulation (EU) No 168/2013 of the European Parliament and of the Council[12], Directive 2014/90/EU of the European Parliament and of the Council[13], Directive (EU) 2016/797 of the European Parliament and of the Council[14], Regulation (EU) 2018/858 of the European Parliament and of the Council[15], Regulation (EU) 2018/1139 of the European Parliament and of the Council[16], and Regulation (EU)		

[12] Regulation (EU) No 168/2013 of the European Parliament and of the Council of 15 January 2013 on the approval and market surveillance of two- or three-wheel vehicles and quadricycles (OJ L 60, 2.3.2013, p. 52).

[13] Directive 2014/90/EU of the European Parliament and of the Council of 23 July 2014 on marine equipment and repealing Council Directive 96/98/EC (OJ L 257, 28.8.2014, p. 146).

[14] Directive (EU) 2016/797 of the European Parliament and of the Council of 11 May 2016 on the interoperability of the rail system within the European Union (OJ L 138, 26.5.2016, p. 44).

[15] Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles, amending Regulations (EC) No 715/2007 and (EC) No 595/2009 and repealing Directive 2007/46/EC (OJ L 151, 14.6.2018, p. 1).

[16] Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91 (OJ L 212, 22.8.2018, p. 1).

PUBLIC

2019/2144 of the European Parliament and of the Council[17], it is appropriate to amend those acts to ensure that the Commission takes into account, on the basis of the technical and regulatory specificities of each sector, and without interfering with existing governance, conformity assessment and enforcement mechanisms and authorities established therein, the mandatory requirements for high-risk AI systems laid down in this Regulation when adopting any relevant future delegated or implementing acts on the basis of those acts.		
(30) As regards AI systems that are safety components of products, or which are themselves products, falling within the scope of		

[17] Regulation (EU) 2019/2144 of the European Parliament and of the Council of 27 November 2019 on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users, amending Regulation (EU) 2018/858 of the European Parliament and of the Council and repealing Regulations (EC) No 78/2009, (EC) No 79/2009 and (EC) No 661/2009 of the European Parliament and of the Council and Commission Regulations (EC) No 631/2009, (EU) No 406/2010, (EU) No 672/2010, (EU) No 1003/2010, (EU) No 1005/2010, (EU) No 1008/2010, (EU) No 1009/2010, (EU) No 19/2011, (EU) No 109/2011, (EU) No 458/2011, (EU) No 65/2012, (EU) No 130/2012, (EU) No 347/2012, (EU) No 351/2012, (EU) No 1230/2012 and (EU) 2015/166 (OJ L 325, 16.12.2019, p. 1).

PUBLIC

certain Union harmonisation legislation, it is appropriate to classify them as high-risk under this Regulation if the product in question undergoes the conformity assessment procedure with a third-party conformity assessment body pursuant to that relevant Union harmonisation legislation. In particular, such products are machinery, toys, lifts, equipment and protective systems intended for use in potentially explosive atmospheres, radio equipment, pressure equipment, recreational craft equipment, cableway installations, appliances burning gaseous fuels, medical devices, and in vitro diagnostic medical devices.		
(31) The classification of an AI system as high-risk pursuant to this Regulation should not necessarily mean that the product whose safety component is the AI system, or the AI system itself as a product, is considered 'high-risk' under the criteria established in the relevant		

PUBLIC

Union harmonisation legislation that applies to the product. This is notably the case for Regulation (EU) 2017/745 of the European Parliament and of the Council[18] and Regulation (EU) 2017/746 of the European Parliament and of the Council[19], where a third-party conformity assessment is provided for medium-risk and high-risk products.		
(32) As regards ~~stand-alone AI systems, meaning~~ high-risk AI systems other than those that are safety components of products, or which are themselves products, it is appropriate to classify them as high-risk if, in the light of their intended purpose, they pose a high risk of harm to the health and safety or the fundamental rights of persons, taking into account both the		In line with the inclusion of AI systems posing high risks to the environment in Annex III, 2.b) (new), the list of risks of harm should be extended to include risks of harm to the environment.

[18] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (OJ L 117, 5.5.2017, p. 1).

[19] Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU (OJ L 117, 5.5.2017, p. 176).

PUBLIC

severity of the possible harm and its probability of occurrence, and they are used in a number of specifically pre-defined areas specified in the Regulation. The identification of those systems is based on the same methodology and criteria envisaged also for any future amendments of the list of high-risk AI systems. **On top of that, the significance of the ouput of the AI system in relation to the decision or action taken by a human, as well as the immediacy of the effect should also be taken into account when classifying AI systems as high risk.**	pose a high risk of harm to the health and safety or the fundamental rights of persons **or to the environment**, taking into account both the severity of the possible harm and its probability of occurrence,	Furthermore, we welcome the changes in recital 32. Respecting the significance of human decision making makes sense and hence allows – especially regarding public security and law enforcement to emphasize the fact that a human employee makes the final decision regarding a measure, notwithstanding an AI supported indication regarding the decision.
(33) Technical inaccuracies of AI systems intended for the ~~remote~~ biometric identification of natural persons can lead to biased results and entail discriminatory effects. This is particularly relevant when it comes to age, ethnicity, sex or disabilities. Therefore, 'real-time' and 'post' ~~remote~~ biometric identification systems should be classified as high-risk. In view of the risks		

PUBLIC

that they pose, both types of ~~remote~~ biometric identification systems should be subject to specific requirements on logging capabilities and human oversight.		
(34) As regards the management and operation of critical infrastructure, it is appropriate to classify as high-risk the 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, since their failure or malfunctioning may put at risk the life and health of persons at large scale and lead to appreciable disruptions in the ordinary conduct of social and economic activities. **Considering the increasing digitalisation of all sectors of the economic and public life, it is also appropriate to classify as high risk AI systems intended to be used ~~to control or~~ as safety components of critical digital infrastructure as listed in**	As regards the management and operation of critical infrastructure, it is appropriate to classify as high-risk the 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 and the collection, treatment and discharge of wastewater, since their failure or malfunctioning may put at risk the life and health of persons at large scale and lead to appreciable disruptions in the ordinary conduct of social and economic	Pursuant the first preamble and recital no. 2, the legal bases of the AIA are Art. 16 and 114 TFEU and not the EURATOM Treaty. Subsequently, rather than including this crucial clarification in the operative clause, the proposed insertion is best placed in the relevant recital as interpretative parameter. Cf. Annex III, 2.b) (new)

PUBLIC

Annex I point 8 of the Directive on the resilience of critical entities. ~~**Furthermore, AI systems that control emissions and pollution should also be classified as high-risk, taking into account the serious incidents and the irreversible damage to the environment and health that can be caused.**~~	activities. Within the meaning of this regulation, pursuant to its legal basis and without prejudice to the rules and regulations of the EURATOM-Treaty, the supply of electricity shall only apply to non-nuclear sources. Considering the increasing digitalisation of all sectors of the economic and public life, it is also appropriate to classify as high risk AI systems intended to be used to control or as safety components of critical digital infrastructure as listed in Annex I point 8 of the Directive on the resilience of critical entities. Furthermore, AI systems that control industrial activities of the energy	

PUBLIC

	industries, production or processing of metals, mineral industry, chemical industry and waste management as referred to in the Industrial Emission Directive (IED) should also be classified as high-risk, taking into account the substantial emissions, serious incidents and the irreversible damage to the environment and health that can be caused	
(35) AI systems used in education or vocational training, notably for determining access or assigning persons to educational and vocational training institutions or to evaluate persons on tests as part of or as a precondition for their education should be considered high-risk, since they may determine the educational and professional course of a person's life and		

PUBLIC

therefore affect their ability to secure their livelihood. When improperly designed and used, such systems may violate the right to education and training as well as the right not to be discriminated against and perpetuate historical patterns of discrimination.		
(36) AI systems used in employment, workers management and access to self-employment, notably for the recruitment and selection of persons, for making decisions on promotion and termination and for task allocation, monitoring or evaluation of persons in work-related contractual relationships, should also be classified as high-risk, since those systems may appreciably impact future career prospects and livelihoods of these persons. Relevant work-related contractual relationships should involve employees and persons providing services through platforms as referred to in the Commission Work Programme 2021. Such		

PUBLIC

persons should in principle not be considered users within the meaning of this Regulation. Throughout the recruitment process and in the evaluation, promotion, or retention of persons in work-related contractual relationships, such systems may perpetuate historical patterns of discrimination, for example against women, certain age groups, persons with disabilities, or persons of certain racial or ethnic origins or sexual orientation. AI systems used to monitor the performance and behaviour of these persons may also impact their rights to data protection and privacy.		
(37) Another area in which the use of AI systems deserves special consideration is the access to and enjoyment of certain essential private and public services and benefits necessary for people to fully participate in society or to improve one's standard of living. In particular, AI systems used to evaluate the	Finally, AI systems used to dispatch or establish priority in the dispatching of emergency first response services should also be classified as high-risk since they make decisions in very critical situations for the life and health of persons and	Reinserting the highlighted passage, see also annotation regarding Annex III, line 701.

PUBLIC

credit score or creditworthiness of natural persons should be classified as high-risk AI systems, since they determine those persons' access to financial resources or essential services such as housing, electricity, and telecommunication services. AI systems used for this purpose may lead to discrimination of persons or groups and perpetuate historical patterns of discrimination, for example based on racial or ethnic origins, disabilities, age, sexual orientation, or create new forms of discriminatory impacts. Considering the very limited scale of the impact and the available alternatives on the market, it is appropriate to exempt AI systems for the purpose of creditworthiness assessment and credit scoring when put into service by ~~small-scale providers~~ **SMEs, including start-ups,** for their own use. Natural persons applying for or receiving public assistance benefits and services from public authorities are typically dependent on those	their property. **AI systems are also increasingly used in insurance for premium setting, underwriting and claims assessment which, if not duly designed, developed and used, can lead to serious consequences for people's life, including financial exclusion and discrimination.**	

PUBLIC

benefits and services and in a vulnerable position in relation to the responsible authorities. If AI systems are used for determining whether such benefits and services should be denied, reduced, revoked or reclaimed by authorities, they may have a significant impact on persons' livelihood and may infringe their fundamental rights, such as the right to social protection, non-discrimination, human dignity or an effective remedy. Those systems should therefore be classified as high-risk. Nonetheless, this Regulation should not hamper the development and use of innovative approaches in the public administration, which would stand to benefit from a wider use of compliant and safe AI systems, provided that those systems do not entail a high risk to legal and natural persons. Finally, AI systems used to dispatch or establish priority in the dispatching of emergency first response services should also be classified as high-risk since they make		

PUBLIC

decisions in very critical situations for the life and health of persons and their property. ~~**AI systems are also increasingly used in insurance for premium setting, underwriting and claims assessment which, if not duly designed, developed and used, can lead to serious consequences for people's life, including financial exclusion and discrimination.**~~		
(38) Actions by law enforcement authorities involving certain uses of AI systems are characterised by a significant degree of power imbalance and may lead to surveillance, arrest or deprivation of a natural person's liberty as well as other adverse impacts on fundamental rights guaranteed in the Charter. In particular, if the AI system is not trained with high quality data, does not meet adequate requirements in terms of its accuracy or robustness, or is not properly designed and tested before being put		

PUBLIC

on the market or otherwise put into service, it may single out people in a discriminatory or otherwise incorrect or unjust manner. Furthermore, the exercise of important procedural fundamental rights, such as the right to an effective remedy and to a fair trial as well as the right of defence and the presumption of innocence, could be hampered, in particular, where such AI systems are not sufficiently transparent, explainable and documented. It is therefore appropriate to classify as high-risk a number of AI systems intended to be used in the law enforcement context where accuracy, reliability and transparency is particularly important to avoid adverse impacts, retain public trust and ensure accountability and effective redress. In view of the nature of the activities in question and the risks relating thereto, those high-risk AI systems should include in particular AI systems intended to be used by law enforcement authorities for		

PUBLIC

individual risk assessments, polygraphs and similar tools or to detect the emotional state of natural person, ~~to detect 'deep fakes'~~, for the evaluation of the reliability of evidence in criminal proceedings, for predicting the occurrence or reoccurrence of an actual or potential criminal offence based on profiling of natural persons, or assessing personality traits and characteristics or past criminal behaviour of natural persons or groups, for profiling in the course of detection, investigation or prosecution of criminal offences, as well as for crime analytics regarding natural persons. AI systems specifically intended to be used for administrative proceedings by tax and customs authorities should not be considered high-risk AI systems used by law enforcement authorities for the purposes of prevention, detection, investigation and prosecution of criminal offences.		

PUBLIC

(39) AI systems used in migration, asylum and border control management affect people who are often in particularly vulnerable position and who are dependent on the outcome of the actions of the competent public authorities. The accuracy, non-discriminatory nature and transparency of the AI systems used in those contexts are therefore particularly important to guarantee the respect of the fundamental rights of the affected persons, notably their rights to free movement, non-discrimination, protection of private life and personal data, international protection and good administration. It is therefore appropriate to classify as high-risk AI systems intended to be used by the competent public authorities charged with tasks in the fields of migration, asylum and border control management as polygraphs and similar tools or to detect the emotional state of a natural person; for assessing certain risks posed by natural persons entering the territory of a Member State		

PUBLIC

or applying for visa or asylum; ~~for verifying the authenticity of the relevant documents of natural persons;~~ for assisting competent public authorities for the examination of applications for asylum, visa and residence permits and associated complaints with regard to the objective to establish the eligibility of the natural persons applying for a status. AI systems in the area of migration, asylum and border control management covered by this Regulation should comply with the relevant procedural requirements set by the Directive 2013/32/EU of the European Parliament and of the Council[20], the Regulation (EC) No 810/2009 of the European Parliament and of the Council[21] and other relevant legislation.		

[20] Directive 2013/32/EU of the European Parliament and of the Council of 26 June 2013 on common procedures for granting and withdrawing international protection (OJ L 180, 29.6.2013, p. 60).

[21] Regulation (EC) No 810/2009 of the European Parliament and of the Council of 13 July 2009 establishing a Community Code on Visas (Visa Code) (OJ L 243, 15.9.2009, p. 1).

PUBLIC

(40) Certain AI systems intended for the administration of justice and democratic processes should be classified as high-risk, considering their potentially significant impact on democracy, rule of law, individual freedoms as well as the right to an effective remedy and to a fair trial. In particular, to address the risks of potential biases, errors and opacity, it is appropriate to qualify as high-risk AI systems intended to assist judicial authorities in ~~researching and~~ interpreting facts and the law and in applying the law to a concrete set of facts. Such qualification should not extend, however, to AI systems intended for purely ancillary administrative activities that do not affect the actual administration of justice in individual cases, such as anonymisation or pseudonymisation of judicial decisions, documents or data, communication between personnel, administrative tasks ~~or allocation of resources~~.		

PUBLIC

(41) The fact that an AI system is classified as high risk under this Regulation should not be interpreted as indicating that the use of the system is ~~necessarily~~ lawful under other acts of Union law or under national law compatible with Union law, such as on the protection of personal data, on the use of polygraphs and similar tools or other systems to detect the emotional state of natural persons. Any such use should continue to occur solely in accordance with the applicable requirements resulting from the Charter and from the applicable acts of secondary Union law and national law. This Regulation should not be understood as providing for the legal ground for processing of personal data, including special categories of personal data, where relevant**, unless it is provided for otherwise in this Regulation**.		
(42) To mitigate the risks from high-risk AI		

PUBLIC

systems placed or otherwise put into service on the Union market for users and affected persons, certain mandatory requirements should apply, taking into account the intended purpose of the use of the system and according to the risk management system to be established by the provider.		
(43) Requirements should apply to high-risk AI systems as regards the quality of data sets used, technical documentation and record-keeping, transparency and the provision of information to users, human oversight, and robustness, accuracy and cybersecurity. Those requirements are necessary to effectively mitigate the risks for health, safety and fundamental rights, as applicable in the light of the intended purpose of the system, and no other less trade restrictive measures are reasonably available, thus avoiding unjustified restrictions to trade.		

PUBLIC

(44) High data quality is essential for the performance of many AI systems, especially when techniques involving the training of models are used, with a view to ensure that the high-risk AI system performs as intended and safely and it does not become the source of discrimination prohibited by Union law. High quality training, validation and testing data sets require the implementation of appropriate data governance and management practices. Training, validation and testing data sets should be sufficiently relevant, representative and ~~free of errors and complete in view of the intended purpose of the system. They should also~~ have the appropriate statistical properties, including as regards the persons or groups of persons on which the high-risk AI system is intended to be used. **These datasets should also be as free of errors and complete as possible in view of the intended purpose of the AI system, taking into account, in a proportionate manner,**		

PUBLIC

technical feasibility and state of the art, the availability of data and the implementation of appropriate risk management measures so that possible shortcomings of the datasets are duly addressed. The requirement for the datasets to be complete and free of errors should not affect the use of privacy-preserving techniques in the context of the the development and testing of AI systems. ~~In particular,~~ tTraining, validation and testing data sets should take into account, to the extent required ~~in the light of~~ **by** their intended purpose, the features, characteristics or elements that are particular to the specific geographical, behavioural or functional setting or context within which the AI system is intended to be used. In order to protect the right of others from the discrimination that might result from the bias in AI systems, the providers should be able to process also special categories of personal data, as a matter of substantial public interest		

PUBLIC

within the meaning of Article 9(2)(g) of Regulation (EU) 2016/679 and Article 10(2)g) of Regulation (EU) 2018/1725, in order to ensure the bias monitoring, detection and correction in relation to high-risk AI systems.		
(44a) When applying the principles referred to in Article 5(1)(c) of Regulation 2016/679 and Article 4(1)(c) of Regulation 2018/1725, in particular the principle of data minimisation, in regard to training, validation and testing data sets under this Regulation, due regard should be had to the full life cycle of the AI system.		
(45) For the development of high-risk AI systems, certain actors, such as providers, notified bodies and other relevant entities, such as digital innovation hubs, testing experimentation facilities and researchers, should be able to access and use high quality		

PUBLIC

datasets within their respective fields of activities which are related to this Regulation. European common data spaces established by the Commission and the facilitation of data sharing between businesses and with government in the public interest will be instrumental to provide trustful, accountable and non-discriminatory access to high quality data for the training, validation and testing of AI systems. For example, in health, the European health data space will facilitate non-discriminatory access to health data and the training of artificial intelligence algorithms on those datasets, in a privacy-preserving, secure, timely, transparent and trustworthy manner, and with an appropriate institutional governance. Relevant competent authorities, including sectoral ones, providing or supporting the access to data may also support the provision of high-quality data for the training, validation and testing of AI systems.		

PUBLIC

(46) Having information on how high-risk AI systems have been developed and how they perform throughout their lifecycle is essential to verify compliance with the requirements under this Regulation. This requires keeping records and the availability of a technical documentation, containing information which is necessary to assess the compliance of the AI system with the relevant requirements. Such information should include the general characteristics, capabilities and limitations of the system, algorithms, data, training, testing and validation processes used as well as documentation on the relevant risk management system. The technical documentation should be kept up to date. **Furthermore, providers or users should keep logs automatically generated by the high-risk AI system, to the extent that such logs are under their control, for a period that is appropriate to enable**		

PUBLIC

them to fufil their obligations.		
(47) To address the opacity that may make certain AI systems incomprehensible to or too complex for natural persons, a certain degree of transparency should be required for high-risk AI systems. Users should be able to interpret the system output and use it appropriately. High-risk AI systems should therefore be accompanied by relevant documentation and instructions of use and include concise and clear information, including in relation to possible risks to fundamental rights and discrimination, where appropriate. **To facilitate the understanding of the instructions of use by users, they should contain illustrative examples, as appropriate.**		
(48) High-risk AI systems should be designed and developed in such a way that natural persons can oversee their functioning. For this		We refer to our comment regarding Art. 14(5).

PUBLIC

purpose, appropriate human oversight measures should be identified by the provider of the system before its placing on the market or putting into service. In particular, where appropriate, such measures should guarantee that the system is subject to in-built operational constraints that cannot be overridden by the system itself and is responsive to the human operator, and that the natural persons to whom human oversight has been assigned have the necessary competence, training and authority to carry out that role. **Considering the significant consequences for persons in case of incorrect matches by certain biometric identification systems, it is appropriate to provide for an enhanced human oversight requirement for those systems so that no action or decision may be 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.**		

PUBLIC

Those persons could be from one or more entities and include the person operating or using the system. This requirement should not pose unnecessary burden or delays and it could be sufficient that the separate verifications by the different persons are automatically recorded in the logs generated by the system.		
(49) High-risk AI systems should perform consistently throughout their lifecycle and meet an appropriate level of accuracy, robustness and cybersecurity in accordance with the generally acknowledged state of the art. The level of accuracy and accuracy metrics should be communicated to the users.		
(50) The technical robustness is a key requirement for high-risk AI systems. They should be resilient **in relation to harmful or otherwise undesirable behaviour that may**		

PUBLIC

result from ~~against risks connected to the~~ limitations **within the systems or the environment in which the systems operate** ~~of the system~~ (e.g. errors, faults, inconsistencies, unexpected situations)**. High-risk AI systems should therefore be designed and developed with appropriate technical solutions to prevent or minimize that harmful or otherwise undesirable behaviour, such as for instance mechanisms enabling the system to safely interrupt its operation (fail-safe plans) in the presence of certain anomalies or when operation takes place outside certain predetermined boundaries** ~~as well as against malicious actions that may compromise the security of the AI system and result in harmful or otherwise undesirable behaviour~~. Failure to protect against these risks could lead to safety impacts or negatively affect the fundamental rights, for example due to erroneous decisions or wrong or biased outputs generated by the AI		

PUBLIC

system.		
(51) Cybersecurity plays a crucial role in ensuring that AI systems are resilient against attempts to alter their use, behaviour, performance or compromise their security properties by malicious third parties exploiting the system's vulnerabilities. Cyberattacks against AI systems can leverage AI specific assets, such as training data sets (e.g. data poisoning) or trained models (e.g. adversarial attacks), or exploit vulnerabilities in the AI system's digital assets or the underlying ICT infrastructure. To ensure a level of cybersecurity appropriate to the risks, suitable measures should therefore be taken by the providers of high-risk AI systems, also taking into account as appropriate the underlying ICT infrastructure.		
(52) As part of Union harmonisation legislation, rules applicable to the placing on the		

PUBLIC

market, putting into service and use of high-risk AI systems should be laid down consistently with Regulation (EC) No 765/2008 of the European Parliament and of the Council[22] setting out the requirements for accreditation and the market surveillance of products, Decision No 768/2008/EC of the European Parliament and of the Council[23] on a common framework for the marketing of products and Regulation (EU) 2019/1020 of the European Parliament and of the Council[24] on market surveillance and compliance of products ('New Legislative Framework for the marketing of products').		
(52a) In line with New Legislative		

[22] Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93 (OJ L 218, 13.8.2008, p. 30).

[23] Decision No 768/2008/EC of the European Parliament and of the Council of 9 July 2008 on a common framework for the marketing of products, and repealing Council Decision 93/465/EEC (OJ L 218, 13.8.2008, p. 82).

[24] Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011 (Text with EEA relevance) (OJ L 169, 25.6.2019, p. 1–44).

PUBLIC

Framework principles, specific obligations for relevant operators within the AI value chain should be set to ensure legal certainty and facilitate compliance with this Regulation. In certain situations those operators could act in more than one role at the same time and should therefore fufil cumulatively all relevant obligations associated with those roles. For example, an operator could act as a distributor and an importer at the same time.		
(53) It is appropriate that a specific natural or legal person, defined as the provider, takes the responsibility for the placing on the market or putting into service of a high-risk AI system, regardless of whether that natural or legal person is the person who designed or developed the system.		
(54) The provider should establish a sound		

PUBLIC

quality management system, ensure the accomplishment of the required conformity assessment procedure, draw up the relevant documentation and establish a robust post-market monitoring system. Public authorities which put into service high-risk AI systems for their own use may adopt and implement the rules for the quality management system as part of the quality management system adopted at a national or regional level, as appropriate, taking into account the specificities of the sector and the competences and organisation of the public authority in question.		
(54a) To ensure legal certainty, it is necessary to clarify that any natural or legal person should be considered a provider of a new high-risk AI system and therefore assume all the relevant obligations under certain specific conditions. For example, this would be the case if that person puts its name or		The statement in recital 54a „… it is necessary to clarify that any natural or legal person should be considered a provider of a new high-risk AI system" is not comprehensible. It is proposed to take the wording of Art. 23a into

PUBLIC

trademark on a high-risk AI system already placed on the market or put into service, or if that person modifies the intended purpose of an AI system which is not high-risk and is already placed on the market or put into service, in a way that makes the modified system a high-risk AI system. These provisions should apply without prejudice to more specific provisions established in certain New Legislative Framework sectorial legislation with which this Regulation should apply jointly. For example, Article 16, paragraph 2 of Regulation 745/2017, establishing that certain changes should not be considered modifications of a device that could affect its compliance with the applicable requirements, should continue to apply to high-risk AI systems that are medical devices within the meaning of that Regulation.		account, which is supposedly refered to here.

PUBLIC

(55) Where a high-risk AI system that is a safety component of a product which is covered by a relevant New Legislative Framework sectorial legislation is not placed on the market or put into service independently from the product, the **product** manufacturer ~~of the final product~~ as defined under the relevant New Legislative Framework legislation should comply with the obligations of the provider established in this Regulation and notably ensure that the AI system embedded in the final product complies with the requirements of this Regulation.		
(56) To enable enforcement of this Regulation and create a level-playing field for operators, and taking into account the different forms of making available of digital products, it is important to ensure that, under all circumstances, a person established in the Union can provide authorities with all the necessary		

PUBLIC

information on the compliance of an AI system. Therefore, prior to making their AI systems available in the Union, where an importer cannot be identified, providers established outside the Union shall, by written mandate, appoint an authorised representative established in the Union.		
(56a) For providers who are not established in the Union, the authorised representative plays a pivotal role in ensuring the compliance of the high-risk AI systems placed on the market or put into service in the Union by those providers and in serving as their contact person established in the Union. Given that pivotal role, and in order to ensure that responsibility is assumed for the purposes of enforcement of this Regulation, it is appropriate to make the authorised representative jointly and severally liable with the provider for		

PUBLIC

defective high-risk AI systems. The liability of the authorised representative provided for in this Regulation is without prejudice to the provisions of Directive 85/374/EEC on liability for defective products.		
(57) ~~In line with New Legislative Framework principles, specific obligations for relevant economic operators, such as importers and distributors, should be set to ensure legal certainty and facilitate regulatory compliance by those relevant operators.~~		
(58) Given the nature of AI systems and the risks to safety and fundamental rights possibly associated with their use, including as regard the need to ensure proper monitoring of the performance of an AI system in a real-life setting, it is appropriate to set specific responsibilities for users. Users should in particular use high-risk AI systems in		

PUBLIC

accordance with the instructions of use and certain other obligations should be provided for with regard to monitoring of the functioning of the AI systems and with regard to record-keeping, as appropriate. **These obligations should not apply where the use is made in the course of a personal non-professional activity.**		
(58a) The obligations placed on various operators involved in the AI value chain under this Regulation should apply without prejudice to all other applicable Union and Member States laws aiming to protect fundamental rights and to regulate certain activities, products and services regardless of whether AI systems are used or not. In particular, it is appropriate to clarify that this Regulation does not affect the obligations of providers and users of AI systems in their role as data controllers or processors		We appreciate these further clarifications concerning the relationship between this Regulation and data protection law, but we suggest to include any supplementing provisions of national law clearlier within the whole Regulation (in Recitals, e.g. in Recital 58a, as well as in Articles).

PUBLIC

stemming from Union law on the protection of personal data in so far as the design, the development or the use of AI systems involves the processing of personal data. It is also appropriate to clarify that data subjects continue to enjoy all the rights and guarantees awarded to them by such Union law, including the rights related to solely automated individual decision-making, including profiling. Harmonised rules for the placing on the market, the putting into service and the use of AI systems established under this Regulation should facilitate the effective implementation and enable the exercise of the data subjects' rights and other remedies guaranteed under Union law on the protection of personal data and of other fundamental rights.	**[…] In particular, it is appropriate to clarify that this Regulation does not affect the obligations of providers and users of AI systems in their role as data controllers or processors stemming from Union law on the protection of personal data including any supplementing provisions of national law**	
(59) ~~It is appropriate to envisage that the user of the AI system should be the natural or legal~~		

PUBLIC

~~person, public authority, agency or other body under whose authority the AI system is operated except where the use is made in the course of a personal non-professional activity~~.		
(60) ~~In the light of the complexity of the artificial intelligence value chain, relevant third parties, notably the ones involved in the sale and the supply of software, software tools and components, pre-trained models and data, or providers of network services, should cooperate, as appropriate, with providers and users to enable their compliance with the obligations under this Regulation and with competent authorities established under this Regulation.~~		
(61) Standardisation should play a key role to provide technical solutions to providers to ensure compliance with this Regulation. Compliance with harmonised standards as defined in Regulation (EU) No 1025/2012 of the		

PUBLIC

European Parliament and of the Council[25] should be a means for providers to demonstrate conformity with the requirements of this Regulation. However, the Commission could adopt common technical specifications in areas where no harmonised standards exist or where they are insufficient. **An appropriate involvement of small and medium enterprises in the elaboration of standards supporting the implementation of this Regulation is essential to promote innovation and competitiveness in the field of artificial intelligence within the Union. Such involvement should be appropriately ensured in accordance with Article 5 and 6 of Regulation 1025/2012.**		

[25] Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council (OJ L 316, 14.11.2012, p. 12).

PUBLIC

(61a) It is appropriate that, without prejudice to the use of harmonised standards and common specifications, providers benefit from a presumption of conformity with the relevant requirement on data when their high-risk AI system has been trained and tested on data reflecting the specific geographical, behavioural or functional setting within which the AI system is intended to be used. Similarly, in line with Article 54(3) of Regulation (EU) 2019/881 of the European Parliament and of the Council , high-risk AI systems that have been certified or for which a statement of conformity has been issued under a cybersecurity scheme pursuant to that Regulation and the references of which have been published in the Official Journal of the European Union should be presumed to be in compliance with the cybersecurity requirement of this Regulation. This remains without prejudice		

PUBLIC

to the voluntary nature of that cybersecurity scheme.		
(62) In order to ensure a high level of trustworthiness of high-risk AI systems, those systems should be subject to a conformity assessment prior to their placing on the market or putting into service.		
(63) It is appropriate that, in order to minimise the burden on operators and avoid any possible duplication, for high-risk AI systems related to products which are covered by existing Union harmonisation legislation following the New Legislative Framework approach, the compliance of those AI systems with the requirements of this Regulation should be assessed as part of the conformity assessment already foreseen under that legislation. The applicability of the requirements of this Regulation should thus not affect the specific		

PUBLIC

logic, methodology or general structure of conformity assessment under the relevant specific New Legislative Framework legislation. This approach is fully reflected in the interplay between this Regulation and the [Machinery Regulation]. While safety risks of AI systems ensuring safety functions in machinery are addressed by the requirements of this Regulation, certain specific requirements in the [Machinery Regulation] will ensure the safe integration of the AI system into the overall machinery, so as not to compromise the safety of the machinery as a whole. The [Machinery Regulation] applies the same definition of AI system as this Regulation.		
(64) Given the more extensive experience of professional pre-market certifiers in the field of product safety and the different nature of risks involved, it is appropriate to limit, at least in an initial phase of application of this Regulation,		

PUBLIC

the scope of application of third-party conformity assessment for high-risk AI systems other than those related to products. Therefore, the conformity assessment of such systems should be carried out as a general rule by the provider under its own responsibility, with the only exception of AI systems intended to be used for the ~~remote~~ biometric identification of persons, for which the involvement of a notified body in the conformity assessment should be foreseen, to the extent they are not prohibited.		
(65) In order to carry out third-party conformity assessment for AI systems intended to be used for the ~~remote~~ biometric identification of persons, notified bodies should be designated under this Regulation by the national competent authorities, provided they are compliant with a set of requirements, notably on independence, competence and absence of conflicts of interests.		

PUBLIC

(66) In line with the commonly established notion of substantial modification for products regulated by Union harmonisation legislation, it is appropriate that **whenever a change occurs which may affect the compliance of a high risk AI system with this Regulation (e.g. change of operating system or software architecture, new or modified training datasets), or when the intended purpose of the system changes, that AI system should be considered a new AI system which should undergo** ~~an AI system undergoes~~ a new conformity assessment ~~whenever a change occurs which may affect the compliance of the system with this Regulation or when the intended purpose of the system changes~~. ~~In addition~~ **However**, **changes occuring to the algorithm and the performance of AI systems which continue to 'learn' after being placed on the market or put into service (i.e.**		

PUBLIC

automatically adapting how functions are carried out) should not constitute a substantial modification, provided that those changes have been pre-determined by the provider and assessed at the moment of the conformity assessment. ~~as regards AI systems which continue to 'learn' after being placed on the market or put into service (i.e. they automatically adapt how functions are carried out), it is necessary to provide rules establishing that the changes to the algorithm and its performance that have been pre-determined by the provider and assessed at the moment of the conformity assessment should not constitute a substantial modification.~~		
(67) High-risk AI systems should bear the CE marking to indicate their conformity with this Regulation so that they can move freely within the internal market. Member States should not create unjustified obstacles to the placing on the		

PUBLIC

market or putting into service of high-risk AI systems that comply with the requirements laid down in this Regulation and bear the CE marking.		
(68) Under certain conditions, rapid availability of innovative technologies may be crucial for health and safety of persons and for society as a whole. It is thus appropriate that under exceptional reasons of public security or protection of life and health of natural persons and the protection of industrial and commercial property, Member States could authorise the placing on the market or putting into service of AI systems which have not undergone a conformity assessment.		
(69) In order to facilitate the work of the Commission and the Member States in the artificial intelligence field as well as to increase the transparency towards the public, providers		

PUBLIC

of high-risk AI systems other than those related to products falling within the scope of relevant existing Union harmonisation legislation, should be required to register their high-risk AI system in a EU database, to be established and managed by the Commission. The Commission should be the controller of that database, in accordance with Regulation (EU) 2018/1725 of the European Parliament and of the Council[26]. In order to ensure the full functionality of the database, when deployed, the procedure for setting the database should include the elaboration of functional specifications by the Commission and an independent audit report.		
(70) Certain AI systems intended to interact with natural persons or to generate content may pose specific risks of impersonation or		

[26] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

PUBLIC

deception irrespective of whether they qualify as high-risk or not. In certain circumstances, the use of these systems should therefore be subject to specific transparency obligations without prejudice to the requirements and obligations for high-risk AI systems. In particular, natural persons should be notified that they are interacting with an AI system, unless this is obvious from the circumstances and the context of use. Moreover, natural persons should be notified when they are exposed **to systems that, by processing their biometric data, can identify or infer the emotions or intentions of those persons or assign them to specific categories. Such specific categories can relate to physical aspects, such as sex, age, hair colour, eye colour, ethnic origin or to personal preferences and interests such as sexual or political orientation.** ~~to an emotion recognition system or a biometric categorisation system~~. Such information and notifications		

PUBLIC

should be provided in accessible formats for persons with disabilities. Further, users, who use an AI system to generate or manipulate image, audio or video content that appreciably resembles existing persons, places or events and would falsely appear to a person to be authentic, should disclose that the content has been artificially created or manipulated by labelling the artificial intelligence output accordingly and disclosing its artificial origin. **The compliance with the information obligations referred to above should not be interpreted as indicating that the use of the system or its output is lawful under this Regulation or other Union and Member State law.**		
~~**(70a) In the light of the nature and complexity of the value chain for AI systems, it is essential to clarify the role of persons who may contribute to the development of AI systems covered by this Regulation, without**~~	(70a) In order to indicate the environmental footprint of AI systems as well as to allow users to differentiate between particularly sustainable or	For further explanations, see Article 52 (1, new).

PUBLIC

~~**being providers and thus being obliged to comply with the obligations and requirements established herein. In particular, it is necessary to clarify that general purpose AI systems - understood as AI system that are able to perform generally applicable functions such as image/speech recognition, audio/video generation, pattern detection, question answering, translation etc. - should not be considered as having an intended purpose within the meaning of this Regulation. Therefore the placing on the market, putting into service or use of a general purpose AI system, irrespective of whether it is licensed as open source software or otherwise, should not, as such, trigger any of the requirements or obligations of this Regulation. However, if a person places on the market or puts into service under its own name or trademark or uses a general purpose AI system made available on the market for**~~	unsustainable AI systems, the Commission shall be empowered to adopt delegated acts to establish a common scheme for describing and at a later stage rating the environmental sustainability of AI systems. The scheme shall only concern direct environmental impacts of AI systems. It shall be composed of easy-to-monitor key indicators such as the use of renewably powered or sustainably cooled data centres or the following of good programming practice concerning energy efficiency during AI development. To define these indicators, while taking into account the environmental significance, avoiding unnecessary burden by minimising monitoring and reporting and	

PUBLIC

~~**an intended purpose within the meaning of this Regulation, that person should be considered the provider of the AI system. Similarly, if a person integrates a general purpose AI system made available on the market, with or without modifying it, into an AI system that is subject to the provisions of this Regulation, that person should also be considered the provider of the latter AI system. The providers of general purpose AI systems and, as relevant, other third parties that may supply other software tools and components, including pre-trained models and data should cooperate, as appropriate, with providers and users to enable their compliance with the relevant obligations under this Regulation and with the competent authorities established under this Regulation.**~~	considering the possibility of exemptions for SME providers, relevant stakeholder from academia, enterprises, civil society and standardisation organisations shall be heard. This scheme does not impose any additional requirements for AI systems, nor does Union law require a specific outcome of the sustainability rating.	
(71) Artificial intelligence is a rapidly		

PUBLIC

developing family of technologies that requires novel forms of regulatory oversight and a safe space for experimentation, while ensuring responsible innovation and integration of appropriate safeguards and risk mitigation measures. To ensure a legal framework that is innovation-friendly, future-proof and resilient to disruption, national competent authorities from one or more Member States should be encouraged to establish artificial intelligence regulatory sandboxes to facilitate the development and testing of innovative AI systems under strict regulatory oversight before these systems are placed on the market or otherwise put into service.		
(72) The objectives of the **AI** regulatory sandboxes should be to foster AI innovation by establishing a controlled experimentation and testing environment in the development and pre-marketing phase with a view to ensuring		

PUBLIC

compliance of the innovative AI systems with this Regulation and other relevant Union and Member States legislation; to enhance legal certainty for innovators and the competent authorities' oversight and understanding of the opportunities, emerging risks and the impacts of AI use, and to accelerate access to markets, including by removing barriers for small and medium enterprises (SMEs)**, including** ~~and~~ start-ups. **The participation in the AI regulatory sandbox should focus on issues that raise legal uncertainty for providers and prospective providers to innovate and experiment with AI in the Union. The supervision of the AI systems in the AI regulatory sandbox should therefore cover their development, training, testing and validation before the systems are placed on the market or put into service, as well as the notion and occurrence of substantial modification that may require a new**		

PUBLIC

conformity assessment procedure. ~~**Access to the AI regulatory sandbox and regulatory supervision should be in principle free of charge without prejudice to exceptional costs that may be recovered by national authorities in a fair and proportionate manner, in particular in cases where the authorities have provided additional services for the actual development, testing and validation of the AI system such as technical or physical environment and tools for the testing, access to data, etc.**~~ To ensure uniform implementation across the Union and economies of scale, it is appropriate to establish common rules for the regulatory sandboxes' implementation and a framework for cooperation between the relevant authorities involved in the supervision of the sandboxes. This Regulation should provide the legal basis for the use of personal data collected ~~for other purposes~~ **for other purposes** for developing certain AI systems in the public		

PUBLIC

interest within the AI regulatory sandbox, in line with Article 6**(4)(~~1)(e)~~ and 9(2)(g)** of Regulation (EU) 2016/679, and Article 5 **and 10** of Regulation (EU) 2018/1725, and without prejudice to Article**s 4(2) ~~8~~ and 10** of Directive (EU) 2016/680. ~~**This new legal basis under this Regulation is without prejudice to the possibility for participants to rely on other legal bases for processing of personal data under Articles 6(1) and 9(2) of Regulation (EU) 2016/679 and Articles 5 and 10(2) of Regulation (EU) 2018/1725.**~~ **All other obligations of data controllers and rights of data subjects under Regulation (EU) 2016/679, Regulation (EU) 2018/1725 and Directive (EU) 2016/680 remain applicable. In particular, this Regulation should not provide a legal basis in the meaning of Article 22(2)(b) of Regulation (EU) 2016/679 and Article 24(2)(b) of Regulation (EU) 2018/1725.** Participants in the sandbox should		

PUBLIC

ensure appropriate safeguards and cooperate with the competent authorities, including by following their guidance and acting expeditiously and in good faith to mitigate any high-risks to safety and fundamental rights that may arise during the development and experimentation in the sandbox. The conduct of the participants in the sandbox should be taken into account when competent authorities decide whether to impose an administrative fine under Article 83(2) of Regulation 2016/679 and Article 57 of Directive 2016/680. **AI regulatory sandboxes established under this Regulation should be without prejudice to existing legislation allowing for the establishment of other sandboxes aiming at ensuring compliance with legislation other that this Regulation. Upon agreement between the national competent authorities and the participants in the AI regulatory sandbox, testing in real world conditions may**		

PUBLIC

also be operated and supervised in the framework of the AI regulatory sandbox.	[..] This Regulation should provide the legal basis for the use of personal data collected ~~for other purposes~~ **for other purposes** for developing certain AI systems in the public interest within the AI regulatory sandbox, in line with Article 6**(4)(~~1~~)(~~e~~) and 9(2)(g)** of Regulation (EU) 2016/679, and Article 5 **and 10** of Regulation (EU) 2018/1725, and without prejudice to Article**s 4(2) ~~8~~ and 10** of Directive (EU) 2016/680. **Article 54 is an Union law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23 (1) of Regulation (EU) 2016/679 and Article 25 (1) of Regulation (EU) 2018/1725.**	Add: *"Article 54 is an Union law..":* We support the Commission's proposal for further processing of personal data in regulatory sandboxes as an important means of promoting innovation, since the further processing would provide significant benefit the development of AI systems in the public interest.

PUBLIC

(72a) In order to accelerate the process of development and placing on the market of high risk AI systems listed in Annex III, it is important that providers or prospective providers of such systems may also benefit from a specific regime for testing those systems in real world conditions, without participating in an AI regulatory sandbox. However, in such cases and taking into account the possible consequences of such testing on individuals, it should be ensured that appropriate and sufficient guarantees and conditions are introduced by the Regulation for providers or prospective providers.		
(73) In order to promote and protect innovation, it is important that the interests of ~~small-scale~~**SME** providers and users of AI systems are taken into particular account. To		

PUBLIC

this objective, Member States should develop initiatives, which are targeted at those operators, including on awareness raising and information communication. Moreover, the specific interests and needs of ~~small scale~~**SME** providers shall be taken into account when ~~N~~**n**otified **b**~~B~~odies set conformity assessment fees. Translation costs related to mandatory documentation and communication with authorities may constitute a significant cost for providers and other operators, notably those of a smaller scale. Member States should possibly ensure that one of the languages determined and accepted by them for relevant providers' documentation and for communication with operators is one which is broadly understood by the largest possible number of cross-border users.		
(73a) In order to promote and protect innovation, the AI-on demand platform, all relevant EU funding programmes and		

PUBLIC

projects, such as Digital Europe Programme, Horizon Europe, implemented by the Commission and the Member States at national or EU level should contribute to the achievement of the objectives of this Regulation.		
(74) **In particular, i**~~I~~n order to minimise the risks to implementation resulting from lack of knowledge and expertise in the market as well as to facilitate compliance of providers, **notably SMEs,** and notified bodies with their obligations under this Regulation, the AI-on demand platform, the European Digital Innovation Hubs and the Testing and Experimentation Facilities established by the Commission and the Member States at national or EU level should possibly contribute to the implementation of this Regulation. Within their respective mission and fields of competence, they may provide in particular technical and		

PUBLIC

scientific support to providers and notified bodies.		
(74a) Moreover, in order to ensure proportionality considering the very small size of some operators regarding costs of innovation, it is appropriate to exempt microenterprises from the most costly obligations, such as to establish a quality management system which would reduce the administrative burden and the costs for those enterprises without affecting the level of protection and the need for compliance with the requirements for high-risk AI systems.		
(75) It is appropriate that the Commission facilitates, to the extent possible, access to Testing and Experimentation Facilities to bodies, groups or laboratories established or accredited pursuant to any relevant Union harmonisation legislation and which fulfil tasks		

PUBLIC

in the context of conformity assessment of products or devices covered by that Union harmonisation legislation. This is notably the case for expert panels, expert laboratories and reference laboratories in the field of medical devices pursuant to Regulation (EU) 2017/745 and Regulation (EU) 2017/746.		
(76) In order to facilitate a smooth, effective and harmonised implementation of this Regulation a European Artificial Intelligence Board should be established. **The Board should reflect the various interests of the AI eco-system and be composed of representatives of the Member States** ~~**and of permanent experts representing different stakeholders**~~. **In order to ensure the involvement of relevant stakeholders, a standing subgroup of the Board should be created.** The Board should be responsible for a number of advisory tasks, including issuing opinions, recommendations,		

PUBLIC

advice or **contributing to** guidance on matters related to the implementation of this Regulation, including on **enforcement matters,** technical specifications or existing standards regarding the requirements established in this Regulation and providing advice to ~~**and assisting**~~ the Commission **and the Member States and their national competent authorities** on specific questions related to artificial intelligence. **In order to give some flexibility to Member States in the designation of their representatives in the AI Board, such representatives may be any persons or public entities who should have the relevant competences and powers to facilitate coordination at national level and contribute to the achievement of the Board's tasks.**		
(76a) The Commission should actively support the Member States and operators in the implementation and enforcement of this		

PUBLIC

Regulation. In this regard it should develop guidelines on particular topics aiming at facilitating the application of this Regulation, while paying particular attention to the needs of SMEs and start-us in sectors most likely to be affected. In order to support adequate enforcement and the capacities of the Member States, Union testing facilities on AI and a pool of relevant experts should be established and made available to the Member States.		
(77) Member States hold a key role in the application and enforcement of this Regulation. In this respect, each Member State should designate one or more national competent authorities for the purpose of supervising the application and implementation of this Regulation. ~~In order to increase organisation efficiency on the side of Member States and to set an official point of contact vis-à-vis the~~		

PUBLIC

~~public and other counterparts at Member State and Union levels, in each Member State one national authority should be designated as national supervisory authority.~~ **Member States may decide to appoint any kind of public entity to perform the tasks of the national competent authorities within the meaning of this Regulation, in accordance with their specific national organisational characteristics and needs.**		
(78) In order to ensure that providers of high-risk AI systems can take into account the experience on the use of high-risk AI systems for improving their systems and the design and development process or can take any possible corrective action in a timely manner, all providers should have a post-market monitoring system in place. This system is also key to ensure that the possible risks emerging from AI systems which continue to 'learn' after being		

PUBLIC

placed on the market or put into service can be more efficiently and timely addressed. In this context, providers should also be required to have a system in place to report to the relevant authorities any serious incidents or any breaches to national and Union law protecting fundamental rights resulting from the use of their AI systems.		
(79) In order to ensure an appropriate and effective enforcement of the requirements and obligations set out by this Regulation, which is Union harmonisation legislation, the system of market surveillance and compliance of products established by Regulation (EU) 2019/1020 should apply in its entirety. **Although the majority of AI systems are not subject to specific requirements and obligations under this Regualtion, market surveillance authorities may take measures in relation to all AI systems when they present a risk in**	A specific safeguard procedure should be set for ensuring adequate and timely enforcement against AI systems presenting a risk to health, safety ~~and~~, fundamental rights and the environment.	In line with the inclusion of AI systems posing high risks to the environment in Annex III, 2.b) (new), the safeguard procedure should also ensure enforcement to prevent risks to the environment.

PUBLIC

accordance with this Regulation. Where necessary for their mandate, national public authorities or bodies, which supervise the application of Union law protecting fundamental rights, including equality bodies, should also have access to any documentation created under this Regulation. A specific safeguard procedure should be set for ensuring adequate and timely enforcement against AI systems presenting a risk to health, safety and fundamental rights. The procedure for such AI systems presenting a risk should be applied to high-risk AI systems presenting a risk, prohibited systems which have been placed on the market, put into service or used in violation of the prohibited practices laid down in this Regulation and AI systems which have been made available in violation of the transparency requirements laid down in this Regulation and present a risk.	Where necessary for their mandate, equality bodies as relevant national bodies in cases of discrimination, as well as other national public authorities or bodies, which supervise the application of Union law protecting fundamental rights should also have access to any documentation created under this Regulation.	

PUBLIC

(80) Union legislation on financial services includes internal governance and risk management rules and requirements which are applicable to regulated financial institutions in the course of provision of those services, including when they make use of AI systems. In order to ensure coherent application and enforcement of the obligations under this Regulation and relevant rules and requirements of the Union financial services legislation, the authorities responsible for the supervision and enforcement of the financial services legislation~~,~~ ~~including where applicable the European Central Bank,~~ should be designated as competent authorities for the purpose of supervising the implementation of this Regulation, including for market surveillance activities, as regards AI systems provided or used by regulated and supervised financial institutions. **It is appropriate to envisage that,**		

PUBLIC

when acting as market surveillance authorities under this Regulation, the national authorities responsible for the supervision of credit institutions regulated under Directive 2013/36/EU should report, without delay, to the European Central Bank any information identified in the course of their market surveillance activities that may be of potential interest for the European Central Bank's prudential supervisory tasks as specified in Council Regulation (EU) No 1204/2013 establishing the Single Supervisory Mechanism (SSM). To further enhance the consistency between this Regulation and the rules applicable to credit institutions regulated under Directive 2013/36/EU of the European Parliament and of the Council[27], it is also appropriate to integrate the conformity assessment procedure and some of the		

[27] Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC (OJ L 176, 27.6.2013, p. 338).

PUBLIC

providers' procedural obligations in relation to risk management, post marketing monitoring and documentation into the existing obligations and procedures under Directive 2013/36/EU. In order to avoid overlaps, limited derogations should also be envisaged in relation to the quality management system of providers and the monitoring obligation placed on users of high-risk AI systems to the extent that these apply to credit institutions regulated by Directive 2013/36/EU.		
(81) The development of AI systems other than high-risk AI systems in accordance with the requirements of this Regulation may lead to a larger uptake of trustworthy artificial intelligence in the Union. Providers of non-high-risk AI systems should be encouraged to create codes of conduct intended to foster the voluntary application of the mandatory requirements applicable to high-risk AI systems.		

PUBLIC

Providers should also be encouraged to apply on a voluntary basis additional requirements related, for example, to environmental sustainability, accessibility to persons with disability, stakeholders' participation in the design and development of AI systems, and diversity of the development teams. The Commission may develop initiatives, including of a sectorial nature, to facilitate the lowering of technical barriers hindering cross-border exchange of data for AI development, including on data access infrastructure, semantic and technical interoperability of different types of data.		
(82) It is important that AI systems related to products that are not high-risk in accordance with this Regulation and thus are not required to comply with the requirements set out herein are nevertheless safe when placed on the market or put into service. To contribute to this objective,		

PUBLIC

the Directive 2001/95/EC of the European Parliament and of the Council[28] would apply as a safety net.		
(83) In order to ensure trustful and constructive cooperation of competent authorities on Union and national level, all parties involved in the application of this Regulation should respect the confidentiality of information and data obtained in carrying out their tasks.		
(84) Member States should take all necessary measures to ensure that the provisions of this Regulation are implemented, including by laying down effective, proportionate and dissuasive penalties for their infringement, **and in respect of the *ne bis in idem* principle**. For certain specific infringements, Member States should take into account the margins and criteria		

[28] Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety (OJ L 11, 15.1.2002, p. 4).

PUBLIC

set out in this Regulation. The European Data Protection Supervisor should have the power to impose fines on Union institutions, agencies and bodies falling within the scope of this Regulation.		
(85) In order to ensure that the regulatory framework can be adapted where necessary, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission to amend the techniques and approaches referred to in Annex I to define AI systems, the Union harmonisation legislation listed in Annex II, the high-risk AI systems listed in Annex III, the provisions regarding technical documentation listed in Annex IV, the content of the EU declaration of conformity in Annex V, the provisions regarding the conformity assessment procedures in Annex VI and VII and the provisions establishing the high-risk AI systems to which the conformity		

PUBLIC

assessment procedure based on assessment of the quality management system and assessment of the technical documentation should apply. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making[29]. In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts. **Such consultations and advisory support should also be carried out in the framework of the**		

[29] OJ L 123, 12.5.2016, p. 1.

PUBLIC

activities of the AI Board and its subgroups.		
(86) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council[30]. **It is of particular importance that, in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making, whenever broader expertise is needed in the early preparation of draft implementing acts, the Commission makes use of expert groups, consults targeted stakeholders or carries out public consultations, as appropriate. Such consultations and advisory support should**		

[30] Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p.13).

PUBLIC

also be carried out in the framework of the activities of the AI Board and its subgroups, including the preparation of implementing acts in relation to Articles 4 and 6.		
(87) Since the objective of this Regulation cannot be sufficiently achieved by the Member States and can rather, by reason of the scale or effects of the action, be better achieved at Union level, the Union may adopt measures in accordance with the principle of subsidiarity as set out in Article 5 TEU. In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective.		
(87a) In order to ensure legal certainty, ensure an appropriate adaptation period for operators and avoid disruption to the market, including by ensuring continuity of		

PUBLIC

the use of AI systems, it is appropriate that this Regulation applies to the high-risk AI systems that have been placed on the market or put into service before the general date of application thereof, only if, from that date, those systems are subject to significant changes in their design or intended purpose. It is appropriate to clarify that, in this respect, the concept of significant change should be understood as equivalent in substance to the notion of substantial modification, which is used with regard only to high-risk AI systems as defined in this Regulation.		
(88) This Regulation should apply from … [*OP – please insert the date established in Art. 85*]. However, the infrastructure related to the governance and the conformity assessment system should be operational before that date, therefore the provisions on notified bodies and		

PUBLIC

governance structure should apply from … [*OP – please insert the date – three months following the entry into force of this Regulation*]. In addition, Member States should lay down and notify to the Commission the rules on penalties, including administrative fines, and ensure that they are properly and effectively implemented by the date of application of this Regulation. Therefore the provisions on penalties should apply from [*OP – please insert the date – twelve months following the entry into force of this Regulation*].		
(89) The European Data Protection Supervisor and the European Data Protection Board were consulted in accordance with Article 42(2) of Regulation (EU) 2018/1725 and delivered an opinion on […]".		
HAVE ADOPTED THIS REGULATION:		

PUBLIC

TITLE I		
GENERAL PROVISIONS		
Article 1 *Subject matter*		
This Regulation lays down:		
(a) harmonised rules for the placing on the market, the putting into service and the use of artificial intelligence systems ('AI systems') in the Union;		
(a) prohibitions of certain artificial intelligence practices;		The enumeration of the following paragraphs is wrong. This paragraph would have to follow as (b).
(b) specific requirements for high-risk AI systems and obligations for operators of such		

PUBLIC

systems;		
(c) harmonised transparency rules for **certain** AI systems ~~intended to interact with natural persons, emotion recognition systems and biometric categorisation systems, and AI systems used to generate or manipulate image, audio or video content~~;	(c) harmonised transparency rules for **certain** AI systems **and rights for natural persons** ~~intended to interact with natural persons, emotion recognition systems and biometric categorisation systems, and AI systems used to generate or manipulate image, audio or video content~~;	For DEU a right for natural persons need to be included in the AI Act. Otherwise, it would not be possible for individuals to legally address the impact of harmful AI applications with the user. However, regarding LEAs it might be necessary to amend or restrict certain rights of natural persons to ensure a balanced regulation – as in a feasible method to operate public administration, being bound to respect the fundamental rights of the individual as such.
(d) rules on market monitoring**,** ~~and~~ **market** surveillance **and governance**~~.;~~		
(e) measures in support of innovation.		
Article 2		*Regarding the scope, please refer to the*

PUBLIC

Scope		*separate position paper handed in, proposing necessary diverging regulations for public administration (especially LEAs and migration authorities) „[TITLE]“.*
1. 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 **physically present or** established within the Union or in a third country;		
(b) users of AI systems **who are physically present or established** ~~located~~ within the Union;		
(c) providers and users of AI systems ~~that~~ **who are physically present or established** ~~located~~ in a third country, where the output produced by the system is used in the Union;		

PUBLIC

(d) **importers and distributors of AI systems;**		
(e) **product manufacturers placing on the market or putting into service an AI system together with their product and under their own name or trademark;**		
(f) authorised representatives of providers, which are established in the Union;		
2. For **AI systems classified as** high-risk AI **systems in accordance with Articles 6(1) and 6(2) related to products covered by Union harmonisation legislation listed in Annex II, section B** ~~systems that are safety components of products or systems, or which are themselves products or systems, falling within the scope of the following acts~~ only Article**s 53 and** 84 of this Regulation shall apply**.**~~:~~		

PUBLIC

~~(a) Regulation (EC) 300/2008;~~		
~~(b) Regulation (EU) No 167/2013;~~		
~~(c) Regulation (EU) No 168/2013;~~		
~~(d) Directive 2014/90/EU;~~		
~~(e) Directive (EU) 2016/797;~~		
~~(f) Regulation (EU) 2018/858;~~		
~~(g) Regulation (EU) 2018/1139;~~		
~~(h) Regulation (EU) 2019/2144.~~		
3. This Regulation shall not apply to AI systems **if and insofar** ~~developed~~ **placed on the market or put into service** ~~or used [exclusively]~~ for **the purpose of activities**		Thank you very much for the draft of Article 2 (3) concerning AI systems for the purpose of activities which fall outside the scope of Union law! Regarding this paragraph, we have a

PUBLIC

which fall outside the scope of Union law, and in any event activities concerning military**, defence or national security** ~~purposes~~**, regardless of the type of entity carrying out those activities**.		comprehension question concerning the meaning of the words "and in any event": How is the second half of the sentence, introduced by the words "in any event", related to the first half of the sentence? Moreover, we would like to know why the development of AI is not expressly mentioned? In any case, it seems important to clarify that all activities which fall outside the scope of Union law are not within the scope of the regulation and that this includes the development of AI for the areas mentioned (in other words: It should be clear in the text of Art. 2 that not only the distribution or use is excluded from the scope of the AI Act but also the development for the mentioned purposes).
In addition, this Regulation shall not apply to AI systems which are not placed on the market or put into service in the Union, where the output is used in the Union for the purpose of activities which fall outside the		See above

PUBLIC

scope of Union law, and in any event activities concerning military, defence or national security.		
	(new) Member States remain free to take measures at national level to protect minors (persons below the age of 18 years) in accordance with UNCRC General Comment No. 25.	DEU considers it necessary to include an opening clause for the adoption of national rules in the area of protection of minors.
3a. Entities carrying out activities referred to in paragraph 3, shall not be subject to user's obligations provided for in this Regulation.		
4. This Regulation shall not apply to public authorities in a third country nor to international organisations falling within the scope of this Regulation pursuant to paragraph 1, where those authorities or organisations use AI systems in the framework of international agreements for law enforcement and judicial cooperation with the Union or with one or more Member States.		

PUBLIC

5. This Regulation shall not affect the application of the provisions on the liability of intermediary service providers set out in Chapter II, Section ~~IV~~**4** of Directive 2000/31/EC of the European Parliament and of the Council[31] [*as to be replaced by the corresponding provisions of the Digital Services Act*].		
6. This Regulation shall not apply to AI systems, including their output, specifically developed and put into service for the sole purpose of scientific research and development.		
7. **This Regulation shall not affect any research and development activity regarding**	or putting it into service within the scope of this regulation.	Due to the questions concerning the interpretation of Article 2 (3) it is not

[31] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') (OJ L 178, 17.7.2000, p. 1).

PUBLIC

AI systems in so far as such activity does not lead to or entail placing an AI system on the market or putting it into service.		sufficiently clear, if the development of AI for national security purposes is excluded from the scope of the AI-Act (see above). We suggest a clarification by the suggested addition in Article 2 (7).
	8. This Regulation is without prejudice to Union law on the protection of personal data, in particular Regulation (EU) 2016/679 and Directive 2002/58/EC including any supplementing provisions of national law (1) Member States may, by law or collective agreements, provide for more specific rules for	Please see our commentary regarding Article 62 para. 1 (line 170 of the Art. 56-end table). We appreciate further clarifications concerning the relationship between this Regulation and data protection law, but we suggest to include any supplementing provisi-ons of national law clearlier within the whole Regulation (see Recital 58a, for example Recital 9). The AI Act must not be a „regulatory ceiling“ for specific requirements imposed by Member States in the area of employment. The more

PUBLIC

	AI systems used in the employment context, in particular to ensure the protection of employees' rights, freedoms and health and safety at work.(2) Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to paragraph 1 and, without delay, any subsequent amendment affecting them	generalized rules of the AI Act might prove insufficient for the specific nature of the employment relationship with its structural imbalance of power. Therefore, it is necessary to ensure that Member States and social partners are still able to set more specific rules for AI deployed in the context of employment, without generally precluding the use of AI applications in the employment context. This includes requirements for employers deploying AI systems and grant rights to workers and their representatives regarding the use of AI at the workplace.
Article 3 *Definitions*		
For the purpose of this Regulation, the following definitions apply:		
~~(1) 'artificial intelligence system' (AI system) means software that is developed with one or~~		

PUBLIC

~~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;~~		
~~'artificial intelligence system' (AI system) means a system that~~		
~~(i) receives machine and/or human-based data and inputs,~~		
~~(ii) infers how to achieve a given set of human-defined objectives using learning, reasoning or modelling implemented with the techniques and approaches listed in Annex I, and~~		
~~(iii) generates outputs in the form of content (generative AI systems), predictions,~~		

PUBLIC

~~**recommendations or decisions, which influence the environments it interacts with;**~~		
'artificial intelligence system' (AI system) means a system that is designed to operate with a certain level of autonomy and that, based on machine and/or human-provided data and inputs, infers how to achieve a given set of human-defined objectives using machine learning and/or logic- and knowledge based approaches, and produces system-generated outputs such as content (generative AI systems), predictions, recommendations or decisions , influencing the environments with which the AI system interacts;	**'artificial intelligence system' (AI system) means a system that is designed to operate with elements ~~a certain level~~ of autonomy and that, based on machine and/or human-provided data and inputs, infers how to achieve a given set of human-defined objectives using machine learning and/or logic- and knowledge based approaches, and produces system-generated outputs such as content (generative AI systems), predictions, recommendations or decisions , influencing the environments with which the AI system interacts;**	For DEU, it is very important that the scope of the regulation is clear so providers know whether their systems have to comply with it. By contrast, the newly added requirement, that a system must be designed to operate with a "certain level of autonomy" in order to be classified as an AI system, creates legal uncertainty. Whilst DEU understands that autonomy is at present one of the signifying components of an AI system, a 'certain level' is too broad. The required threshold remains unclear at least until the CJEU provides further clarification. DEU therefore proposes 'elements of', since this is a prerequisite, which is verifiable – a system either operates with (elements of) autonomy, or it does not. DEU further suggests that the term 'autonomy'

PUBLIC

		may be defined or explained in the sense of this Directive in the recitals. In addition, it would be helpful to amend recital 6b.
(1a) 'life cycle of an AI system' means the duration of an AI system, from design through retirement. Such retirement may happen at any point in time during the post-market monitoring phase upon the decision of the provider and implies that the system may not be used further. An AI system lifecycle is also ended by a substantial modification to the AI system made by the provider or any other natural or legal person.	**(1a) 'life cycle of an AI system' means the duration of an AI system, from design through retirement. Such retirement may happen at any point in time during the post-market ~~monitoring~~ phase upon the decision of the provider and implies that the system may not be used further. An AI system lifecycle ~~is~~ may also ended by a substantial modification to the AI system made by the provider or any other natural or legal person.**	Clarification. Post-market monitoring is a task for providers. It is not a lifecycle phase. When serious incidents or other non-compliance occure e. g. in data governance, substantial modification are required to achieve compliance with the provisions of this Regulation. A substantial modification may end the lifecycle.
(1b) 'general purpose AI system' means an AI system that - irrespective of how ~~the~~		We welcome the provisions for exceptionsfor "general purpose AI systems". However, to

PUBLIC

~~modality in which~~ it is placed on the market or put into service, including as open source software - is intended by the provider to perform generally applicable functions such as image and speech recognition, audio and video generation, pattern detection, question answering, translation and others; a general purpose AI system may be used in a plurality of contexts and be integrated in a plurality of other AI systems;		some extent this leads to several questions regarding Data Protection Policies: We welcome the addition of a definition of general purpose AI. However, we still see the problem that classification as a GPAI seems solely to depend on the providers' intentions regarding his AI system. Most notably, it remains undefined *when* the provider's intention is to be determined (at the start of the development, during or after the launch of the market?), *by whom and how* (purely subjectively from the provider's point of view or more objectively, e.g. also from the supervisory authorities' perspective?). Furthermore, we wonder how the line would be drawn between "multiple-purpose AI" and "general purpose AI". If any AI system with more than one (very) specific purpose would be

PUBLIC

		considered GPAI, we wonder how many AI systems would consequently still fall under "normal" AI requirements under this Regulation. Our suggestion would be to make at least qualification as GPAI not only dependent on the provider's intentions.
(2) 'provider' means a natural or legal person, public authority, agency or other body that develops an AI system or that has an AI system developed **and places that system on the market or puts it into service** ~~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;		
~~(3) 'small-scale provider' means a provider that is a micro or small enterprise within the~~		

PUBLIC

~~meaning of Commission Recommendation 2003/361/EC[32];~~		
(3a) 'small and medium-sized enterprises' (SMEs) means an enterprise as defined in the Annex of Commission Recommendation 2003/361/EC concerning the definition of micro, small and medium-sized enterprises.		
(4) 'user' means 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~~;		
(5) 'authorised representative' means any natural or legal person ~~established~~ **physically present or established** in the Union who has received **and accepted** a written mandate from		

[32] Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36).

PUBLIC

a provider of an AI system to, respectively, perform and carry out on its behalf the obligations and procedures established by this Regulation;		
(5a) 'product manufacturer' means a manufacturer within the meaning of any of the Union harmonisation legislation listed in Annex II;		
(6) 'importer' means any natural or legal person ~~established~~ **physically present or established** in the Union that places on the market ~~or puts into service~~ an AI system that bears the name or trademark of a natural or legal person established outside the Union;		
(7) 'distributor' means any natural or legal person in the supply chain, other than the provider or the importer, that makes an AI system available on the Union market ~~without~~		

PUBLIC

~~affecting its properties~~;		
(8) 'operator' means the provider, the user, the authorised representative, the importer and the distributor;	'economic operators' shall mean the provider, the authorised representative, the importer and the distributor;	An adjusted definition of economic opera-tor of R1 of Decision 2008/768 should be used (provider instead of manufacturer).
	(new) 'operator' means any natural or legal person who is responsible for the operation of the company, public authority, agency or other facility in which the AI system is operated or used by employees.	An adjust definition of operator based on Ordinance on Operators of Medical Devices.
(9) 'placing on the market' means the first making available of an AI system on the Union market;		
(10) 'making available on the market' means any supply of an AI system for distribution or use on the Union market in the course of a commercial activity, whether in return for payment or free of charge;		
(11) 'putting into service' means the supply of		Does the reference to "own use" create a

PUBLIC

an AI system for first use directly to the user or for own use ~~on the Union market~~ **in the Union** for its intended purpose~~;~~**. ~~By way of derogation, field testing taking place under the conditions of Article 64a shall not be considered as putting into service;~~**		different scope than that provided for in the definition under the Regulation (EU) 2017/745 and 2017/746?
(12) 'intended purpose' means the use for which an AI system is intended by the provider, including the specific context and conditions of use, as specified in the information supplied by the provider in the instructions for use, promotional or sales materials and statements, as well as in the technical documentation**;** ~~**general purpose AI systems shall not be considered as having an intended purpose within the meaning of this Regulation;**~~		
		The draft does not define risk or harm while using these terms throughout the draft. Risk is used as a keyterm e. g. in the risk management and conformity assessment. (source: Legal

PUBLIC

		analysis - European legislativ proposal draft AI Act and MDR/IVDR, 2022). Having this in mind, does the presidency consider it necessary to define "risk"? We suggest to add the following definition, based on Regulation (EU) 2019/1020: 'risk' means the combination of the degree of severity of a harm and the probability of an occurrence of a hazard causing this harm to health, safety, information security or the probability of occurrence of harm caused by an adverse impact on the fundamental rights.
(13) 'reasonably foreseeable misuse' means the use of an AI system in a way that is not in accordance with its intended purpose, but which may result from reasonably foreseeable human behaviour or interaction with other systems;		Shall this definition also include a malfunctioning of the system due malicious cyber-attacks?

PUBLIC

(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;		
(15) 'instructions for use' means the information provided by the provider to inform the user of in particular an AI system's intended purpose and proper use ~~inclusive of the specific geographical, behavioural or functional setting within which the high-risk AI system is intended to be used~~;		
(16) 'recall of an AI system' means any measure aimed at achieving the return to the provider **or taking it out of service or disabling the use** of an AI system made available to users;		

PUBLIC

(17) 'withdrawal of an AI system' means any measure aimed at preventing **an AI system in the supply chain being made available on the market**~~. the distribution, display and offer of an AI system~~;		
(18) 'performance of an AI system' means the ability of an AI system to achieve its intended purpose;		
(19) **'conformity assessment' means the process of verifying whether the requirements set out in Title III, Chapter 2 of this Regulation relating to a~~n~~ high-risk AI system have been fulfilled;** ~~'notifying authority' means the national authority responsible for setting up and carrying out the necessary procedures for the assessment, designation and notification of conformity assessment bodies and for their monitoring;~~	**'conformity assessment' means the process of demonstrating ~~of verifying~~ whether the requirements set out in ~~Title III, Chapter 2 of~~ this Regulation relating to a~~n~~ high-risk AI system have been fulfilled;**	The exact wording of 'conformity assessment' of R1 of Decision 2008/768 should be used. **~~Title III, Chapter 2 of~~:** Taking into account other requirements, e. g. quality management system, post-market-surveilliance system, etc.

PUBLIC

(20) ~~'conformity assessment' means the process of verifying whether the requirements set out in Title III, Chapter 2 of this Regulation relating to an AI system have been fulfilled;~~ **'notifying authority' means the national authority responsible for setting up and carrying out the necessary procedures for the assessment, designation and notification of conformity assessment bodies and for their monitoring;**		
(21) 'conformity assessment body' means a body that performs third-party conformity assessment activities, including testing, certification and inspection;		
(22) 'notified body' means a conformity assessment body designated in accordance with this Regulation and other relevant Union harmonisation legislation;		

PUBLIC

(23) 'substantial modification' means a change to the AI system following its placing on the market or putting into service which affects the compliance of the AI system with the requirements set out in Title III, Chapter 2 of this Regulation, or ~~results in~~ a modification to the intended purpose for which the AI system has been assessed~~;~~**. For high-risk AI systems that continue to learn after being placed on the market or put into service, changes to the high-risk AI system and its performance that have been pre-determined by the provider at the moment of the initial conformity assessment and are part of the information contained in the technical documentation referred to in point 2(f) of Annex IV, shall not constitute a substantial modification.**	(23) 'substantial modification' means a change to the AI system following its placing on the market or putting into service which **exceeds updates and technical adaptations** and **results in a new assessement of the compliance** with the requirements set out in Title III, Chapter 2 of of this Regulation, or ~~results in~~ a modification to the intended purpose for which the AI system has been assessed~~;~~**. For high-risk AI systems that continue to learn after being placed on the market or put into service, changes to the high-risk AI system and its performance optimisation, except changes regarding the intended purpose and use, that have been pre-determined by the provider at the moment of the initial conformity assessment and are part of the information contained in the technical documentation referred to in point 2(f) of Annex IV, shall not constitute a substantial modification.**	We consider the term "affects" as too vague for practical use, therefore further clarification is needed. Furthermore, there is a need for AI systems that continues to learn after being placed on the market or put into service, changes should not constitute a substantial modification as follows: 1. allow changes to performance optimisation and minor software changes; 2. changes to the intended purpose and use must be excluded.

PUBLIC

	For AI systems related to products covered by the Machinery Regulation listed in Annex II, section A, the definition of "substantial modification" according to the Machinery Regulation listed in Annex II, section A applies.	This last addition is necessary in case that the AI system is related to a product covered by the Machinery Regulation listed in Annex II, section A. Otherwise, e.g. a substantially modified AI system, which is part of a machinery, would follow the definition for a substantial modification of the AI Regulation and not the definition for "substantial modification" according to the Machinery Regulation.
(24) 'CE marking of conformity' (CE marking)	'CE marking of conformity' (CE marking)	Taking into account other requirements, e. g.

PUBLIC

means a marking by which a provider indicates that an AI system is in conformity with the requirements set out in Title III, Chapter 2 **or in Article 4b** of this Regulation and other applicable Union ~~legislation~~ **legal act** harmonising the conditions for the marketing of products ('Union harmonisation legislation') providing for its affixing;	means a marking by which a provider indicates that an AI system is in conformity with the requirements set out in ~~Title III, Chapter 2 **or in Article 4b** of~~ this Regulation and other applicable Union ~~legislation~~ **legal act** harmonising the conditions for the marketing of products ('Union harmonisation legislation') providing for its affixing;	quality management system, post-market-surveilliance system, etc..
(25) 'post-market monitoring **system**' means all activities carried out by providers of AI systems to ~~proactively~~ collect and review experience gained from the use of AI systems they place on the market or put into service for the purpose of identifying any need to immediately apply any necessary corrective or preventive actions;	'post-market monitoring **system**' means all activities carried out by providers of AI systems to proactively collect and review experience gained from the use of AI systems they place on the market or put into service for the purpose of identifying any need to immediately apply any necessary corrective or preventive actions;	A proactive post-market monitoring system is mandatory especially to meet the requirements for preventive and corrective actions
(26) 'market surveillance authority' means the national authority carrying out the activities and taking the measures pursuant to Regulation		

PUBLIC

(EU) 2019/1020;		
(27) 'harmonised standard' means a European standard as defined in Article 2(1)(c) of Regulation (EU) No 1025/2012;		
(28) 'common specifications' means a **set of technical specifications** ~~document~~, other than a standard, ~~containing solutions,~~ providing ~~a~~ **mandatory** means to~~,~~ comply with certain requirements and obligations established under this Regulation;	(28) 'common specifications' means a **set of technical specifications** ~~document~~, other than a standard, developed according to section 41 of this Regulation ~~containing solutions,~~ providing ~~a~~ ~~**mandatory**~~ means to~~,~~ comply with ~~certain requirements and obligations~~ the essential requirements established under this Regulation;	
(29) 'training data' means data used for training an AI system through fitting its learnable parameters~~, including the weights of a neural network~~;	an AI ~~system~~ algorithm or model	An AI algorithm or model is the main part of the back-end of the AI system. The front-end of the AI system is not part of data or data governance and management practices.

PUBLIC

		The provider has to demonstrate that the trained, validated and tested AI algorithm or model achieves the intended purpose and the provider has to ensure bias monitoring detection and correction as well as performance, robustness and cybersecurity (prevent manipulation through "data poisoning"). As required under Article 9 (3), the provider shall also take into account the effects and possible interactions resulting from the design and development including training, validation and testing of the high-risk AI system. Having this in mind does the presidency consider it necessary to specify the general term „data" towards more specifically "labelled" data?
(30) 'validation data' means data used for providing an evaluation of the trained AI system and for tuning its non-learnable parameters and	an AI ~~system~~ algorithm or model	See comment above

PUBLIC

its learning process, among other things, in order to prevent overfitting; whereas the validation dataset can be a separate dataset or part of the training dataset, either as a fixed or variable split;		
(31) 'testing data' means data used for providing an independent evaluation of the trained and validated AI system in order to confirm the expected performance of that system before its placing on the market or putting into service;	an AI ~~system~~ algorithm or model	See comment above
(32) 'input data' means data provided to or directly acquired by an AI system on the basis of which the system produces an output;		
(33) 'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person,	(33) 'biometric data' means personal data **as defined in point 14 of Article 4 of Regulation (EU) 2016/679**	

PUBLIC

~~which allow or confirm the unique identification of that natural person,~~ such as facial images or dactyloscopic data;		
(34) 'emotion recognition system' means an AI system for the purpose of identifying or inferring emotions or intentions of natural persons on the basis of their biometric data;		
(35) 'biometric categorisation system' means an AI system for the purpose of assigning natural persons to specific categories~~, such as sex, age, hair colour, eye colour, tattoos,~~ **health, personal traits,** ~~ethnic origin or sexual or political orientation,~~ on the basis of their biometric data;		
(36) '~~remote~~ biometric identification system' means an AI system for the purpose of identifying **natural persons**~~, at a distance~~ through the comparison of a person's biometric		DEU assumes that the definition in Art. 3 para 36 („biometric identification systems") entails alternative exemptions (regarding „(…) and systems") and not a cumulative conditions to

PUBLIC

data with the biometric data contained in a reference ~~database~~ **data repository, excluding verification/authentification systems whose sole purpose is to confirm that a specific natural person is the person he or she claims to be, and systems that are used to confirm the identity of a natural person for the sole purpose of having access to a service, a device or premises;** ~~and without prior knowledge of the user of the AI system whether the person will be present and can be identified ;~~		fulfil the exemption?
(37) ''real-time' ~~remote~~ biometric identification system' means a ~~remote~~ biometric identification system whereby the capturing of biometric data, the comparison and the identification all occur **instantaneously or near instantaneously** ~~without a significant delay~~. ~~This comprises not only instant identification, but also limited short delays in order to avoid circumvention.~~		

PUBLIC

~~(38) ''post' remote biometric identification system' means a remote biometric identification system other than a 'real-time' remote biometric identification system;~~		
(39) 'publicly accessible space' means any **publicly or privately owned** physical place accessible to **an undetermined number of natural persons** ~~the public~~, regardless of whether certain conditions **or circumstances** for access **have been predetermined, and regardless of the potential capacity restrictions** ~~**may apply**~~;		
(40) 'law enforcement authority' means:		The definition is identical to the definition of "competent authority" in Directive (EU) 2016/680. Is the same meaning of different legal terms intended?
(a) any public authority competent for the		

PUBLIC

prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; or		
(b) any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;		
(41) 'law enforcement' means activities carried out by law enforcement authorities **or on their behalf** for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of		The term is not defined in the Directive (EU) 2016/680. This could lead to legal uncertainties when interpreting the Directive.

PUBLIC

threats to public security;		
~~(42) 'national supervisory authority' means the authority to which a Member State assigns the responsibility for the implementation and application of this Regulation, for coordinating~~ **~~the related~~** ~~activities~~ **~~of the national competent authorities~~** ~~entrusted to that Member State, for acting as the single contact point for the Commission, and for representing the Member State at the European Artificial Intelligence Board;~~		
(43) 'national competent authority' **means any of the following:** ~~the national supervisory authority,~~ the notifying authority~~, and~~ **and** the market surveillance authority~~;~~**. As regards EU institutions, agencies, offices and bodies, the EPDS shall act as a national competent authority, for the purposes of this Regulation;**		

PUBLIC

(44) 'serious incident' means any incident **or malfunctioning of an AI system** that directly or indirectly leads~~, might have led or might lead~~ to any of the following:	'serious incident' means any incident **or malfunctioning of an AI system** that directly or indirectly leads, might have led or might lead to any of the following:	For medical devices and IVDs post-market and vigilance system, it is necessary to match the definition of "serious incident" to the term in the Regulation (EU) 2017/746 and 2017/745.
(a) the death of a person or serious damage to a person's health~~, to property or the environment,~~	the death of a user or other person or the temporary or permanent serious deterioration of a patient's, user's or other person's state of health ~~serious damage to a person's health, to property or the environment, or~~ or a serious and irreversible public threat	See comment above
(b) a serious and irreversible disruption of the management and operation of critical infrastructure.	A serious ~~and irreversible~~ disruption of the management and operation of critical infrastructure.	See comment above
(c) breach of obligations under Union law intended to protect fundamental rights;		
(d) serious damage to property or the		

PUBLIC

environment;		
(45) 'critical infrastructure' means an asset, system or part thereof which is necessary for the delivery of a service that is essential for the maintenance of vital societal functions or economic activities within the meaning of Article 2(4) and (5) of Directive …../….. on the resilience of critical entities;	(45) 'critical infrastructure' means an asset, **facility, equipment, network,** system or part thereof, which is necessary for the ~~delivery~~ **provision of an essential service** ~~that is essential for the maintenance of vital societal functions or economic activities within the meaning~~ of Article 2(4) and (5) of Directive …../….. on the resilience of critical entities;	Adaptation to the directive on the resilience of critical facilities negotiated in parallel (CER-RL – 2020/0365 (COD)) based on the discussions in council working group ProCiv-CER regarding CER-DIRECTIVE.
(46) 'personal data' means data as defined in point (1) of Article 4 of Regulation (EU) 2016/679;		
(47) 'non-personal data' means data other than personal data as defined in point (1) of Article 4 of Regulation (EU) 2016/679.		
(48) 'testing in real world conditions' means the temporary testing of an AI system for its	**for its intended purpose ~~in real world conditions~~ outside of a laboratory or**	With regards to norm clarity we advise to delete "in real world conditions" as part of its own

PUBLIC

intended purpose in real world conditions outside of a laboratory or otherwise simulated environment with a view to gathering reliable and robust data and to assessing and verifying the conformity of the AI system with the requirements of this Regulation; testing in real world conditions shall not be considered as placing the AI system on the market or putting it into service within the meaning of this Regulation, provided that all conditions under Article 53 or Article 54a are fulfilled;	**otherwise simulated environment**	definition.
(49) 'real world testing plan' means a document that describes the objectives, methodology, geographical, population and temporal scope, monitoring, organisation and conduct of testing in real world conditions;		
(50) 'subject' for the purpose of real world testing means a natural person who	**'subject' for the purpose of ~~real world testing~~ testing in real world conditions means a**	"real world testing" is neither defined nor used in the regulation anywhere else.

PUBLIC

participates in ~~a real world~~ testing in real world conditions;	**natural person**	
(51) 'informed consent' means a subject's free and voluntary expression of his or her willingness to participate in a particular testing in real world conditions, after having been informed of all aspects of the testing that are relevant to the subject's decision to participate; in the case of minors and of incapacitated subjects, the informed consent shall be given by their legally designated representative;		Should "informed consent" be a different form of consent than in Art. 6 (1) lit a, 7 GDPR? If this is the case, we might suggest clarifying this in a recital. We suggest that the possibility to revoke consent be included directly here in the definition and not in Art. 54a (5).
(52) 'AI regulatory sandbox' means a concrete framework set up by a national competent authority which offers providers or prospective providers of AI systems the possibility to develop, train, validate and test, where appropriate in real world conditions, an innovative AI system, pursuant to a		

PUBLIC

specific plan for a limited time under regulatory supervision.		
Article 4 ~~*Amendments to Annex I*~~***Implementing acts***		
~~The Commission is empowered to adopt delegated acts~~ **In order to ensure uniform conditions for the implementation of this Regulation as regards machine learning approaches and logic- and knowledged based approaches referred to in Article 3(1), the Commission may adopt implementing acts to specify the technical elements of those approaches, taking into account market and technological developments. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 74(2).** ~~in accordance with Article 73 to amend the list of techniques and approaches listed in Annex I~~ ~~**within the scope**~~		

PUBLIC

~~**of the definition of an AI system as provided for in Article 3(1)**, in order to update that list to market and technological developments on the basis of characteristics that are similar to the techniques and approaches listed therein.~~		
	New Article: For High-risk AI systems covered by Regulation (EU) 2017/745 or Regulation (EU) 2017/746, the requirements set out in this regulation shall apply to the extent, to which these requirements are more specific than the sector specific requirements and provisions with the same objective, nature or effect, such as requirements on data and data governance, AI system validation and AI systems that continuously learn in the field.	This Regulation should complement and strengthen existing provisions such as Regulations (EU) 2017/745 and (EU) 2017/746 relating to the ensuring of compliance of medical device AI systems and controls on those products by notified bodies. However, because of the specific nature of and the specific risks related to medical device AI systems and in accordance with the principle of *lex specialis*, this Regulation should apply only in so far as there are no specific provisions with the same objective, nature or effect in Regulation 2017/745 and 2017/746. In so far the requirements of this Regulation on data and data governance, AI system validation, AI systems that continuously learn in the field and the

PUBLIC

		necessary qualification of Notified Bodies are fully applicable. Other provisions of this Regulation should not apply in the areas covered by more specific provisions set out in Regulations (EU) 2017/745 and (EU) 2017/746.
TITLE IA		
GENERAL PURPOSE AI SYSTEMS		
Article 4a		
Compliance of general purpose AI systems with this Regulation		
1. **Without prejudice to Articles 5 and 52 of this Regulation, general purpose AI systems shall only comply with the requirements and obligations set out in Article 4b.**		

PUBLIC

2. **Such requirements and obligations shall apply irrespective of whether the general purpose AI system is placed on the market or put into service as a pre-trained model and whether further fine-tuning of the model is to be performed by the user of the general purpose AI system.**		
Article 4b ***Requirements for general purpose AI systems and obligations for providers of such systems***		
1. General purpose AI systems which may be used as high risk AI systems or as components of AI high risk systems in the meaning of Article 6, shall comply with the requirements established in Articles, 9, 10, 11, 13(2) and 13(3)(a) to (c) and 13(3)(e) and 15 of this Regulation. When fulfilling those requirements, the generally acknowledged		This Article does not state *who* decides *when* as to whether a general purpose AI system (GPAI) may be used as a high risk AI system. However, this seems to be a crucial point: If the providers would be the (only) ones to decide on possible (future) uses of their GPAI, regulations proposed in this Article could easily be circumvented by placing a disclaimer such as

PUBLIC

state of the art shall be taken into account, including as reflected in relevant harmonised standards or common specifications.	**~~including as reflected in relevant harmonised standards or common specifications.~~**	"Not intended for high-risk uses as defined by the EU's AI Act" in the terms and conditions or user instructions. Does the Presidency see this risk as well? In general, the application of harmonised standards and common specifications is voluntary. By pointing out harmonised standards and common specifications in this context it sounds like a required mandatory application.
2. Providers of general purpose AI systems referred to in paragraph 1 shall		

PUBLIC

comply with the obligations set out in Articles 16aa, 16e, 16f, 16g, 16i, 16j, 25, 48 and 61.		
3. For the purpose of complying with the obligations set out in Article 16e, providers shall follow the conformity assessment procedure based on internal control set out in Annex VI, points 3 and 4.		
4. Providers of such systems shall also keep the technical documentation referred to in Article 11 at the disposal of the national competent authorities for a period ending ten years after the general purpose AI system is placed on the Union market or put into service in the Union.		
5. Providers of general purpose AI systems shall cooperate with and provide the necessary information to other providers intending to put into service or place such		From our understanding, this would only cover the case that a provider puts a GPAI onto the market or into service and *another* provider decides to use it for a more specific purpose. Is

PUBLIC

systems on the Union market as high-risk AI systems or as components of high-risk AI systems, with a view to enabling the latter to comply with their obligations under this Regulation. Such cooperation between providers shall preserve, as appropriate, intellectual property rights, and confidential business information or trade secrets.		this understanding correct? If so, what would happen if - the GPAI provider *himself* decides later on to use his system for a more specific purpose; here, it should be clearly regulated that this provider would then have to comply to all relevant requirements for high-risk AI, including the then-applicable conformity assessment; - a *user*, without being provider, uses a provider's GPAI in a high-risk context (putting it into service, but not under their own name or trademark); for example, an image recognition AI for analysis of photos of applicants in a recruitment process; how would compliance with high-risk AI requirements be ensured here?
6. In complying with the requirements and obligations referred to in paragraphs 1, 2 and 3:		

PUBLIC

- any reference to the intended purpose shall be understood as referring to possible use of the general purpose AI systems as high risk AI systems or as components of AI high risk systems in the meaning of Article 6; **- any reference to the requirements for high-risk AI systems in Chapter II, Title III shall be understood as referring only to the requirements set out in the present Article.**		
Article 4c ***Exceptions to Article 4b***		
1. Article 4b shall not apply when the provider has explicitly excluded any high-risk uses in the instructions of use or information accompanying the general purpose AI system.		
2. Such exclusion shall be made in good		

PUBLIC

faith and shall not be deemed justified if the provider has sufficient reasons to consider that the system may be misused.		
3. When the provider detects or is informed about statistically significant trends of market misuse, they shall take all necessary measures to prevent such further misuse.		
TITLE II		
PROHIBITED ARTIFICIAL INTELLIGENCE PRACTICES		
Article 5		
1. The following artificial intelligence practices shall be prohibited:		Remote real-time biometric identification in public spaces through AI must be ruled out by European law. However, retrograde biometric

PUBLIC

		identification, e.g. during the evaluation of evidence, must not be ruled out by European law. DEU reserves the right to an in-depth comment regarding biometric identification systems at a later stage, final discussions are still ongoing.
(a) the placing on the market, putting into service or use of an AI system that deploys subliminal techniques beyond a person's consciousness **with the objective to or the effect of** ~~in order to~~ materially distort**ing** a person's behaviour in a manner that causes or is **reasonably** 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		

PUBLIC

persons due to their age, ~~physical or~~ ~~mental~~ disability **or social or economic situation**, **with the objective to or the effect of** ~~in order to~~ materially distort**ing** the behaviour of a person pertaining to that group in a manner that causes or is **reasonably** 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:		We assume that paragraph 1 c) is only intended to prohibit so-called social scoring. We therefore assume that it will still be possible to use AI in the context of security background checks. We also assume, that systems which are operated in connection with the systems listed in Annex IX, are not prohibited under paragraph 1 c). Both must be ensured and must not be restricted by the prohibition in letter c).
(i) detrimental or unfavourable treatment of certain natural persons or ~~whole~~ groups thereof in social contexts which are unrelated to the		

PUBLIC

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 disproportionate to their social behaviour or its gravity;		
(d) the use of 'real-time' ~~remote~~ biometric identification systems in publicly accessible spaces **by law enforcement authorities or on their behalf** for the purpose of law enforcement, unless and in as far as such use is strictly necessary for one of the following objectives:		Remote real-time biometric identification in public spaces through AI must be ruled out by European law. However, retrograde biometric identification, e.g. during the evaluation of evidence, must not be ruled out by European law. DEU reserves the right to an in-depth comment regarding biometric identification systems at a later stage, final discussions are still ongoing.
(i) the targeted search for specific potential		

PUBLIC

victims of crime~~, including missing children~~;		
(ii) the prevention of a specific **and** substantial ~~and imminent~~ threat to **the critical infrastructure,** life**, health** or physical safety of natural persons or **the prevention** of ~~a~~ terrorist attack**s**;		
(iii) the ~~detection,~~ localisation~~,~~ **or** identification ~~or prosecution~~ of a **natural person for the purposes of conducting a criminal investigation, prosecution or executing a criminal penalty for offences** ~~perpetrator~~**,** ~~or~~ ~~suspect~~ ~~**or convict** of a criminal offence~~ referred to in Article 2(2) of Council Framework Decision 2002/584/JHA[33] and punishable in the Member State concerned by a custodial sentence or a detention order for a		

[33] Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (OJ L 190, 18.7.2002, p. 1).

PUBLIC

maximum period of at least three years, **or other specific offences punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least five years,** as determined by the law of that Member State.		
	(g) AI systems that substitute human judges in judicial proceedings when issuing judicial decisions on the merits; (h) AI systems intended to be used by law enforcement authorities for making individual risk assessments of natural persons in order to assess the risk of a natural person for offending or reoffending; (i) AI systems intended to be used by public authorities as polygraphs and similar tools or to	AI systems should in no event be used to replace human judges. To ensure this, mere regulation through classification as high-risk AI is not sufficient in our view. Thus, we suggest to explicitly include this aspect in the list of prohibited AI.

PUBLIC

	detect the emotional state of a natural person (j) the placing on the market, putting into service or use of an AI system that is for comprehensive, systematic surveillance and monitoring employee performance and behaviour without a specific reason and that is suited to creating psychological pressure to adapt in a way that significantly inhibits employees in their self-determination and the free development of their personality.	Certain AI systems used in the work environment can enable employers to systematically and comprehensively monitor their employees. Especially in a digital work environment, such systems can monitor almost every step of an employee and, for example, process data on communication, applications used or an employee's search history. Using this data, these AI systems can accurately track employee performance and behavior, generate scores on an employees' likelihood of quitting or their productivity, indicate which employees might be spreading negative sentiment, and ultimately create comprehensive profiles of employees. If an employer monitors his

PUBLIC

		workforce in this way without a specific reason, it can lead to immense psychological pressure and endanger the mental health of employees. In order to effectively deal with these dangers, it is necessary to ensure that systems designed for such a purpose cannot be legally placed on the market in the first place.
2. The use of 'real-time' ~~remote~~ biometric identification systems in publicly accessible spaces for the purpose of law enforcement for any of the objectives referred to in paragraph 1 point d) shall take into account the following elements:		
(a) the nature of the situation giving rise to the possible use, in particular the seriousness, probability and scale of the harm caused in the absence of the use of the system;		
(b) the consequences of the use of the system for the rights and freedoms of all persons		

PUBLIC

concerned, in particular the seriousness, probability and scale of those consequences.		
In addition, the use of 'real-time' ~~remote~~ biometric identification systems in publicly accessible spaces for the purpose of law enforcement for any of the objectives referred to in paragraph 1 point d) shall comply with necessary and proportionate safeguards and conditions in relation to the use, in particular as regards the temporal, geographic and personal limitations.		
3. As regards paragraphs 1, point (d) and 2, each ~~individual~~ use for the purpose of law enforcement of a 'real-time' ~~remote~~ biometric identification system in publicly accessible spaces shall be subject to a prior authorisation granted by a judicial authority or by an independent administrative authority of the Member State in which the use is to take place,		

PUBLIC

issued upon a reasoned request and in accordance with the detailed rules of national law referred to in paragraph 4. However, in a duly justified situation of urgency, the use of the system may be commenced without an authorisation ~~and the authorisation may be requested only during or after the use~~ **provided that, such authorisation shall be requested without undue delay during ~~its~~ use of the AI system, and if such authorisation is rejected, its use shall be stopped with immediate effect.**		
The competent judicial or administrative authority shall only grant the authorisation where it is satisfied, based on objective evidence or clear indications presented to it, that the use of the 'real-time' ~~remote~~ biometric identification system at issue is necessary for and proportionate to achieving one of the objectives specified in paragraph 1, point (d), as identified in the request. In deciding on the		

PUBLIC

request, the competent judicial or administrative authority shall take into account the elements referred to in paragraph 2.		
4. A Member State may decide to provide for the possibility to fully or partially authorise the use of 'real-time' ~~remote~~ biometric identification systems in publicly accessible spaces for the purpose of law enforcement within the limits and under the conditions listed in paragraphs 1, point (d), 2 and 3. That Member State shall lay down in its national law the necessary detailed rules for the request, issuance and exercise of, as well as supervision **and reporting** relating to, the authorisations referred to in paragraph 3. Those rules shall also specify in respect of which of the objectives listed in paragraph 1, point (d), including which of the criminal offences referred to in point (iii) thereof, the competent authorities may be authorised to use those systems for the purpose		

PUBLIC

of law enforcement.		
4a. ~~The prohibition mentioned in Article 5(1)(d) shall not apply to situations where the person refuses or is not a capacity to disclose his or her identity in front of the law enforcement authority in publicly accessible spaces when that authority is authorised by Union or national law to carry out such identity checks.~~ The prohibition mentioned in Article 5(1)(d) is without prejudice to the use of information systems by law enforcement, migration or asylum authorities of systems referred to in annex IX where these authorities are authorized by Union or national law to carry out identity checks.		DEU reserves the right to an in-depth comment regarding biometric identification systems at a later stage, final discussions are still ongoing. We also refer to our comment regarding Art. 5 I c)
TITLE III		
HIGH-RISK AI SYSTEMS		

PUBLIC

CHAPTER 1		
CLASSIFICATION OF AI SYSTEMS AS HIGH-RISK		
Article 6 *Classification rules for high-risk AI systems*		
~~1. Irrespective of whether an AI system is placed on the market or put into service independently from the products referred to in points (a) and (b), that AI system shall be considered high-risk where both of the following conditions are fulfilled:~~		
~~(a) the AI system is intended to be used as a safety component of a product, or is itself a product, covered by the Union harmonisation legislation listed in Annex II;~~		

PUBLIC

~~(b) 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.~~		
~~2. In addition to the high-risk AI systems referred to in paragraph 1, AI systems referred to in Annex III shall also be considered high-risk.~~		
1. **An AI system that is itself a product covered by the Union harmonisation legislation listed in Annex II shall be considered as high risk if it 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**		

PUBLIC

to the above mentioned legislation.		
2. **An AI system intended to be used as a safety component of a product covered by the legislation referred to in paragraph 1 shall be considered as high risk if it 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 above mentioned legislation. This provision shall apply irrespective of whether the AI system is placed on the market or put into service independently from the product.**		
3. **AI systems referred to in Annex III shall be considered high-risk in any of the following cases:**	**Deletion**	While we understand the intend of the presidency's work this proposal falls short in many regards so we propose its deletion. As we understand it, the provider must make the

PUBLIC

		assessment to determine whether its AI system is a high-risk AI system. Under the new proposal, this classification now depends not only on the area of application chosen, but also on the specific use in each case. This will not be known to the provider, so he will have to anticipate typical use cases. However, he will hardly be able to ensure that his AI system will later only be used for these specific use cases in individual cases. In this respect, there is a lack of enforcement possibilities. The intended powers of the market surveillance authorities against providers does not lead any further, since the duty of users to use the system as intended in Art. 29(1) only applies to high-risk AI systems. In addition, supervisory rights of the authorities against individual users are per se not very effective in enforcing the law. Also missing are obligations of the provider for non-high-risk systems, e.g. documentation obligations on how he reached his classification.

PUBLIC

		Currently, the proposal therefore contains numerous possibilities for circumvention and leads to gaps in protection.
(a) the output of the system is immediately effective with respect to the intended purpose of the system without the need for a human to validate it;	Deletion	
(b) the output of the system consists of information that constitutes the sole basis or is not purely accessory in respect of the relevant action or decision to be taken by the human, and may therefore lead to a significant risk to the health, safety or fundamental rights.	Deletion	
In order to ensure uniform conditions for the implementation of this Regulation, the Commission shall, no later than one year after the entry into force of this Regulation,	Deletion	

PUBLIC

adopt implementing acts to specify further the purely accessory nature of the information across the relevant high-risk AI systems referred to in Annex III. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 74, paragraph 2.		
Article 7 *Amendments to Annex III*		Please refer to our comment to Art. 73 regarding consultation obligations.
1. The Commission is empowered to adopt delegated acts in accordance with Article 73 to ~~update~~ **amend** the list in Annex III by adding high-risk AI systems where both of the following conditions are fulfilled:		
(a) the AI systems are intended to be used in any of the areas listed in points 1 to 8 of Annex III;		

PUBLIC

(b) the AI systems pose a risk of harm to the health and safety, or a risk of adverse impact on fundamental rights, that is, in respect of its severity and probability of occurrence, equivalent to or greater than the risk of harm or of adverse impact posed by the high-risk AI systems already referred to in Annex III.	(b) the AI systems pose a risk of harm to the health and safety, or a risk of adverse impact on fundamental rights or the environment, that is, in respect of its severity and probability of occurrence, equivalent to or greater than the risk of harm or of adverse impact posed by the high-risk AI systems already referred to in Annex III.	In the evaluation of risks stemming from AI systems it is important to consider risks to the environment that are not immediately linked to personal health and safety but threaten human well-being in the long run. This risk potential arises from e.g. technical errors due to insufficient training data or testing of AI systems, which are used to control industrial processes and may lead to accidents and environmental damages. This addition of environmental risks mirrors Annex 2.b) (new).
2. When assessing for the purposes of paragraph 1 whether an AI system poses a risk of harm to the health and safety or a risk of adverse impact on fundamental rights that is equivalent to or greater than the risk of harm posed by the high-risk AI systems already referred to in Annex III, the Commission shall take into account the following criteria:		

PUBLIC

(a) the intended purpose of the AI system;		
(b) the extent to which an AI system has been used or is likely to be used;		
(c) the extent to which the use of an AI system has already caused harm to the health and safety or adverse impact on the fundamental rights or has given rise to significant concerns in relation to the materialisation of such harm or adverse impact, as demonstrated by reports or documented allegations submitted to national competent authorities;		
(d) the potential extent of such harm or such adverse impact, in particular in terms of its intensity and its ability to affect a plurality of persons;		
(e) the extent to which potentially harmed or adversely impacted persons are dependent on		

PUBLIC

the outcome produced with an AI system, in particular because for practical or legal reasons it is not reasonably possible to opt-out from that outcome;		
(f) the extent to which potentially harmed or adversely impacted persons are in a vulnerable position in relation to the user of an AI system, in particular due to an imbalance of power, knowledge, economic or social circumstances, or age;	(f) the extent to which potentially harmed or adversely impacted persons are in a vulnerable position in relation to the user of an AI system, in particular due to an imbalance of power, knowledge, economic or social circumstances, ~~physical or mental~~ disability or age;	
(g) the extent to which the outcome produced with an AI system is easily reversible, whereby outcomes having an impact on the health or safety of persons shall not be considered as easily reversible;		
(h) the extent to which existing Union legislation provides for:		

PUBLIC

(i) effective measures of redress in relation to the risks posed by an AI system, with the exclusion of claims for damages;		
(ii) effective measures to prevent or substantially minimise those risks.		
3. The Commission is empowered to adopt delegated acts in accordance with Article 73 to amend the list in Annex III by deleting high-risk AI systems where the following conditions are fulfilled:	**Deletion**	
(a) the high-risk AI system(s) concerned no longer pose any significant risks to fundamental rights, health or safety, taking into account the criteria listed in paragraph 2;	**Deletion**	
(b) the deletion does not decrease the overall level of protection of health, safety	**Deletion**	

PUBLIC

and fundamental rights under Union law.		
CHAPTER 2		
REQUIREMENTS FOR HIGH-RISK AI SYSTEMS		
Article 8 *Compliance with the requirements*		
1. High-risk AI systems shall comply with the requirements established in this Chapter**, taking into account the generally acknowledged state of the art, including as reflected in relevant harmonised standards or common specifications**.	~~**including as reflected in relevant harmonised standards or common specifications**~~.	In general, the application of harmonised standards and common specifications is voluntary. By pointing out harmonised standards and common specifications in this context it sounds like a required mandatory application.
2. The intended purpose of the high-risk AI system and the risk management system referred to in Article 9 shall be taken into account when		

PUBLIC

ensuring compliance with those requirements.		
Article 9 *Risk management system*		
1. A risk management system shall be established, implemented, documented and maintained in relation to high-risk AI systems.		
2. The risk management system shall consist of a continuous iterative process run throughout the entire lifecycle of a high-risk AI system, requiring regular systematic updating. It shall comprise the following steps:	The risk management system shall ~~consist of~~ be understood as a continuous iterative process run throughout the entire lifecycle of a high-risk AI system, requiring regular systematic updating. It shall comprise the following steps:	Clarification, an iterative process is an approach for tasks or projects, etc.
	(new a) establish and document a risk management plan for the AI system;	A risk management plan is necessary to implement continuous iterative processes throughout the entire lifecycle.
(a) identification and analysis of the known and foreseeable risks **most likely to occur to health, safety and fundamental rights in view of the intended purpose of the high-risk AI**	(b) identification and analysis of the known and foreseeable risks **most likely to occur to health, safety ~~and~~, fundamental rights and the environment in view of the intended**	As key measure to prevent risks from materializing, risks to the environment should also be identified, analysed and mitigated (cf. 7.b).

PUBLIC

system ~~associated with each high-risk AI system~~;	**purpose of the high-risk AI system,** including taking into account information security and data protection**.** ~~associated with each high-risk AI system~~	
	(new c) estimation and evaluation of risks associated with data and data governance	Taking into account risks related to Data and Data governance.
~~(b) estimation and evaluation of the risks that may emerge when the high-risk AI system is used in accordance with its intended purpose and under conditions of reasonably foreseeable misuse;~~	(new d) estimation and evaluation of risks associated with the possible negative interaction between the high-risk AI system and the environment within which it operates and interacts, including taking into account information security and data protection;	Taking into account risks related to the technical environment, information security and data protection.
(c) evaluation of other possibly arising risks based on the analysis of data gathered from the	(~~e~~ e)	

PUBLIC

post-market monitoring system referred to in Article 61;		
(d) adoption of suitable risk management measures in accordance with the provisions of the following paragraphs.	(~~d~~ f) ~~adoption of suitable risk management measures in accordance with the provisions of the following paragraphs.~~ eliminate or control the risks referred to in point (c) to (e) in accordance with the requirements of Chapter 2	Risk elimination and control is a main part of a risk management system.
The risks referred to in this paragraph shall concern only those which may be reasonably mitigated or eliminated through the development or design of the high-risk AI system, or the provision of adequate technical information.	~~**The risks referred to in this paragraph shall concern only those which may be reasonably mitigated or eliminated through the development or design of the high-risk AI system, or the provision of adequate technical information.**~~	The formulation "risks referred to this paragraph shall concern only those which may be reasonably mitigated or eliminated through development or design […] or provision of adequate technical information" limited risks and does not taking into account risks related to the environment, cybersecurity, post-market monitoring, etc..
3. The risk management measures referred to in paragraph 2, point (d) shall give due		

PUBLIC

consideration to the effects and possible interaction resulting from the combined application of the requirements set out in this Chapter 2**, with a view to minimising risks more effectively while achieving an appropriate balance in implementing the measures to fulfil those requirements**. ~~They shall take into account the generally acknowledged state of the art, including as reflected in relevant harmonised standards or common specifications.~~		
4. The risk management measures referred to in paragraph 2, point (d) shall be such that any residual risk associated with each hazard as well as the overall residual risk of the high-risk AI systems is judged acceptable~~, provided that the high-risk AI system is used in accordance with its intended purpose or under conditions of reasonably foreseeable misuse. Those residual risks shall be communicated to the user.~~		

PUBLIC

In identifying the most appropriate risk management measures, the following shall be ensured:		
(a) elimination or reduction of **identified and evaluated** risks as far as possible through adequate design and development **of the high risk AI system**;		
(b) where appropriate, implementation of adequate mitigation and control measures in relation to risks that cannot be eliminated;		
(c) provision of adequate information pursuant to Article 13, in particular as regards the risks referred to in paragraph 2, point (b) of this Article, and, where appropriate, training to users.		
In eliminating or reducing risks related to the	In eliminating or reducing risks related to the	From DEU point of view, the adequate risk-

PUBLIC

use of the high-risk AI system, due consideration shall be given to the technical knowledge, experience, education, training to be expected by the user and the environment in which the system is intended to be used.	use of the high-risk AI system, due consideration shall be given to the technical knowledge, experience, education, training to be expected by the user and the environment in which the system is intended to be used **and if the high-risk AI system is used by a public authority if the provider of this high-risk AI system also is a public authority.**	management system for AI systems may have to be altered if used in a case of public governance, for example if touching aspects of fundamental rights, organizational or operational considerations. Since these special aspects may vary depending on the circumstances of each individual case, in terms of aggravation or simplification of the measure at stake, the proposed clarification should be included.
5. High-risk AI systems shall be tested for the purposes of identifying the most appropriate risk management measures. Testing shall ensure that high-risk AI systems perform consistently for their intended purpose and they are in compliance with the requirements set out in this Chapter.	~~High-risk AI systems shall be tested for the purposes of identifying the most appropriate risk management measures. Testing shall ensure that high-risk AI systems perform consistently for their intended purpose and they are in compliance with the requirements set out in this Chapter.~~	Software can only be verified and/or validated. A risk management measure or risk control has to eliminate or control risks and cannot be found trough testing, e. g. software penetration tests can be used to identify gaps in software design, but not to identify appropriate risk management measures. Every identified risk management measure or risk control has to be evaluated. Because of the continuous iterative process, the effect of the

PUBLIC

		risk management measure will be evaluated continuously.
6. Testing procedures shall be suitable to achieve the intended purpose of the AI system ~~and do not need to go beyond what is necessary to achieve that purpose~~. **Testing procedures may include testing in real world conditions in accordance with Article 54a.**	~~Testing procedures shall be suitable to achieve the intended purpose of the AI system and do not need to go beyond what is necessary to achieve that purpose. **Testing procedures may include testing in real world conditions in accordance with Article 54a.**~~	See comment above.
7. The testing of the high-risk AI systems shall be performed, as appropriate, at any point in time throughout the development process, and, in any event, prior to the placing on the market or the putting into service. Testing shall be made against preliminarily defined metrics and probabilistic thresholds that are appropriate to the intended purpose of the high-risk AI system.	~~The testing of the high-risk AI systems shall be performed, as appropriate, at any point in time throughout the development process, and, in any event, prior to the placing on the market or the putting into service. Testing shall be made against preliminarily defined metrics and probabilistic thresholds that are appropriate to the intended purpose of the high-risk AI system.~~	See comment above.
8. ~~When implementing t~~**T**he risk		

PUBLIC

management system described in paragraphs 1 to 7 **shall give** specific consideration **to** ~~shall be given to~~ whether the high-risk AI system is likely to be accessed by or have an impact on **persons under the age of 18** ~~children~~.		
	(new) The characteristics and performance of a high-risk AI system shall not be adversely affected to such a degree that the health or safety of the user and, where applicable, of other persons are compromised during the lifetime of the high-risk AI system, as indicated by the provider, when the high-risk AI system is subjected to the stresses which can occur during normal conditions of use.	Entire lifecycle approach.
9. For credit institutions regulated by Directive 2013/36/EU, the aspects described in paragraphs 1 to 8 shall be part of the risk management procedures established by those institutions pursuant to Article 74 of that Directive.		

PUBLIC

Article 10 *Data and data governance*		
1. 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.	validation and testing data sets ~~that meet the quality criteria referred to in paragraphs 2 to 5~~.	Not every requirement in paragraph 2 to 5 do contain a quality criteria, e. g. practices in paragraph 2.
2. Training, validation and testing data sets shall be subject to appropriate data governance and management practices. Those practices shall concern in particular,		
(a) the relevant design choices;		
	(new b) the formulation of relevant assumptions, that are required by the intended purpose, the	Some more specific requirements are needed to clarify the process of how to get usable data. These State of the art practices in a logical order based on the Questionnaire „Artificial

PUBLIC

	characteristics or elements that are particular to the specific geographical, behavioural or functional setting within which the high-risk AI system is intended to be used; (new c) an assessment of the availability, quantity and suitability of the data sets that are needed; (new d) the specification of the inclusion and exclusion criteria for data on the basis of relevant 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; (new e) the specification of the needed number of data	Intelligence (AI) in medical devices“from the German Notified Bodies Alliance and Guideline for AI for medical devices by Christian Johner, Christoph Molnar et. al..

PUBLIC

	sets based on statistical power;	
(b) data collection **processes**;	(~~b~~ f) data collection ~~**processes**~~;	The requirements in paragraph 2 are part of the data collection process.
(c) relevant data preparation processing operations, such as annotation, labelling, cleaning, enrichment and aggregation;	(~~c~~ g)	
(d) the formulation of relevant assumptions, notably with respect to the information that the data are supposed to measure and represent;	~~(d) the formulation of relevant assumptions, notably with respect to the information that the data are supposed to measure and represent;~~	Move forward to lit. new b.
(e) a prior assessment of the availability, quantity and suitability of the data sets that are needed;	~~(e) a prior assessment of the availability, quantity and suitability of the data sets that are needed;~~	Move forward to lit. new c
(f) examination in view of possible biases **that are likely to affect health and safety of persons or lead to discrimination prohibited by Union law**;	(~~f~~ h)examination in view of possible biases, **in particular that are likely to affect the health ~~and~~ or safety of persons or lead to discrimination captured ~~prohibited~~ by Union law**;	We do not see the necessity to restrict the field of biases to the aforementioned. Furthermore, "prohibited" also includes the rejection of possible justifications under

PUBLIC

		discrimination law. The consideration of individual cases that this requires is very difficult. The requirement could therefore easily be circumvented. Instead, we propose that the regulated grounds of discrimination be sufficient. Furthermore, why does the provision only entail discrimination prohibited by Union law and not also by national law?
(g) the identification of any possible data gaps or shortcomings, and how those gaps and shortcomings can be addressed.	(~~g~~ i)	
3. Training, validation and testing data sets shall be relevant, representative, **and to the best extent possible,** 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		DEU discusses how it can be ensured that the specifications in the regulation correspond to the current state of the art in the development of AI and the current scientific standard for ensuring AI that is as error-free and unbiased as possible. In this context, the question is raised, for example, to what extent a requirement that

PUBLIC

used. These characteristics of the data sets may be met at the level of individual data sets or a combination thereof.		training data be "error-free" corresponds to the current state of scientific research on AI development that is as error- and bias-free as possible. What is the view of the Commission or other Member States on this issue?
4. Training, validation and testing data sets shall take into account, to the extent required by the intended purpose, the characteristics or elements that are particular to the specific geographical, behavioural or functional setting within which the high-risk AI system is intended to be used.	~~4. Training, validation and testing data sets shall take into account, to the extent required by the intended purpose, the characteristics or elements that are particular to the specific geographical, behavioural or functional setting within which the high-risk AI system is intended to be used.~~	Move forward to paragraph 2 lit new b.
5. To the extent that it is strictly necessary for the purposes of ensuring bias monitoring, detection and correction in relation to the high-risk AI systems, the providers of such systems may process special categories of personal data referred to in Article 9(1) of Regulation (EU) 2016/679, Article 10 of Directive (EU)	5. To the extent that it is strictly necessary for the purposes of ensuring bias monitoring, detection and correction in relation to the high-risk AI systems, the providers of such systems may process special categories of personal data referred to in Article 9(1) of Regulation (EU) 2016/679, Article 10 of Directive (EU)	Anonymisation should be named as a preferred measure; pseudonymisation/encryption should be a subordinate alternative. LEAs already use anonymised data as far as possible.

PUBLIC

2016/680 and Article 10(1) of Regulation (EU) 2018/1725, subject to appropriate safeguards for the fundamental rights and freedoms of natural persons, including technical limitations on the re-use and use of state-of-the-art security and privacy-preserving measures, such as pseudonymisation, or encryption where anonymisation may significantly affect the purpose pursued.	2016/680 and Article 10(1) of Regulation (EU) 2018/1725, subject to appropriate safeguards for the fundamental rights and freedoms of natural persons, including technical limitations on the re-use and use of state-of-the-art security and privacy-preserving measures, such as **anonymization, or** pseudonymisation, or encryption where anonymisation may significantly affect the purpose pursued.	
6. **For the development of high-risk AI systems not using techniques involving the training of models, paragraphs 2 to 5 shall apply only to the testing data sets.**	~~6. **For the development of high-risk AI systems not using techniques involving the training of models, paragraphs 2 to 5 shall apply only to the testing data sets.**~~	Move to new Article 10a (1)
~~Appropriate data governance and management practices shall apply for the development of high-risk AI systems other than those which make use of techniques involving the training of models in order to ensure that those high-risk AI systems comply with~~		

PUBLIC

~~paragraph 2.~~		
~~**6a. In order to comply with the requirements laid out in this Article, the data minimisation principle referred to in Article 5 paragraph 1c of Regulation (EU) 2016/679 shall be applied with consideration for the full life cycle of the system.**~~		
	New Article 10a Model training 1. For high-risk AI systems which make use of techniques involving the training of algorithms and models, the providers shall specify the stratification it uses to divided up the data in to training, validation and testing data. For the development of high-risk AI systems not using techniques involving the training of	There are no rules specify the model training. The state of the art practices based on Questionnaire „Artificial Intelligence (AI) in medical devices“ in a logical order from the German Notified Bodies Alliance and Guideline for AI for medical devices by Christian Johner, Christoph Molnar et. al..

PUBLIC

	models, paragraphs Article 10 (2) to (5) shall apply only to the testing data sets. 2. Providers shall perform the algorithm or model training through fitting its learnable parameters, with the training data, an evaluation of the trained algorithm and model and for tuning its non-learnable parameters and its learning process, among other things, in order to prevent overfitting, with the validation data (cross-validation). The provider should train and validate reasonable different algorithms and models and compare the results. The provider shall document, characteristics and parameters made and the results obtained.	

PUBLIC

	3. The provider shall test the high-risk AI system with independent test data in a simulated or actual user environment.	
Article 11 *Technical documentation*		
1. The technical documentation of a high-risk AI system shall be drawn up before that system is placed on the market or put into service and shall be kept up-to date.		For reasons of secrecy and protection of methods, updating the technical documentation pursuant to Art. 11 Par. 1 for a provider is also viewed critically as soon as the AI system is used in the law enforcement area. Could a solution in this area also be to shift certain obligations under Article 16 from the provider to the user, if and to the extent that state secrecy interests require this? Do the Commission or other Member States also see these issues?
The technical documentation shall be drawn up in such a way to demonstrate that the high-risk AI system complies with the requirements set out in this Chapter and provide national		

PUBLIC

competent authorities and notified bodies with all the necessary information to assess the compliance of the AI system with those requirements. It shall contain, at a minimum, the elements set out in Annex IV **or, in the case of SMEs, including ~~and~~ start-ups, any equivalent documentation meeting the same objectives, subject to approval of the competent authority**.		
2. Where a high-risk AI system related to a product, to which the legal acts listed in Annex II, section A apply, is placed on the market or put into service one single technical documentation shall be drawn up containing all the information set out in Annex IV as well as the information required under those legal acts.		
3. The Commission is empowered to adopt delegated acts in accordance with Article 73 to amend Annex IV where necessary to ensure		

PUBLIC

that, in the light of technical progress, the technical documentation provides all the necessary information to assess the compliance of the system with the requirements set out in this Chapter.		
Article 12 *Record-keeping*		Art. 12 shall entail expressedly state that sectoral data privacy provisions must prevail, similar to Art. 20 and 29 para 5. Otherwise Art. 12 poses a risk to establish a prohibited manner of data retention regarding personal data. A mere reference in the recitals is not sufficient.
1. High-risk AI systems shall ~~be designed and developed with capabilities enabling~~ **technically allow for** the automatic recording of events ('logs') **over the duration of the life cycle of the system** ~~while the high-risk AI systems is operating~~. ~~Those logging capabilities shall conform to recognised standards or common specifications.~~	1. High-risk AI systems shall ~~be designed and developed with capabilities enabling~~ **technically allow for** the automatic recording of events ('logs'), including output data and interim results as well as stop points requiring human intervention (audit records), **over the duration of the life cycle of the system** ~~while the high-risk AI systems is operating~~. ~~Those~~	To increase explainability, traceability and trust of an AI system in event of a serious incident, especially in healthcare sector. For human intervention, see Article 14 (4) lit. e.

PUBLIC

	~~logging capabilities shall conform to recognised standards or common specifications.~~	
2. ~~The logging capabilities shall ensure~~ **In order to ensure** a level of traceability of the AI system's functioning ~~throughout its lifecycle~~ that is appropriate to the intended purpose of the system~~,~~. ~~3. In particular,~~ logging capabilities shall enable the **recording of events relevant for** ~~monitoring of the operation of the high-risk AI system with respect to the occurrence of~~		
(i) identification of situations that may result in the AI system presenting a risk within the meaning of Article 65(1) or ~~lead to~~ **in** a substantial modification**;**~~, and~~		
(ii) ~~facilitate~~ **facilitation of** the post-market monitoring referred to in Article 61~~.~~**; and**		

PUBLIC

(iii) monitoring of the operation of high-risk AI systems referred to in Article 29(4).		
4. For high-risk AI systems referred to in paragraph 1, point (a) of Annex III, the logging capabilities shall provide, at a minimum:		
(a) recording of the period of each use of the system (start date and time and end date and time of each use);		
(b) the reference database against which input data has been checked by the system;		
(c) the input data for which the search has led to a match;		
(d) the identification of the natural persons involved in the verification of the results, as referred to in Article 14 (5).		

PUBLIC

Article 13 *Transparency and provision of information to users*		
1. High-risk AI systems shall be designed and developed in such a way to ensure that their operation is sufficiently transparent ~~to enable users to interpret the system's output and use it appropriately. An appropriate type and degree of transparency shall be ensured,~~ with a view to achieving compliance with the relevant obligations of the user and of the provider set out in Chapter 3 of this Title **and enabling users to understand and use the system appropriately**.	~~High-risk AI systems shall be designed and developed in such a way to ensure that their operation is sufficiently transparent to enable users to interpret the system's output and use it appropriately. An appropriate type and degree of transparency shall be ensured, with a view to achieving compliance with the relevant obligations of the user and of the provider set out in Chapter 3 of this Title **and enabling users to understand and use the system appropriately**.~~	Design and developing rule. Moved to modified Article 15.
2. High-risk AI systems shall be accompanied by instructions for use in an appropriate digital format or otherwise that include concise, complete, correct and clear information that is relevant, accessible and		

PUBLIC

comprehensible to users.		
3. The information referred to in paragraph 2 shall specify:		
(a) the identity and the contact details of the provider and, where applicable, of its authorised representative;		
(b) the characteristics, capabilities and limitations of performance of the high-risk AI system, including:		
(i) its intended purpose**, inclusive of the specific geographical, behavioural or functional setting within which the high-risk AI system is intended to be used**;		
(ii) the level of accuracy, **including its metrics,** robustness and cybersecurity referred to in Article 15 against which the high-risk AI		

PUBLIC

system has been tested and validated and which can be expected, and any known and foreseeable circumstances that may have an impact on that expected level of accuracy, robustness and cybersecurity;		
(iii) any known or foreseeable circumstance, related to the use of the high-risk AI system in accordance with its intended purpose ~~or under conditions of reasonably foreseeable misuse~~, which may lead to risks to the health and safety or fundamental rights **referred to in Aricle 9(2)**;		
(iv) **when appropriate,** its ~~performance~~ **behaviour regarding specific** ~~as regards the~~ persons or groups of persons on which the system is intended to be used;		
(v) when appropriate, specifications for the input data, or any other relevant information in		

PUBLIC

terms of the training, validation and testing data sets used, taking into account the intended purpose of the AI system.		
(c) the changes to the high-risk AI system and its performance which have been pre-determined by the provider at the moment of the initial conformity assessment, if any;		
(d) the human oversight measures referred to in Article 14, including the technical measures put in place to facilitate the interpretation of the outputs of AI systems by the users;		
(e) **the computational and hardware resources needed,** the expected lifetime of the high-risk AI system and any necessary maintenance and care measures to ensure the proper functioning of that AI system, including as regards software updates~~.~~**;**		

PUBLIC

(f) a description of the mechanism included within the AI system that allows users to properly collect, store and interpret the logs, where relevant.		
Article 14 *Human oversight*		
1. High-risk AI systems shall be designed and developed in such a way, including with appropriate human-machine interface tools, that they can be effectively overseen by natural persons during the period in which the AI system is in use.		
2. Human oversight shall aim at preventing or minimising the risks to health, safety or fundamental rights that may emerge when a high-risk AI system is used in accordance with its intended purpose or under conditions of reasonably foreseeable misuse, in particular		

PUBLIC

when such risks persist notwithstanding the application of other requirements set out in this Chapter.		
3. Human oversight shall be ensured through either one or all of the following **types of** measures:		
(a) **measures** identified and built, when technically feasible, into the high-risk AI system by the provider before it is placed on the market or put into service;		
(b) **measures** identified by the provider before placing the high-risk AI system on the market or putting it into service and that are appropriate to be implemented by the user.		
4. ~~The measures referred to in paragraph 3 shall enable the individuals~~ **For the purpose of implementing paragraphs 1 to 3, the high-**		

PUBLIC

risk AI system shall be provided to the user in such a way that natural persons to whom human oversight is assigned **are enabled,** ~~to do the following~~, as appropriate **and proportionate** to the circumstances:		
(a) ~~fully~~ **to** understand the capacities and limitations of the high-risk AI system and be able to duly monitor its operation~~, so that signs of anomalies, dysfunctions and unexpected performance can be detected and addressed as soon as possible~~;		
(b) **to** remain aware of the possible tendency of automatically relying or over-relying on the output produced by a high-risk AI system ('automation bias')~~, in particular for high-risk AI systems used to provide information or recommendations for decisions to be taken by natural persons~~;		

PUBLIC

(c) ~~be able~~ to correctly interpret the high-risk AI system's output, taking into account **for example** ~~in particular~~ ~~the characteristics of the system and~~ the interpretation tools and methods available;		
(d) ~~be able~~ to decide, in any particular situation, not to use the high-risk AI system or otherwise disregard, override or reverse the output of the high-risk AI system;		
(e) ~~be able~~ to intervene on the operation of the high-risk AI system or interrupt the system through a "stop" button or a similar procedure.		
5. For high-risk AI systems referred to in point 1(a) of Annex III, the measures referred to in paragraph 3 shall be such as to ensure that, in addition, no action or decision is taken by the user on the basis of the identification resulting from the system unless this has been **separately**		The DEU security authorities are concerned whether the provisions on the four-eyes principle in Article 14 (5) of the Draft Regulation in the area of law enforcement could cover cases of application that currently exist for procedures within the meaning of Annex III

PUBLIC

verified and confirmed by at least two natural persons.		No. 1 a) of the Draft Regulation and, in particular, could also affect constellations in which only one person acts on the side of the authority authorized to intervene, so that the four-eyes principle provided for in the AI Regulation could lead to disproportionate compliance costs in this respect. Please also refer to the separate position paper handed in, proposing necessary diverging regulations for public administration (especially LEAs and migration authorities) „[TITLE]“.

PUBLIC

Article 15 *Accuracy, robustness and cybersecurity*	*Article 15* ~~*Accuracy, robustness and cybersecurity*~~ *Design principles*	For a better understanding in particular for providers, moved main design requirements into one single Article and rename. Rename the Article. Furthermore, from a technical point of view, "performance"instead of "accuracy" would be the appropriate and correct term in the regulation. Accuracy is only one of many different performance metrics (such as precision, recall, F1 score); in many cases, accuracy is actually not the best measure for assessing the performance of an AI system. Restricting performance regulation artificially to accuracy is, from a technical point of view, quite unconvincing.
	(new 1.)	Based on Annex I Nr. 17.1 Regulation (EU) 2017/745 (essential requirement for Medical

PUBLIC

	AI systems shall be designed and developed in accordance with the state of the art taking into account the principles of development life cycle, risk management, including information security, as well as the AI systems verification and validation.	Device Software - principle of software-development).
1. High-risk AI systems shall be designed and developed in such a way that they achieve, in the light of their intended purpose, an appropriate level of accuracy, robustness and cybersecurity, and perform consistently in those respects throughout their lifecycle.	~~1~~ 2. High-risk AI systems shall be designed and developed in such a way that they achieve, in the light of their intended purpose, an appropriate level of ~~accuracy,~~ performance criteria, e. g. robustness and cybersecurity, for the high-risk AI system and the used algorithm or model as well as ~~and~~ perform consistently in those respects throughout their lifecycle, in particular the expected value ranges of output data.	The accuracy of an AI system is unclear. AI systems have the ability to do tasks without explicitly programmed. The provider cannot predict the performance like with standard software. The provider can predict performance criteria and expected value ranges of output data based on risk management measures, data governance, data modelling, etc. See above: Performance instead of accuracy would have to be adapted throughout the Regulation
2. The levels of accuracy and the relevant accuracy metrics of high-risk AI systems shall	~~2~~ 3. The levels of ~~accuracy~~ expected value ranges of output data and the relevant	Accuracy is itself a metric so there is only one "accuracy metric"

PUBLIC

be declared in the accompanying instructions of use.	performance metrics ~~accuracy metrics~~ of high-risk AI systems shall be declared in the accompanying instructions of use.	
3. High-risk AI systems shall be resilient as regards errors, faults or inconsistencies that may occur within the system or the environment in which the system operates, in particular due to their interaction with natural persons or other systems.		
The robustness of high-risk AI systems may be achieved through technical redundancy solutions, which may include backup or fail-safe plans.	~~The robustness of high-risk AI systems~~ These may be achieved through technical redundancy solutions	Wording
High-risk AI systems that continue to learn after being placed on the market or put into service shall be developed in such a way to ensure that possibly biased outputs ~~due to outputs used as~~ **influencing** ~~an~~ input for future operations	shall be developed in such a way to ~~ensure that~~ eliminate or reduce as far as possible the risk of possibly biased outputs	Risks of possibly biased output has to be eliminate or reduce as far as possible.

PUBLIC

('feedback loops') are duly addressed with appropriate mitigation measures.		
4. High-risk AI systems shall be resilient as regards attempts by unauthorised third parties to alter their use or performance by exploiting the system vulnerabilities.		
The technical solutions aimed at ensuring the cybersecurity of high-risk AI systems shall be appropriate to the relevant circumstances and the risks.		
The technical solutions to address AI specific vulnerabilities shall include, where appropriate, measures to prevent and control for attacks trying to manipulate the training dataset ('data poisoning'), inputs designed to cause the model to make a mistake ('adversarial examples'), or model flaws.		

PUBLIC

	new 5. High-risk AI systems shall be designed and developed ~~in such a way to ensure that their operation is sufficiently transparent~~ to enable users to interpret the system's output and use it appropriately (explainability of the AI algorithm and model). ~~An appropriate type and~~ A high degree of transparency shall be ensured, with a view to achieving compliance with the relevant ~~obligations of the user and of the provider~~ requirement set out in this regulation ~~Chapter 3 of this Title~~ ~~**and enabling users to understand and use the system appropriately**~~. new 6. High-risk AI systems that are intended to be used in combination with mobile computing platforms shall be designed and developed taking into account the specific features of the	Moved from Article 13 (1).

PUBLIC

	mobile platform and the external factors related to their use.	
CHAPTER 3		
OBLIGATIONS OF PROVIDERS AND USERS OF HIGH-RISK AI SYSTEMS AND OTHER PARTIES		
Article 16 *Obligations of providers of high-risk AI systems*		In DEU it is being discussed whether further requirements for the protection of confidentiality interests must be established in Art. 16 for cases in which high-risk AI systems of a (private) provider are used in the law enforcement area. Specifically, one solution could be that the information required under Article 16 of the Draft Regulation is not transmitted to the national authority by the (private) provider, but rather by the user directly. Please also see our seperate paper titled [TITLE] on this issue.

PUBLIC

Providers of high-risk AI systems shall:	1.	Due to inserting para 2 below
(a) ensure that their high-risk AI systems are compliant with the requirements set out in Chapter 2 of this Title;		
(aa) indicate their name, registered trade name or registered trade mark, the address at which they can be contacted on the high-risk AI system or, where that is not possible, on its packaging or its accompanying documentation, as applicable;		
(b) have a quality management system in place which complies with Article 17;		
(c) ~~draw up~~ **keep** the ~~technical~~ documentation **referred to in Article 18** ~~of the high-risk AI system~~;		

PUBLIC

(d) when under their control, keep the logs automatically generated by their high-risk AI systems **as referred to in Article 20**;		
(e) ensure that the high-risk AI system undergoes the relevant conformity assessment procedure **as referred to in Article 43**, prior to its placing on the market or putting into service;		
(f) comply with the registration obligations referred to in Article 51;		
(g) take the necessary corrective actions **as referred to in Article 21**, if the high-risk AI system is not in conformity with the requirements set out in Chapter 2 of this Title;		
(h) inform the national competent authorities of the Member States in which they made the AI system available or put it into service and, where applicable, the notified body of the non-		

PUBLIC

compliance and of any corrective actions taken;		
(i) to affix the CE marking to their high-risk AI systems to indicate the conformity with this Regulation in accordance with Article 49;		
(j) upon request of a national competent authority, demonstrate the conformity of the high-risk AI system with the requirements set out in Chapter 2 of this Title.		
	2. For providers of high-risk AI systems which are credit institutions regulated by Directive 2013/36/EU or entities regulated by Directive 2009/138/EC, Directive (EU) 2016/2341, Directive 2014/65/EU resp. Directive (EU) 2015/2366, Directive 2009/65/EG and Directive 2011/61/EU, the requirements regarding high-risk AI defined in Annex III 5. b are limited to the requirements set out in paragraph 1 (i) and Article 51of this regulation [potentially Article 52a].	As the entities regulated by Directive 2013/36/EU, Directive 2009/138/EC, Directive (EU) 2016/2341, Directive 2014/65/EU, Directive (EU) 2015/2366, Directive 2009/65/EG resp. Directive 2011/61/EU already follow highest standards and double regulation has to be avoided, these entities should be exempt from requirements already laid down in sector-specific regulation.

PUBLIC

Article 17 *Quality management system*		
1. Providers of high-risk AI systems shall put a quality management system in place that ensures compliance with this Regulation. That system shall be documented in a systematic and orderly manner in the form of written policies, procedures and instructions, and shall include at least the following aspects:		
(a) a strategy for regulatory compliance, including compliance with conformity assessment procedures and procedures for the management of modifications to the high-risk AI system;		
(b) techniques, procedures and systematic actions to be used for the design, design control and design verification of the high-risk AI system;		

PUBLIC

(c) techniques, procedures and systematic actions to be used for the development, quality control and quality assurance of the high-risk AI system;		
(d) examination, test and validation procedures to be carried out before, during and after the development of the high-risk AI system, and the frequency with which they have to be carried out;		
(e) technical specifications, including standards, to be applied and, where the relevant harmonised standards are not applied in full, the means to be used to ensure that the high-risk AI system complies with the requirements set out in Chapter 2 of this Title;		
(f) systems and procedures for data management, including data collection, data		

PUBLIC

analysis, data labelling, data storage, data filtration, data mining, data aggregation, data retention and any other operation regarding the data that is performed before and for the purposes of the placing on the market or putting into service of high-risk AI systems;		
(g) the risk management system referred to in Article 9;		
(h) the setting-up, implementation and maintenance of a post-market monitoring system, in accordance with Article 61;		
(i) procedures related to the reporting of serious incidents ~~and of malfunctioning~~ in accordance with Article 62;		
(j) the handling of communication with national competent authorities, competent authorities, including sectoral ones, providing or		

PUBLIC

supporting the access to data, notified bodies, other operators, customers or other interested parties;		
(k) systems and procedures for record keeping of all relevant documentation and information;		
(l) resource management, including security of supply related measures;		
(m) an accountability framework setting out the responsibilities of the management and other staff with regard to all aspects listed in this paragraph.		
2. The implementation of aspects referred to in paragraph 1 shall be proportionate to the size of the provider's organisation.		
3. For providers that are credit institutions regulated by Directive 2013/36/ EU, the		

PUBLIC

obligation to put **in place** a quality management system ~~**in place**~~ **with the exception of paragraph 1, points (g), (h) and (i)** 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. In that context, any harmonised standards referred to in Article 40 of this Regulation shall be taken into account.		
Article 18 ~~*Obligation to draw up technical documentation*~~ ***Documentation keeping***		
1. ~~Providers of high-risk AI systems shall draw up the technical documentation referred to in Article 11 in accordance with Annex IV.~~ **The provider shall, for a period ending 10 years after the AI system has been placed on the market or put into service, keep at the disposal of the national competent**		

PUBLIC

authorities:		
(a) the technical documentation referred to in Article 11;		
(b) the documentation concerning the quality management system referred to in Article 17;		
(c) the documentation concerning the changes approved by notified bodies where applicable;		
(d) the decisions and other documents issued by the notified bodies where applicable;		
(e) the EU declaration of conformity referred to in Article 48.		
1a. Each Member State shall determine		

PUBLIC

conditions under which the documentation referred to in paragraph 1 remains at the disposal of the national competent authorities for the period indicated in that paragraph for the cases when a provider or its authorised representative established on its territory goes bankrupt or ceases its activity prior to the end of that period.		
2. Providers that are credit institutions regulated by Directive 2013/36/EU shall maintain the technical documentation as part of the documentation concerning internal governance, arrangements, processes and mechanisms pursuant to Article 74 of that Directive.		
Article 19 *Conformity assessment*		
1. Providers of high-risk AI systems shall		

PUBLIC

ensure that their systems undergo the relevant conformity assessment procedure in accordance with Article 43, prior to their placing on the market or putting into service. Where the compliance of the AI systems with the requirements set out in Chapter 2 of this Title has been demonstrated following that conformity assessment, the providers shall draw up an EU declaration of conformity in accordance with Article 48 and affix the CE marking of conformity in accordance with Article 49.		
2. For high-risk AI systems referred to in point 5(b) of Annex III that are placed on the market or put into service by providers that are credit institutions regulated by Directive 2013/36/EU, the conformity assessment shall be carried out as part of the procedure referred to in Articles 97 to101 of that Directive.	~~For high-risk AI systems referred to in point 5(b) of Annex III that are placed on the market or put into service by providers that are credit institutions regulated by Directive 2013/36/EU, the conformity assessment shall be carried out as part of the procedure referred to in Articles 97 to101 of that Directive~~	It is not feasible to carry out the internal product-oriented conformity assessment as part of the procedure referred to in Art. 97 to 101 in the Directive 2013/36/EU. The ICT-related part of SREP is based on a questionnaire that institutions fill out in self-disclosure. The main focus of the questions is process related and does not target technical aspects such as

PUBLIC

		development details concerning AI- or any other ICT- Systems. Moreover, it is not clear why the conformity assessesment of credit institutions would seemingly include the involvement of a supervisory authority, whereas for all other AI systems in point 2 to 8 of Annex III, an assessment based on internal control is sufficient.
Article 20 *Automatically generated logs*		
1. Providers of high-risk AI systems shall keep the logs automatically generated by their high-risk AI systems, to the extent such logs are under their control by virtue of a contractual arrangement with the user or otherwise by law. ~~The logs shall be kept~~ **They shall keep them** for a period **of at least six months, unless provided otherwise in** ~~that is appropriate in the light of the intended purpose of high-risk AI~~		

PUBLIC

~~system and~~ applicable ~~legal obligations under~~ Union or national law**, in particular in Union law on the protection of personal data**.		
2. Providers that are credit institutions regulated by Directive 2013/36/EU shall maintain the logs automatically generated by their high-risk AI systems as part of the documentation under Articles 74 of that Directive.		
Article 21 *Corrective actions*		
Providers of high-risk AI systems which consider or have reason to consider that a high-risk AI system which they have placed on the market or put into service is not in conformity with this Regulation shall **immediately investigate, where applicable, the causes in collaboration with the reporting user and**		

PUBLIC

~~immediately~~ take the necessary corrective actions to bring that system into conformity, to withdraw it or to recall it, as appropriate. They shall inform the distributors of the high-risk AI system in question and, where applicable, the authorised representative and importers accordingly.		
Article 22 *Duty of information*		
Where the high-risk AI system presents a risk within the meaning of Article 65(1) and that risk is known to the provider of the system, that provider shall immediately inform the national competent authorities of the Member States in which it made the system available and, where applicable, the notified body that issued a certificate for the high-risk AI system, in particular of the non-compliance and of any corrective actions taken.		

PUBLIC

Article 23 *Cooperation with competent authorities*		
Providers of high-risk AI systems shall, upon request by a national competent authority, provide that authority with all the information and documentation necessary to demonstrate the conformity of the high-risk AI system with the requirements set out in Chapter 2 of this Title, in **a language which can be easily underestood by the authority of** ~~an official Union language determined by~~ the Member State concerned. Upon a reasoned request from a national competent authority, providers shall also give that authority access to the logs automatically generated by the high-risk AI system, to the extent such logs are under their control by virtue of a contractual arrangement with the user or otherwise by law.		

PUBLIC

Article 23a ***Conditions for other persons to be subject to the obligations of a provider ~~Obligations of distributors, importers, users or any other third-party~~***		
1. Any natural or legal person ~~distributor, importer, user or other third-party~~ shall be considered a provider of a new high-risk AI system for the purposes of this Regulation and shall be subject to the obligations of the provider under Article 16, in any of the following circumstances:		
(a) they put their name or trademark on a high-risk AI system already placed on the market or put into service, without prejudice to contractual arrangements stipulating that the obligations are allocated otherwise;		
~~(b) they modify the intended purpose of a~~		

PUBLIC

~~**high-risk AI system already placed on the market or put into service;**~~		
(c) they make a substantial modification to a high-risk AI system already placed on the market or put into service;		
(d) they modify the intended purpose of an AI system which is not high-risk and is already placed on the market or put ito service, in a way which makes the modified system a high-risk AI system;~~.~~		
(e) they fulfil the conditions referred in Article 52a(2).		
2. Where the circumstances referred to in paragraph 1, point (a) ~~(b)~~ or (c), occur, the provider that initially placed the high-risk AI system on the market or put it into service shall no longer be considered a		

PUBLIC

provider for the purposes of this Regulation.		
3. For high-risk AI systems that are safety components of products to which the legal acts listed in Annex II, section A apply, the manufacturer of those products shall be considered the provider of the high-risk AI system and shall be subject to the obligations under Article 16 under either of the following scenarios:		
(i) the high-risk AI system is placed on the market together with the product under the name or trademark of the product manufacturer;		
(ii) the high-risk AI system is put into service under the the name or trademark of the product manufacturer after the product has been placed on the market.		

PUBLIC

~~*Article 24*~~ ~~*Obligations of product manufacturers*~~		
~~Where a high-risk AI system related to products to which the legal acts listed in Annex II, section A, apply, is placed on the market or put into service together with the product manufactured in accordance with those legal acts and under the name of the product manufacturer, the manufacturer of the product shall take the responsibility of the compliance of the AI system with this Regulation and, as far as the AI system is concerned, have the same obligations imposed by the present Regulation on the provider.~~		
Article 25 *Authorised representatives*		
1. Prior to making their systems available on		

PUBLIC

the Union market~~, where an importer cannot be identified,~~ providers established outside the Union shall, by written mandate, appoint an authorised representative which is established in the Union.		
2. The authorised representative shall perform the tasks specified in the mandate received from the provider. **For the purpose of this Regulation,** ~~T~~**t**he mandate shall empower the authorised representative to carry out **only** the following tasks:		
(-a) verify that the EU declaration of conformity and the technical documentation have been drawn up and that an appropriate conformity assessment procedure has been carried out by the provider;		
(a) **keep at the disposal of the national**		

PUBLIC

competent authorities and national authorities referred to in Article 63(7), for a period ending 10 years after the high-risk AI system has been placed on the market or put into service, a copy of the EU declaration of conformity , the technical documentation and, if applicable, the certificate issued by the notified body ~~keep a copy of the EU declaration of conformity and the technical documentation at the disposal of the national competent authorities and national authorities referred to in Article 63(7)~~;		
(b) provide a national competent authority, upon a reasoned request, with all the information and documentation**, including that kept according to point (b)**, necessary to demonstrate the conformity of a high-risk AI system with the requirements set out in Chapter 2 of this Title, including access to the logs automatically generated by the high-risk AI		

PUBLIC

system to the extent such logs are under the control of the provider by virtue of a contractual arrangement with the user or otherwise by law;		
(c) cooperate with ~~competent~~ national **competent** authorities, upon a reasoned request, on any action the latter takes in relation to the high-risk AI system.		
(d) comply with the registration obligations referred to in Article 51 or, if the registration is carried out by the provider itself, verify that the information referred to in point 3 of Annex VIII is correct.		
The authorised representative shall terminate the mandate if it has sufficient reasons to consider that the provider acts contrary to its obligations under this Regulation. In such a case, it shall also immediately inform the market surveillance authority of the Member		

PUBLIC

State in which it is established, as well as, where applicable, the relevant notified body, about the termination of the mandate and the reasons thereof.		
The authorised representative shall be legally liable for defective AI systems on the same basis as, and jointly and severally with, the provider in respect of its potential liability under Council Directive 85/374/EEC.		We would consider it helpful to get a little bit more insight into the liability provision at the end of Article 25(2) AIA. We understand that an authorized representative should be jointly and severally liable for damages under this provision, if the provider is itself liable for damages as a producer under the Product Liability Directive (PLD). We wonder whether such a provision is particularly helpful when the AIA is itself silent on all other liability matters because these issues are to be dealt with in the upcoming proposals on revising the PLD and on a new AI Liability Directive. Furthermore it might not be easy to mix a regulation - the AIA - with a directive - the PLD - for the purposes of establishing liability.

PUBLIC

Article 26 *Obligations of importers*		
1. Before placing a high-risk AI system on the market, importers of such system shall ensure **that such a system is in conformity with this Regulation by verifying** that:		
(a) the ~~appropriate~~ **relevant** conformity assessment procedure **referred to in Article 43** has been carried out by the provider of that AI system;		
(b) the provider has drawn up the technical documentation in accordance with Annex IV;		
(c) the system bears the required **CE** conformity marking and is accompanied by **the EU declaration of conformity** and ~~the required documentation and~~ instructions of use~~.~~**;**		

PUBLIC

(d) the authorised representative referred to in Article 25 has been established by the provider.		
2. Where an importer ~~considers or~~ has **sufficient** reason**s** to consider that a high-risk AI system is not in conformity with this Regulation, **or is falsified, or accompanied by falsified documentation,** it shall not place that system on the market until that AI system has been brought into conformity. Where the high-risk AI system presents a risk within the meaning of Article 65(1), the importer shall inform the provider of the AI system and the market surveillance authorities to that effect.		
3. Importers shall indicate their name, registered trade name or registered trade mark, and the address at which they can be contacted on the high-risk AI system or, where that is not		

PUBLIC

possible, on its packaging or its accompanying documentation, as applicable.		
4. Importers shall ensure that, while a high-risk AI system is under their responsibility, where applicable, storage or transport conditions do not jeopardise its compliance with the requirements set out in Chapter 2 of this Title.		
4a. Importers shall keep, for a period ending 10 years after the AI system has been placed on the market or put into service, a copy of the certificate issued by the notified body, where applicable, of the instructions for use and of the EU declaration of conformity.		
5. Importers shall provide national competent authorities, upon a reasoned request, with all necessary information and documentation**, including that kept in**		

PUBLIC

accordance with paragrapah 5, to demonstrate the conformity of a high-risk AI system with the requirements set out in Chapter 2 of this Title in a language which can be easily understood by that national competent authority. **To this purpose they shall also ensure that the technical documentation can be made available to those authorities.** ~~, including access to the logs automatically generated by the high-risk AI system to the extent such logs are under the control of the provider by virtue of a contractual arrangement with the user or otherwise by law. They shall also cooperate with those authorities on any action national competent authority takes in relation to that system.~~		
5a. Importers shall cooperate with national competent authorities on any action those authorities take in relation to an AI system.		Please also clarify whether the duty to cooperate refers only to measures taken under this Regulation or also to measures taken by national competent authorities on the basis of national or

PUBLIC

		Union law in relation to high-risk AI.
Article 27 *Obligations of distributors*		
1. Before making a high-risk AI system available on the market, distributors shall verify that the high-risk AI system bears the required CE conformity marking, that it is accompanied by ~~the required documentation and~~ **EU declaration of conformity and** instruction of use, and that the provider and the importer of the system, as applicable, have complied with the**ir** obligations **set out Article 16, point (b) and 26(3) respectively** ~~in this Regulation~~.		
2. Where a distributor considers or has reason to consider that a high-risk AI system is not in conformity with the requirements set out in Chapter 2 of this Title, it shall not make the high-risk AI system available on the market	the distributor shall inform the market surveillance authorities and the provider or the importer of the system	The market surveillance authority should also be informed (as in Art. 26 para 2).

PUBLIC

until that system has been brought into conformity with those requirements. Furthermore, where the system presents a risk within the meaning of Article 65(1), the distributor shall inform the provider or the importer of the system, as applicable, to that effect.		
3. Distributors shall ensure that, while a high-risk AI system is under their responsibility, where applicable, storage or transport conditions do not jeopardise the compliance of the system with the requirements set out in Chapter 2 of this Title.		
4. A distributor that considers or has reason to consider that a high-risk AI system which it has made available on the market is not in conformity with the requirements set out in Chapter 2 of this Title shall take the corrective actions necessary to bring that system into		

PUBLIC

conformity with those requirements, to withdraw it or recall it or shall ensure that the provider, the importer or any relevant operator, as appropriate, takes those corrective actions. Where the high-risk AI system presents a risk within the meaning of Article 65(1), the distributor shall immediately inform the national competent authorities of the Member States in which it has made the product available to that effect, giving details, in particular, of the non-compliance and of any corrective actions taken.		
5. Upon a reasoned request from a national competent authority, distributors of high-risk AI systems shall provide that authority with all the information and documentation **regarding its activities as described in paragraph 1 to 4** ~~necessary to demonstrate the conformity of a high-risk system with the requirements set out in Chapter 2 of this Title~~. ~~Distributors shall also cooperate with that national competent authority~~		

PUBLIC

~~on any action taken by that authority.~~		
5a. Distributors shall cooperate with national competent authorities on any action those authorities take in relation to an AI system.		Please also clarify whether the duty to cooperate refers only to measures taken under this Regulation or also to measures taken by national competent authorities on the basis of national or Union law in relation to high-risk AI.
~~*Article 28*~~ ~~*Obligations of distributors, importers, users or any other third-party*~~		
~~1. Any distributor, importer, user or other third-party shall be considered a provider~~ ~~**of high-risk AI system**~~ ~~for the purposes of this Regulation and shall be subject to the obligations of the provider under Article 16, in any of the following circumstances:~~		
~~(a) they place on the market or put into service a high-risk AI system under their name~~		

PUBLIC

~~or trademark;~~		
~~(b) they modify the intended purpose of a high-risk AI system already placed on the market or put into service;~~		
~~(c) they make a substantial modification to the high-risk AI system.~~**;**		
~~(d) they modify the intendent purpose of an AI system which is not high-risk and is already placed on the market or put ito service, in a way which makes the modified system a high-risk AI system.~~		
~~2. Where the circumstances referred to in paragraph 1, point (b) or (c), occur, the provider that initially placed the high-risk AI system on the market or put it into service shall no longer be considered a provider for the purposes of this Regulation.~~		

PUBLIC

Article 29 *Obligations of users of high-risk AI systems*		
1. Users of high-risk AI systems shall use such systems **and implement human oversight** in accordance with the instructions of use accompanying the systems, pursuant to paragraphs 2 and 5 **of this Article**.		
1a. Users shall assign human oversight to natural persons who have the necessary competence, training and authority.		
2. The obligations in paragraph 1 **and 1a** are without prejudice to other user obligations under Union or national law and to the user's discretion in organising its own resources and activities for the purpose of implementing the human oversight measures indicated by the provider.		

PUBLIC

3. Without prejudice to paragraph 1, to the extent the user exercises control over the input data, that user shall ensure that input data is relevant in view of the intended purpose of the high-risk AI system.		
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		

PUBLIC

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.		
5. Users of high-risk AI systems shall keep the logs automatically generated by that high-risk AI system, to the extent such logs are under their control ~~and~~. ~~The logs shall be kept~~ **They shall keep them** for a period **of at least six months, unless provided otherwise** ~~that is appropriate in the light of the intended purpose of the high-risk AI system and~~ **in** applicable ~~legal obligations under~~ Union or national law**, in particular in Union law on the protection of personal data**.		

PUBLIC

Users that are credit institutions regulated by Directive 2013/36/EU shall maintain the logs as part of the documentation concerning 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.		
6a. Users shall cooperate with national competent authorities on any action those authorities take in relation to an AI system.		Art. 29 para 6a is quite broad and hence unclear. DEU asks COM to specify. Such obligations of users to cooperate with national competent authorities must be clear and specific. The provision must provide for the

PUBLIC

		possibility to take the principle of proportionality into consideration, especially with cases overlapping data protection regulation and the protection of trade and business secrets or confidentiality agreements. Please also clarify whether the duty to cooperate refers only to measures taken under this Regulation or also to measures taken by national competent authorities on the basis of national or Union law in relation to high-risk AI.
7. The obligations established by this Article shall not apply to users who use the AI system in the course of a personal non-professional activity.		
CHAPTER 4		
NOTIFIYING AUTHORITIES AND		

PUBLIC

NOTIFIED BODIES		
Article 30 *Notifying authorities*		
1. Each Member State shall designate or establish a notifying authority responsible for setting up and carrying out the necessary procedures for the assessment, designation and notification of conformity assessment bodies and for their monitoring.	Each Member State shall designate or establish a notifying authority responsible for setting up and carrying out the necessary procedures for the assessment, designation, notification and for their monitoring, of conformity assessment bodies including their compliance with the provisions of Article 34.	
2. ~~Member States may designate a national accreditation body referred to in Regulation (EC) No 765/2008 as a notifying authority.~~ **Member States may decide that the assessment and monitoring referred to in paragraph 1 shall be carried out by a national accreditation body within the meaning of and in accordance with**		

PUBLIC

Regulation (EC) No 765/2008.		
	(new). The Commission shall provide for the organisation of exchange of experience between national notifying or designating authorities responsible for notification policy.	To improve exchange of experience betweend national notifying or designating authorities responsible for notification policy. Based on R29 Decision 768/2008/EC
3. Notifying authorities shall be established, organised and operated in such a way that no conflict of interest arises with conformity assessment bodies and the objectivity and impartiality of their activities are safeguarded.		
4. Notifying authorities shall be organised in such a way that decisions relating to the notification of conformity assessment bodies are taken by competent persons different from those who carried out the assessment of those bodies.		
5. Notifying authorities shall not offer or provide any activities that conformity assessment bodies perform or any consultancy services on a commercial or competitive basis.		

PUBLIC

6. Notifying authorities shall safeguard the confidentiality of the information they obtain **in accordance with Article 70**.		There are different interpretations, if this provision is also applicable to the cross-border exchange of information between notifying or competent authorities and the COM. Therefor we suggest to add the following sentence: "However, notifying authorities shall exchange information on conformity assessment bodies, the Commission and, when required, with other regulatory authorities of other Member States."
7. Notifying authorities shall have ~~a sufficient~~ **an adequate** number of competent personnel at their disposal for the proper performance of their tasks.		
8. ~~Notifying authorities shall make sure that~~		

PUBLIC

~~conformity assessments are carried out in a proportionate manner, avoiding unnecessary burdens for providers and that notified bodies perform their activities taking due account of the size of an undertaking, the sector in which it operates, its structure and the degree of complexity of the AI system in question.~~		
Article 31 *Application of a conformity assessment body for notification*		
1. Conformity assessment bodies shall submit an application for notification to the notifying authority of the Member State in which they are established.		
2. The application for notification shall be accompanied by a description of the conformity assessment activities, the conformity assessment module or modules and the artificial intelligence	The application for notification shall be accompanied by a description ~~**of**~~ the conformity assessment activities~~,~~ and the conformity assessment module or modules ~~and the artificial~~	No distinction should be made on artificial

PUBLIC

technologies for which the conformity assessment body claims to be competent, as well as by an accreditation certificate, where one exists, issued by a national accreditation body attesting that the conformity assessment body fulfils the requirements laid down in Article 33. Any valid document related to existing designations of the applicant notified body under any other Union harmonisation legislation shall be added.	~~intelligence technologies~~ for which the conformity assessment body claims to be competent, as well as by an accreditation certificate, where one exists, issued by a national accreditation body attesting that the conformity assessment body fulfils the requirements laid down in Article 33. Any valid document related to existing designations of the applicant notified body under any other Union harmonisation legislation shall be added.	intelligence (unclear criteria).
3. Where the conformity assessment body concerned cannot provide an accreditation certificate, it shall provide the notifying authority with the documentary evidence necessary for the verification, recognition and regular monitoring of its compliance with the requirements laid down in Article 33. For notified bodies which are designated under any other Union harmonisation legislation, all documents and certificates linked to those	Where the conformity assessment body concerned cannot provide an accreditation certificate, it shall provide the notifying authority with all the documentary evidence necessary for the verification, recognition and regular monitoring of its compliance with the requirements laid down in Article 33. For notified bodies which are designated under any other Union harmonisation legislation, all documents and certificates linked to those	The exact wording of R22(3) Decision 768/2008/EC should be used.

PUBLIC

designations may be used to support their designation procedure under this Regulation, as appropriate.	designations may be used to support their designation procedure under this Regulation, as appropriate.	
		How to deal with changes to the notification? It should be further examined – also within the upcoming Council Working Parties - whether to add a new paragraph based on Article 38(3) Regulation 2017/745: "The notified body shall update the documentation referred to in paragraph 2 and paragraph 3 whenever relevant changes occur, in order to enable the authority responsible for notified bodies to monitor and verify continuous compliance with all the requirements laid down in Article 33."
Article 32 *Notification procedure*		
1. Notifying authorities may **only** notify ~~only~~ conformity assessment bodies which have		

PUBLIC

satisfied the requirements laid down in Article 33.		
2. Notifying authorities shall notify **those bodies to** the Commission and the other Member States using the electronic notification tool developed and managed by the Commission.	Notifying authorities shall notify ~~those bodies to~~ the Commission and the other Member States using the electronic notification tool within the database of notified bodies developed and managed by the Commission (NANDO).	For clarification, it is propose to modify the reference provision of R23 Decision 768/2008/EC and to add a reference to the database of notified bodies (NANDO).
3. The notification **referrred to in paragraph 2** shall include full details of the conformity assessment activities, the conformity assessment module or modules ~~and the artificial intelligence technologies concerned~~ **and the relevant attestation of competence. Where a notification is not based on an accreditation certificate as referred to in Article 31 (2), the notifying authority shall provide the Commission and the other Member States with documentary evidence which attests to the conformity assessment body's competence**	The notification shall include full details of the conformity assessment activities~~,~~ and the conformity assessment module or modules ~~and the artificial intelligence technologies concerned.~~ which the notified body is authorised to assess and any conditions associated with the notification.	For clarification, it is propose to modify the reference provision of R23 Decision 768/2008/EC. It is noted that notified bodies responsible for measuring instruments should not assess AI systems for educational or vocational training. Therefore, it seems useful to differentiate between different product sectors.

PUBLIC

and the arrangements in place to ensure that that body will be monitored regularly and will continue to satisfy the requirements laid down in Article 33.		
4. The conformity assessment body concerned may perform the activities of a notified body only ~~where~~ **where no objections are raised by the Commission or the other Member States within two weeks of a notification by a notifying authority where it includes an accreditation certificate referred to in Article 31(2), or within two months of a notification by the notifying authority where it includes documentary evidence referred to in Article 31(3)** ~~no objections are raised by the Commission or the other Member States within one month of a notification~~.		
5. Notifying authorities shall notify the Commission and the other Member States of		We would welcome a clear definition of 'relevant changes'.

PUBLIC

any subsequent relevant changes to the notification **referred to in this Article without undue delay**.		
	(new) The Commission shall immediately publish the amended notification in NANDO.	For clarification, it is propose to modify the reference provision of R23 Decision 768/2008/EC and to add this new paragraph.
Article 33 ***Requirements relating to n~~N~~otified bodies***		
1. ~~Notified bodies shall verify the conformity of high-risk AI system in accordance with the conformity assessment procedures referred to in Article 43.~~ **A notified body shall be established under national law and have legal personality.**		
2. Notified bodies shall satisfy the organisational, quality management, resources and process requirements that are necessary to fulfil their tasks.		Maybe specify the requirements by adding a new annex.

PUBLIC

3. The organisational structure, allocation of responsibilities, reporting lines and operation of notified bodies shall be such as to ensure that there is confidence in the performance by and in the results of the conformity assessment activities that the notified bodies conduct.		
4. Notified bodies shall be independent of the provider of a high-risk AI system in relation to which it performs conformity assessment activities. Notified bodies shall also be independent of any other operator having an economic interest in the high-risk AI system that is assessed, as well as of any competitors of the provider.		
5. Notified bodies shall be organised and operated so as to safeguard the independence, objectivity and impartiality of their activities. Notified bodies shall document and implement a structure and procedures to safeguard		

PUBLIC

impartiality and to promote and apply the principles of impartiality throughout their organisation, personnel and assessment activities.		
6. Notified bodies shall have documented procedures in place ensuring that their personnel, committees, subsidiaries, subcontractors and any associated body or personnel of external bodies respect the confidentiality of the information which comes into their possession during the performance of conformity assessment activities, except when disclosure is required by law. The staff of notified bodies shall be bound to observe professional secrecy with regard to all information obtained in carrying out their tasks under this Regulation, except in relation to the notifying authorities of the Member State in which their activities are carried out.		

PUBLIC

7. Notified bodies shall have procedures for the performance of activities which take due account of the size of an undertaking, the sector in which it operates, its structure, the degree of complexity of the AI system in question.		
8. Notified bodies shall take out appropriate liability insurance for their conformity assessment activities, unless liability is assumed by the Member State **in which they are located** ~~concerned~~ in accordance with national law or that Member State is **itself** directly responsible for the conformity assessment.		
9. Notified bodies shall be capable of carrying out all the tasks falling to them under this Regulation with the highest degree of professional integrity and the requisite competence in the specific field, whether those tasks are carried out by notified bodies themselves or on their behalf and under their		

PUBLIC

responsibility.		
10. Notified bodies shall have sufficient internal competences to be able to effectively evaluate the tasks conducted by external parties on their behalf. ~~To that end, at all times and for each conformity assessment procedure and each type of high-risk AI system in relation to which they have been designated, t~~**T**he notified body shall have permanent availability of sufficient administrative, technical**, legal** and scientific personnel who possess experience and knowledge relating to the relevant artificial intelligence technologies, data and data computing and to the requirements set out in Chapter 2 of this Title.		
11. Notified bodies shall participate in coordination activities as referred to in Article 38. They shall also take part directly or be represented in European standardisation		

PUBLIC

organisations, or ensure that they are aware and up to date in respect of relevant standards.		
~~12. Notified bodies shall make available and submit upon request all relevant documentation, including the providers' documentation, to the notifying authority referred to in Article 30 to allow it to conduct its assessment, designation, notification, monitoring and surveillance activities and to facilitate the assessment outlined in this Chapter.~~		
Article 33a ***Presumption of conformity with requirements relating to notified bodies***		
Where a conformity assessment body demonstrates its conformity with the criteria laid down in the relevant harmonised standards or parts thereof the references of which have been published in the Official		

PUBLIC

Journal of the European Union it shall be presumed to comply with the requirements set out in Article 33 in so far as the applicable harmonised standards cover those requirements.		
Article 34 *Subsidiaries of and subcontracting by notified bodies*		
1. Where a notified body subcontracts specific tasks connected with the conformity assessment or has recourse to a subsidiary, it shall ensure that the subcontractor or the subsidiary meets the requirements laid down in Article 33 and shall inform the notifying authority accordingly.		
2. Notified bodies shall take full responsibility for the tasks performed by subcontractors or subsidiaries wherever these		

PUBLIC

are established.		
3. Activities may be subcontracted or carried out by a subsidiary only with the agreement of the provider.		
4. ~~Notified bodies shall keep at the disposal of the notifying authority t~~**T**he relevant documents concerning the assessment of the qualifications of the subcontractor or the subsidiary and the work carried out by them under this Regulation **shall be kept at the disposal of the notifying authority for a period of 5 years from the termination date of the subcontracting activity**.		
Article 34a		
Operational obligations of notified bodies		
1. Notified bodies shall verify the		

PUBLIC

conformity of high-risk AI system in accordance with the conformity assessment procedures referred to in Article 43.		
2. Notified bodies shall perform their activities while avoiding unnecessary burdens for providers, and taking due account of the size of an undertaking, the sector in which it operates, its structure and the degree of complexity of the high risk AI system in question. In so doing, the notified body shall nevertheless respect the degree of rigour and the level of protection required for the compliance of the high risk AI system with the requirements of this Regulation.		
3. Notified bodies shall make available and submit upon request all relevant documentation, including the providers' documentation, to the notifying authority referred to in Article 30 to allow that		

PUBLIC

authority to conduct its assessment, designation, notification, monitoring activities and to facilitate the assessment outlined in this Chapter.		
Article 35 *Identification numbers and lists of notified bodies designated under this Regulation*		
1. The Commission shall assign an identification number to notified bodies. It shall assign a single number, even where a body is notified under several Union acts.		Does a notified body receive a new identification number that has already been notified under a legal act listed in Annex II, section A?
2. The Commission shall make publicly available the list of the bodies notified under this Regulation, including the identification numbers that have been assigned to them and the activities for which they have been notified. The Commission shall ensure that the list is kept up to date.	The Commission shall make ~~publicly available~~ the list of the bodies notified under this Regulation, including the identification numbers that have been assigned to them and the activities for which they have been notified accessible to the public in NANDO. The Commission shall ensure that the list is kept up	The German Federal Government is concerned that the publication of the list of notified bodies in the area of law enforcement, as provided for in Article 35(2) of the AI Regulation, could encourage illegal influence on or research of such bodies, for example by foreign services. Do the Commission or other Member States

PUBLIC

	to date.	share this view? Should an exemption clause be included to enable the Member State concerned, under conditions to be defined in more detail, to refrain from publication in individual cases if and to the extent that interests in the protection of secrets conflict with this? DEU security authorities are in favour of this.
Article 36 *Changes to notifications*		
1. Where a notifying authority has ~~suspicions~~ **sufficient reasons to consider** ~~or has been informed~~ that a notified body no longer meets the requirements laid down in Article 33, or that it is failing to fulfil its obligations, **the notifying authority shall restrict, suspend or withdraw notification as appropriate, depending on the seriousness of the failure to meet those requirements or fulfil those obligations. It shall immediately inform the Commission**		In several sectors the issues of notified bodies ceasing their activities or where a notification has been withdrawn require special provisions to prevent a scenario in which AI systems would lose the marketability during the phase where the provider has to apply for a new qualified notified body. To address this issue this paragraph has been modified from reference provision of R25

PUBLIC

and the other Member States accordingly ~~that authority shall without delay investigate the matter with the utmost diligence. In that context, it shall inform the notified body concerned about the objections raised and give it the possibility to make its views known. If the notifying authority comes to the conclusion that the notified body investigation no longer meets the requirements laid down in Article 33 or that it is failing to fulfil its obligations, it shall restrict, suspend or withdraw the notification as appropriate, depending on the seriousness of the failure. It shall also immediately inform the Commission and the other Member States accordingly.~~		Decision 768/2008/EC and further modifications are needed. There are several procedures missing in the event of insufficient implementation of corrective measures or information of providers in the event of notification changes. It is suggested to consider to add relevant paragraphs from Regulation 2017/745 to clarify these procedures.
2. In the event of restriction, suspension or withdrawal of notification, or where the notified body has ceased its activity, the notifying authority shall take appropriate steps to ensure that the files of that notified body are either		There is no provision/procedure in the event of notified bodies ceasing the conformity assessment activities and in the event of restriction, suspension or withdrawal of a notification as well as exception of certificates

PUBLIC

taken over by another notified body or kept available for the responsible notifying authorities **and market surveillance authorities** at their request.		unduly issued, and where a notification has been suspended or restricted. It is propose to add paragraphs based on Regulation 2017/745 to clarify these procedures.
Article 37 *Challenge to the competence of notified bodies*		
1. The Commission shall, where necessary, investigate all cases where there are reasons to doubt whether a notified body complies with the requirements laid down in Article 33.		
2. The notifying authority shall provide the Commission, on request, with all relevant information relating to the notification of the notified body concerned.		This paragraph has been modified from reference provision of R26 Decision 768/2008/EC and there is a further modification needed that the notifying authority shall monitor the notified bodies.
3. The Commission shall ensure that all confidential information obtained in the course		

PUBLIC

of its investigations pursuant to this Article is treated confidentially.		
4. Where the Commission ascertains that a notified body does not meet or no longer meets the requirements laid down in Article 33, it shall **inform the notifying authority of the reasons of such an ascertainment and request it** ~~adopt a reasoned decision requesting the notifying Member State~~ to take the necessary corrective measures, including ~~withdrawal of~~ **de-**notification if necessary. ~~That implementing act shall be adopted in accordance with the examination procedure referred to in Article 74(2).~~ **Where the notifying authority fails to take the necessary corrective measures, the Commission may, by means of implementing acts, suspend, restrict or withdraw the notification. That implementing act shall be adopted in accordance with the examination procedure referred to in Article 74(2).**	Where the Commission ascertains that a notified body does not meet or no longer meets the requirements laid down in Article 33, it shall ~~adopt a reasoned decision requesting~~ inform the notifying ~~Member State~~ authority to take the necessary corrective measures, including withdrawal of notification if necessary	.

PUBLIC

Article 38 *Coordination of notified bodies*		
1. The Commission shall ensure that, with regard to ~~the areas covered by this Regulation~~ **high-risk AI systems**, appropriate coordination and cooperation between notified bodies active in the conformity assessment procedures ~~of AI systems~~ pursuant to this Regulation are put in place and properly operated in the form of a sectoral group of notified bodies**.**	The Commission shall ensure that, with regard to the ~~areas covered by this Regulation~~ high-risk AI systems covered by Annex III, appropriate coordination and cooperation between notified bodies active in the conformity assessment procedures of AI systems pursuant to this Regulation are put in place and properly operated in the form of a sectoral group of notified bodies**.**	Exception for Annex II products is needed.
2. ~~Member States~~ **The notifying authority** shall ensure that the bodies notified by them participate in the work of that group, directly or by means of designated representatives.		
	(new) The Commission may establish the specific arrangements for the functioning of the coordination group of notified bodies.	To increase functioning of coordination group of notified bodies, it is propose to modify the reference provision of R30 Decision

PUBLIC

		768/2008/EC and to add this new paragraph.
Article 39 *Conformity assessment bodies of third countries*		
Conformity assessment bodies established under the law of a third country with which the Union has concluded an agreement may be authorised to carry out the activities of notified Bodies under this Regulation**, provided that they meet the requirements in Article 33**.	~~an~~ a respective agreement	To increase precision. We do, however, would like to point out that this provision might lead to enforcement gaps as the enforcement depends highly on the content of the respective agreements.
CHAPTER 5		
STANDARDS, CONFORMITY ASSESSMENT, CERTIFICATES, REGISTRATION		
Article 40 *Harmonised standards*		In the area of law enforcement, there are specific requirements for IT security,

PUBLIC

		confidentiality, protection of fundamental rights and data protection as well as specific technical requirements. In DEU, it is being discussed whether it can be ensured that such specific requirements of the security sector can be taken into account within the framework of the standards according to Article 40 and the specifications according to Article 41 of the Draft Regulation. How do the COM and the other Member States see this?
1. High-risk AI systems **or general purpose 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 **or, as applicable, with requirements set out in Article 4a and Article 4b**, to the extent those standards cover those requirements.	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~~ in this Regulation, to the extent those standards cover those requirements.	Taking into account other requirements, e. g. quality management system, post-market-surveilliance system, etc.. The initial draft shall become paragraph 1 and a second paragraph addressing conformity requirements specific to high-risk AI systems

PUBLIC

	This proposal will be reconsidered in light of any alterations of the exemption clause contained in Article 2(3) of the draft	developed or used for purposes of the defence sector or the armed forces. In as much as such AI systems are not exempt from the application of the Regulation by virtue of Article 2(3) of the draft they will nevertheless be developed or used in accordance with relevant military standards. Compliance with these military standards, some of which may be classified or otherwise outside the public domain, shall be deemed equivalent to compliance with standards the references of which have been published in the Official Journal of the European Union.
	(2) High-risk AI systems developed or used for purposes of the defence sector or the armed forces , which are in conformity with relevant military standards, including military standards adopted in the framework of the North Atlantic Treaty Organization, shall be presumed to be in	Furthermore, we propose to shift this paragraph to Art. 42 (Presumption of conformity with certain requirements), because this paragraph is only about the presumption of conformity. The proposal for the Machinery Regulation contains the same structure, which is proposed.

PUBLIC

	conformity with the requirements set out in Chapter 2 of this Title for the purposes of this Regulation.	
2. When issuing a standardisation request to European standardisation organisations in accordance with Article 10 of Regulation 1025/2012, the Commission shall specify that standards are coherent, easy to implement and drafted in such a way that they aim to fulfil in particular the following objectives:		We kindly ask the presidency to verify whether the conditions listed in paragraph 2 should be listed in Article 40, which in principle focuses on the presumption of conformity. Several of the objectives are stated as such in Regulation 1025/2012 (e.g. SME/stakeholder involvment), others are explicitely AI systems-related objectives and could be part of the requirements specified in other places of this Regulation as they are not particularly standardisation specific (see also question below w/r to objective (a)). Sorting out the exact background of the objectives listed in Para. 2 would in our mind help putting in place clear and especially NLF-based requirements for standards and AI-systems alike.

PUBLIC

a) ensure that AI systems placed on the market or put into service in the Union are safe and respect Union values and strenghten the Union's digital sovereignty;	**a) ensure that AI systems placed on the market or put into service in the Union are safe and secure and respect Union values and strenghten the Union's digital sovereignty;**	"Secure" should be added as cyber security and operational resilience should also be an aim for AI systems. We kindly ask for an explanation of how standards can assure that AI systems contribute to the Union's digital sovereignty. In our understanding, standards should be harmonized globally and not different according to regions. We therefore support COM's initiative to strengthen European actors in the international standardisation system to safeguard European fundamental values and human rights in the international system.
b) promote investment and innovation in AI, as well as competitiveness and growth of the Union market;		

PUBLIC

c) enhance multistakeholder governance, representative of all relevant European stakeholders (e.g. industry, SMEs, civil society, researchers).		
d) contribute to strengthening global cooperation on standardisation in the field of AI that is consistent with Union values and interests.		
The Commission shall request the European standardisation organisations to provide evidence of their best efforts to fulfil the above objectives.		
Article 41 *Common specifications*		Commission Nonpaper WK 10046/2022 with respect to common specifications published 8 July 2022 adresses the issue of §40 and following from a horizontal perspective and proposes provisions that can be used in current and future legislative acts. We kindly ask the

PUBLIC

		PCY to take the provisions from the Appendix of this Nonpaper which reproduces the compromise from Machinery Regulation. This would save this Group from long discussions to reach the very same compromises as Common specifications are explicitely not case specific but a horizontal issue without sector specific components. Provisions thus should be the same in all regulation. Inter alia the text contains provisions with respect to the following aspects: - Specificy in which concrete situation common specifications might be developed – i.e. inter alia when an european standardization body rejected the mandate for a harmonized standard. It is not sufficient that there simply is no standard. - No use of undefined words such as "unsufficient" – the text from Machinery refers

PUBLIC

		to a comparison to the mandate of the standard in question. - COM informs the Committee established according to Art. 22 of Regulation 1025/2022 about the fulfilment of the conditions to develop common specifications - As soon as one or several harmonized standards are listed in the OJ that address the same technical issue as common specifications implemented by COM, the common specifications should be repealed with a reasonable time for adaption of market actors. Additionally, we kindly ask to foresee a possibility for the sector specific committee to confirm that the conditions under which COM may proceed to develop common specifications are fulfilled. As COM highlights in its implementation report regarding Regulation 1025/2012 there are several reasons why

PUBLIC

		european standardisation bodies reject a mandate. All these reason are quite good reasons in our view and there should be not automatic cause for common specifications based on a rejection but an evaluation of the situation by the Committee in charge of the AI regulation.
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, **after consulting the AI Board referred to in Article 56**, by means of implementing acts, adopt common specifications in respect of the requirements set out in Chapter 2 of this Title **or, as applicable, with requirements set out in Article 4a and Article 4b**. Those implementing acts shall be adopted in accordance with the examination	1. Where harmonised standards referred to in Article 40 paragraph 1 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, 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.	As explained in the Working Paper referred to above, common specifications are a fallback option if and only if there are no harmonized standards available. They are thus not meant to address specific safety or other concerns if there is no clear link to missing standardization.

PUBLIC

procedure referred to in Article 74(2).		
2. ~~The Commission,~~ **W**~~w~~hen preparing the common specifications referred to in paragraph 1, **the Commission** shall **fulfil the objectives referred of Article 40(2) and** gather the views of relevant bodies or expert groups established under relevant sectorial Union law.		
3. High-risk AI systems **or general purpose AI systems** which are in conformity with the		

PUBLIC

common specifications referred to in paragraph 1 shall be presumed to be in conformity with the requirements set out in Chapter 2 of this Title **or, as applicable, with requirements set out in Article 4a and Article 4b**, to the extent those common specifications cover those requirements.		
4. Where providers do not comply with the common specifications referred to in paragraph 1, they shall duly justify **in the technical documentation referred to in Article 11** that they have adopted technical solutions that are at least equivalent thereto.	Where providers of high-risk AI systems or general purpose AI systems do not comply	"of high-risk AI systems or general purpose AI systems" should be added for clarification.
Article 42 *Presumption of conformity with certain requirements*		
1. ~~Taking into account their intended purpose,~~ ~~h~~**H**igh-risk AI systems that have been		It is not clear how this presumption eases any

PUBLIC

trained and tested on data ~~concerning~~ **reflecting** the specific geographical, behavioural ~~and~~ **or** functional setting within which they are intended to be used shall be presumed to be in compliance with the **respective** requirement**s** set out in Article 10(4).		burden compared to Art. 10 (4). Does this par. mean that high-risk AI Systems that have been trained or tested on data provided or approved for law enforcement purposes shall be presumed to be in compliance with the requirements set out in Article 10 (4)?
	1a. High-risk AI systems that have been trained or tested on data provided or approved for purposes of the defence sector or the armed forces shall be presumed to be in compliance with the requirement set out in Article 10(4).	Inasmuch as high-risk AI systems developed or used for purposes of the defence sector or the armed forces are not exempt from the application of the Regulation by virtue of Article 2(3) of the draft they should be presumed to be in compliance with the requirement set out in Article 10(4) if they are trained on data provided or approved for these purposes.
2. High-risk AI systems **or general purpose AI systems** that have been certified or for which a statement of conformity has been issued under		It must be ensured that AI specific cybersecurity scheme is available before AI Act enters into force. Otherwise, there is too much room for

PUBLIC

a cybersecurity scheme pursuant to Regulation (EU) 2019/881 of the European Parliament and of the Council[34] and the references of which have been published in the Official Journal of the European Union shall be presumed to be in compliance with the cybersecurity requirements set out in Article 15 of this Regulation in so far as the cybersecurity certificate or statement of conformity or parts thereof cover those requirements.		interpretation of how to test security relevant aspects of AI systems.
	3. For high-risk AI systems where the provider is a credit institutions regulated by Directive 2013/36/EU or an entity regulated by Directive 2009/138/EC, Directive (EU) 2016/2341, Directive 2014/65/EU resp. Directive (EU) 2015/2366, Directive 2009/65/EG and Directive 2011/61/EU, conformity is assumed when these entities fulfill the requirements following	As the entities regulated by Directive 2013/36/EU, Directive 2009/138/EC, Directive (EU) 2016/2341, Directive 2014/65/EU, Directive (EU) 2015/2366, Directive 2009/65/EG resp. Directive 2011/61/EU already follow highest standards and double regulation has to be avoided, conformity of high-risk AI systems provided by them should be assumed

[34] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ L 151, 7.6.2019, p. 1).

PUBLIC

	Directive 2013/36/EU, Directive 2009/138/EC, Directive (EU) 2016/2341, Directive 2014/65/EU, Directive (EU) 2015/2366, Directive 2009/65/EG resp. Directive 2011/61/EU to the extent those Directives cover the requirements set out in this Regulation.	when they fulfill the respective requirements to the extent that those requirements cover the requirements set out in this Directive.
Article 43 *Conformity assessment*		
		How may it be assured that LEAs using AI application in ongoing investigations may get the conformity assessment in time? Art. 47 does not fulfil this need as it conflicts with secrecy obligations and implies legal uncertainty.
1. For high-risk AI systems listed in point 1 of Annex III, where, in demonstrating the compliance of a high-risk AI system with the requirements set out in Chapter 2 of this Title, the provider has applied harmonised standards referred to in Article 40, or, where applicable, common specifications referred to in Article 41, the provider shall ~~follow~~ **opt for** one of the	For high-risk AI systems listed in point 1 of Annex III, where, in demonstrating the compliance of a high-risk AI system with the requirements set out in Chapter 2 of ~~this Title~~this Regulation, the provider has applied harmonised standards referred to in Article 40, or, where applicable, common specifications referred to in Article 41, the provider opt for one	Taking into account other requirements, e. g. quality management system, post-market-surveilliance system, etc..

PUBLIC

following procedures:	of the following procedures: For high-risk AI systems listed in point 1 of Annex III, where, in demonstrating the compliance of a high-risk AI system with the requirements set out in Chapter 2 of this Title, the provider has applied harmonised standards referred to in Article 40 paragraph (1), or	This addition reflects the addition of Article 40(2).
(a) the conformity assessment procedure based on internal control referred to in Annex VI; **or**		
(b) the conformity assessment procedure based on assessment of the quality management system and assessment of the technical documentation, with the involvement of a notified body, referred to in Annex VII.		

PUBLIC

Where, in demonstrating the compliance of a high-risk AI system with the requirements set out in Chapter 2 of this Title, the provider has not applied or has applied only in part harmonised standards referred to in Article 40, or where such harmonised standards do not exist and common specifications referred to in Article 41 are not available, the provider shall follow the conformity assessment procedure set out in Annex VII.	Where, in demonstrating the compliance of a high-risk AI system listed in point 1 of Annex III with the requirements set out in ~~Chapter 2 of this Title~~this Regulation, the provider has not applied or has applied only in part harmonised standards referred to in Article 40, or where such harmonised standards do not exist and common specifications referred to in Article 41 are not available, the provider shall follow the conformity assessment procedure set out in Annex VII.	Clarification and taking into account other requirements, e. g. quality management system, post-market-surveilliance system, etc..
For the purpose of the conformity assessment procedure referred to in Annex VII, the provider may choose any of the notified bodies. However, when the system is intended to be put into service by law enforcement, immigration or asylum authorities as well as EU institutions, bodies or agencies, the market surveillance authority referred to in Article 63(5) or (6), as applicable, shall act as a notified body.		It might be helpful to clarify whether providers may choose any notified body across the EU.

PUBLIC

2. For high-risk AI systems referred to in points 2 to 8 of Annex III, providers shall follow the conformity assessment procedure based on internal control as referred to in Annex VI, which does not provide for the involvement of a notified body. For high-risk AI systems referred to in point 5(b) of Annex III, placed on the market or put into service by credit institutions regulated by Directive 2013/36/EU, the conformity assessment shall be carried out as part of the procedure referred to in Articles 97 to101 of that Directive.	~~For high-risk AI systems referred to in point 5(b) of Annex III, placed on the market or put into service by credit institutions regulated by Directive 2013/36/EU, the conformity assessment shall be carried out as part of the procedure referred to in Articles 97~~ to101 ~~to 101 of that Directive.~~	It is not feasible to carry out the internal product-oriented conformity assessment as part of the procedure referred to in Art. 97 to 101 in the Directive 2013/36/EU. The ICT-related part of SREP is based on a questionnaire that institutions fill out in self-disclosure. The main focus of the questions is process related and does not target technical aspects such as development details concerning AI- or any other ICT- Systems. Moreover, it is not clear why the conformity assessesment of credit institutions would seemingly include the involvement of a supervisory authority, whereas for all other AI systems in point 2 to 8 of Annex III, an assessment based on internal control is sufficient.
3. For high-risk AI systems, to which legal	For high-risk AI systems, to which legal acts	Taking into account other requirements, e. g.

PUBLIC

acts listed in Annex II, section A, apply, the provider shall follow the relevant conformity assessment as required under those legal acts. The requirements set out in Chapter 2 of this Title shall apply to those high-risk AI systems and shall be part of that assessment. Points 4.3., 4.4., 4.5. and the fifth paragraph of point 4.6 of Annex VII shall also apply.	listed in Annex II, section A, apply, the provider shall follow the relevant conformity assessment as required under those legal acts. The requirements set out in ~~Chapter 2 of this Title~~ this Regulation shall apply to those high-risk AI systems and shall be part of that assessment. Points 4.3., 4.4., 4.5. and the fifth paragraph of point 4.6 of Annex VII shall also apply.	quality management system, post-market-surveilliance system, etc.
For the purpose of that assessment, notified bodies which have been notified under those legal acts shall be entitled to control the conformity of the high-risk AI systems with the requirements set out in Chapter 2 of this Title, provided that the compliance of those notified bodies with requirements laid down in Article 33(4), (9) and (10) has been assessed in the context of the notification procedure under those legal acts.	For the purpose of that assessment, notified bodies which have been notified under those legal acts shall be entitled to control the conformity of the high-risk AI systems with the requirements set out in Chapter 2 of this Title, provided that the compliance of those notified bodies with requirements laid down in Article 33(4), (9) and (10) has been demonstrated to their authority responsible for notified bodies ~~in the context of the notification procedure under those legal acts~~.	Notified bodies referred to in Annex II Section A should be entitled to control the conformity when the demonstrate to the authority responsible for notified bodies that they have fullfilled the requirements for this task. A full re-assessment procedure should be avoided. For medical devices, a full reassessment takes 18 months.

PUBLIC

Where the legal acts listed in Annex II, section A, enable the manufacturer of the product to opt out from a third-party conformity assessment, provided that that manufacturer has applied all harmonised standards covering all the relevant requirements, that manufacturer may make use of that option only if he has also applied harmonised standards or, where applicable, common specifications referred to in Article 41, covering the requirements set out in Chapter 2 of this Title.	Where the legal acts listed in Annex II, section A, enable the manufacturer of the product to opt out from a third-party conformity assessment, provided that that manufacturer has applied all harmonised standards covering all the relevant requirements, that manufacturer may make use of that option only if he has also applied harmonised standards or, where applicable, common specifications referred to in Article 41, covering the requirements set out in ~~Chapter 2 of this Title~~ this Regulation.	Taking into account other requirements, e. g. quality management system, post-market-surveilliance system, etc..
	Those notified bodies have to demonstrate to the authority responsible for notified bodies under legal acts listed in Annex II that they have the resource and process requirements required for this task according to this regulation.	Where a notified body has to be involved in the conforimty assessment, the notified body shall be entitled to control the conformity when the demonstrate to the authority responsible for notified bodies that they have the resource and process required for this task.
4. ~~High-risk AI systems shall undergo a new conformity assessment procedure whenever they are substantially modified, regardless of whether the modified system is intended to be further~~		How is the procedure of a new conformity assessment procedure in case of a substantial modification going to be regulated?

PUBLIC

~~distributed or continues to be used by the current user.~~		Are there special provisions envisaged for LEAs using commercial AI systems as they may – dues to classified information - not give the information to a private provider for ongoing conformity assessment? We reserve the right to make further comments. We would also like to question if cases in which the intended purpose of an AI system is changed by training also constitutes a substantial modification.
~~For high-risk AI systems that continue to learn after being placed on the market or put into service, changes to the high-risk AI system and its performance that have been pre-determined~~		

PUBLIC

~~by the provider at the moment of the initial conformity assessment and are part of the information contained in the technical documentation referred to in point 2(f) of Annex IV, shall not constitute a substantial modification.~~		
5. The Commission is empowered to adopt delegated acts in accordance with Article 73 for the purpose of updating Annexes VI and Annex VII ~~in order to introduce elements of the conformity assessment procedures that become necessary~~ in light of technical progress.		
6. The Commission is empowered to adopt delegated acts to amend paragraphs 1 and 2 in order to subject high-risk AI systems referred to in points 2 to 8 of Annex III to the conformity assessment procedure referred to in Annex VII or parts thereof. The Commission shall adopt such delegated acts taking into account the		

PUBLIC

effectiveness of the conformity assessment procedure based on internal control referred to in Annex VI in preventing or minimizing the risks to health and safety and protection of fundamental rights posed by such systems as well as the availability of adequate capacities and resources among notified bodies.		
Article 44 *Certificates*	*Article 44* *Certificates of conformity*	Clarification
1. Certificates issued by notified bodies in accordance with Annex VII shall be drawn-up in a~~n official Union~~ language determined by the Member State in which the notified body is established ~~or in an official Union language~~		Does is mean that only one language would be acceptable for the certificates?

PUBLIC

~~otherwise acceptable to the notified body~~.		
2. Certificates shall be valid for the period they indicate, which shall not exceed five years. On application by the provider, the validity of a certificate may be extended for further periods, each not exceeding five years, based on a re-assessment in accordance with the applicable conformity assessment procedures.		In event of certain changes to the product portfolio or to the existing quality management system, the Notified Body usually issues supplements to the existing certificates. These supplements are generally only valid together with the underlying certificate and therefore cannot be valid longer than the certificate they supplement. It should be further examined – also within the upcoming Council Working Parties - whether to add the following sentence "Any supplement to a certificate shall remain valid as long as the certificate which it supplements is valid."
3. Where a notified body finds that an AI system no longer meets the requirements set out in Chapter 2 of this Title, it shall, taking account of the principle of proportionality, suspend or	Where a notified body finds that an AI system no longer meets the requirements set out in ~~Chapter 2 of this Title~~ this Regulation, it shall, taking account of the principle of	Taking into account other requirements, e. g. quality management system, post-market-surveilliance system, etc..

PUBLIC

withdraw the certificate issued or impose any restrictions on it, unless compliance with those requirements is ensured by appropriate corrective action taken by the provider of the system within an appropriate deadline set by the notified body. The notified body shall give reasons for its decision.	proportionality, suspend or withdraw the certificate issued or impose any restrictions on it, unless compliance with those requirements is ensured by appropriate corrective action taken by the provider of the system within an appropriate deadline set by the notified body. The notified body shall give reasons for its decision.	
Article 45 *Appeal against decisions of notified bodies*	*Article 45* *Appeal against decisions of notified bodies*	
Member States shall ensure that an appeal procedure against decisions of the notified bodies is available to parties ~~having a legitimate interest in that decision~~.	~~Member States~~ Notified bodies shall ensure that ~~an~~ a transparent and accessible appeal procedure against their decisions ~~of the notified bodies~~ is available ~~to parties~~.	Based on Art. 4 (7) Decision 768/2008/EC. Wording used in Art. 33 Regulation (EU) 2016/425.
Article 46 *Information obligations of notified bodies*		
1. Notified bodies shall inform the notifying		

PUBLIC

authority of the following:		
(a) any Union technical documentation assessment certificates, any supplements to those certificates, quality management system approvals issued in accordance with the requirements of Annex VII;		
(b) any refusal, restriction, suspension or withdrawal of a Union technical documentation assessment certificate or a quality management system approval issued in accordance with the requirements of Annex VII;		
(c) any circumstances affecting the scope of or conditions for notification;		
(d) any request for information which they have received from market surveillance authorities regarding conformity assessment activities;		

PUBLIC

(e) on request, conformity assessment activities performed within the scope of their notification and any other activity performed, including cross-border activities and subcontracting.		
2. Each notified body shall inform the other notified bodies of:		
(a) quality management system approvals which it has refused, suspended or withdrawn, and, upon request, of quality system approvals which it has issued;		
(b) EU technical documentation assessment certificates or any supplements thereto which it has refused, withdrawn, suspended or otherwise restricted, and, upon request, of the certificates and/or supplements thereto which it has issued.		

PUBLIC

3. Each notified body shall provide the other notified bodies carrying out similar conformity assessment activities covering the same artificial intelligence technologies with relevant information on issues relating to negative and, on request, positive conformity assessment results.		
	4. The obligations in this provision only apply as far as secrecy obligations do not conflict.	Information from the notified body can only be transmitted as far as transmission does not interfer with serecy obligations especially regarding operative scenarios. This may already be covered by Art. 70, but we would still like to emphasize that this is an important issue for us, wich may be addressed here as well.
Article 47 *Derogation from conformity assessment procedure*		We suggest to add a paragraph to empower the EU-COM to extend the validity of an authorisation to the territory of the Union for a limited period of time by means of implementing acts.

PUBLIC

		Please also refer to the separate position paper handed in, proposing necessary diverging regulations for public administration (especially LEAs and migration authorities) „[TITLE]“. Overall, the AI regulation should provide guidelines for a balanced reconciliation of fundamental rights concerns with the operational concern of a legally secure and utilisable certification in such urgent cases and, in particular, specify under which conditions the certification procedure affects the legality of a measure based on the provisional use of AI.
1. By way of derogation from Article 43 **and upon a duly justified request**, any market surveillance authority may authorise the placing on the market or putting into service of specific high-risk AI systems within the territory of the	By way of derogation from Article 43, ~~any market surveillance and upon duly justified request~~ a competent authority may authorise, on a duly justified request, the placing on the	A competent authority shall authorise, on a duly justified request.

PUBLIC

Member State concerned, for exceptional reasons of public security or the protection of life and health of persons, environmental protection and the protection of key industrial and infrastructural assets. That authorisation shall be for a limited period of time **while the necessary conformity assessment procedures are being carried out**, **taking into account the exceptional reasons justifying the derogation.**~~, while the necessary conformity assessment procedures are being carried out, and shall terminate once those procedures have been completed~~. The completion of those procedures shall be undertaken without undue delay.	market or putting into service of specific high-risk AI systems within the territory of the Member State concerned~~, for exceptional reasons~~ for which the applicable requirements referred to in this Regulation have not been carried out but use which is in interest of public security or the protection of life and health of persons, environmental protection and the protection of key industrial and infrastructural assets. That authorisation shall be for a limited period of time **while the necessary conformity assessment procedures are being carried out**, **taking into account the exceptional reasons justifying the derogation.** ~~while the necessary conformity assessment procedures are being carried out, and shall terminate once those procedures have been completed.~~ The completion of those procedures shall be undertaken without undue delay.	Specify exceptional reasons.

PUBLIC

1a. In a duly justified situation of urgency for exceptional reasons of public security or in case of specific, substantial and imminent threat to the life or physical safety of natural persons, law enforcement authorities may put a specific high-risk AI system into service without the authorisation referred to in paragraph 1 provided that such authorisation is requested during or after the use without undue delay, and if such authorisation is rejected, its use shall be stopped with immediate effect.		From the German point of view, the Presidency's proposal for an amendment is in principle understandable. However, the prerequisites for the exception in Article 47(1a) of the Draft Regulation seem too vague. In particular, it remains unclear what is meant by "duly justified situation of urgency for exceptional reasons of public security". It is discussed in DEU whether, from the perspective of the protection of fundamental rights, provisions on safeguards and a regulation on the legal consequences of violations of the provision should be included. DEU also discusses whether the market surveillance authority should be informed in such cases before the provisional commencement of operation in order to enable a review of the preconditions. From an operational point of view, the present draft does not yet answer the question of the usability of the findings from the use of a non-certified AI system in urgent cases.

PUBLIC

		DEU sees the need to address this question in the draft of the AI Act.
2. The authorisation referred to in paragraph 1 shall be issued only if the market surveillance authority concludes that the high-risk AI system complies with the requirements of Chapter 2 of this Title. The market surveillance authority shall inform the Commission and the other Member States of any authorisation issued pursuant to paragraph 1.	The authorisation referred to in paragraph 1 shall be issued only if the ~~market surveillance~~ competent authority concludes that the high-risk AI system complies with the requirements of ~~Chapter 2 of this Title~~ this Regulation. The ~~market surveillance~~ competent authority shall inform the Commission and the other Member States of any authorisation issued pursuant to paragraph 1. (…)**The obligation to inform the Commission and the other Member State applies to AI systems used for law enforcement purposes only as far as secrecy obligations do not conflict.**	Consequential amendments and taking into account other requirements, e. g. quality management system, post-market-surveilliance system, etc.. The obligation to inform the Commission and the other Member States cannot apply for undercover or other sensitive investigations of law enforcement authorities.
~~3. Where, within 15 calendar days of receipt~~		

PUBLIC

~~of the information referred to in paragraph 2, no objection has been raised by either a Member State or the Commission in respect of an authorisation issued by a market surveillance authority of a Member State in accordance with paragraph 1, that authorisation shall be deemed justified.~~		
~~4. Where, within 15 calendar days of receipt of the notification referred to in paragraph 2, objections are raised by a Member State against an authorisation issued by a market surveillance authority of another Member State, or where the Commission considers the authorisation to be contrary to Union law or the conclusion of the Member States regarding the compliance of the system as referred to in paragraph 2 to be unfounded, the Commission shall without delay enter into consultation with the relevant Member State; the operator(s) concerned shall be consulted and have the possibility to present~~		

PUBLIC

~~their views. In view thereof, the Commission shall decide whether the authorisation is justified or not. The Commission shall address its decision to the Member State concerned and the relevant operator or operators.~~		
~~5. If the authorisation is considered unjustified, this shall be withdrawn by the market surveillance authority of the Member State concerned.~~		
6. ~~By way of derogation from paragraphs 1 to 5,f~~**F**or high-risk AI systems ~~*intended to be used as safety components of*~~ ~~devices~~ **related to products**~~, or which are themselves devices,~~ covered by **Union harmonisation legislation, only the conformity assessment derogation procedures established in that legislation shall apply.** ~~Regulation (EU) 2017/745 and Regulation (EU) 2017/746, Article 59 of Regulation (EU) 2017/745 and Article 54 of~~	6. ~~By way of derogation from paragraphs 1 to 5,f~~**F**or high-risk AI systems ~~*intended to be used as safety components of*~~ ~~devices~~ **related to products**~~, or which are themselves devices,~~ covered by **Union harmonisation legislation <u>reffered to in Annex II</u>, only the conformity assessment derogation procedures established in that legislation shall apply.** ~~Regulation (EU) 2017/745 and Regulation (EU) 2017/746, Article 59 of Regulation (EU)~~	Clarification that EU legislation referred to in Annex II is meant

PUBLIC

~~Regulation (EU) 2017/746 shall apply also with regard to the derogation from the conformity assessment of the compliance with the requirements set out in Chapter 2 of this Title.~~.	~~2017/745 and Article 54 of Regulation (EU) 2017/746 shall apply also with regard to the derogation from the conformity assessment of the compliance with the requirements set out in Chapter 2 of this Title.~~By way of derogation from paragraphs 1 to ~~5~~2, for high-risk AI systems intended to be used as safety components of devices, or which are themselves devices, covered by Regulation (EU) 2017/745 and Regulation (EU) 2017/746, Article 59 of Regulation (EU) 2017/745 and Article 54 of Regulation (EU) 2017/746 shall apply also with regard to the derogation from the conformity assessment of the compliance with the requirements set out in ~~Chapter 2 of this Title~~ this Regulation.	
	7. Member States' military authorities may authorise the putting into service of high-risk AI systems developed for purposes of the defence sector or the armed forces. The authorisation shall be issued only if the high-risk AI system	This addition reflects the addition of Article 40(2).

PUBLIC

	complies with the requirements specified in Article 40 paragraph (2).	
Article 48 *EU declaration of conformity*		
1. The provider shall draw up a written **or electronically signed** EU declaration of conformity for each AI system and keep it at the disposal of the national competent authorities for 10 years after the AI system has been placed on the market or put into service. The EU declaration of conformity shall identify the AI system for which it has been drawn up. A copy of the EU declaration of conformity shall be ~~given~~ **submitted** to the relevant national competent authorities upon request.		Does the provider shall draw up a written declaration of conformity before each single AI system is placed on the market or only before the first AI system or a new version of an AI System? Our understanding is that the written declaration of conformity covers several AI system of the same version which are placed on the market or put into service.
2. The EU declaration of conformity shall state that the high-risk AI system in question meets the requirements set out in Chapter 2 of this Title. The EU declaration of conformity	The EU declaration of conformity shall state that the high-risk AI system in question meets the requirements set out in ~~Chapter 2 of this Title~~ this Regulation. The EU declaration of	Taking into account other requirements, e. g. quality management system, post-market-surveilliance system, etc..

PUBLIC

shall contain the information set out in Annex V and shall be translated into ~~an official Union language or~~ **a** languages ~~**that can be easily understood by the national competent authorities of** required by~~ the Member State(s) in which the high-risk AI system is made available.	conformity shall contain the information set out in Annex V and shall be translated into a language ~~that can easily understood~~ determined by the national competent authorities of the Member State(s) in which the high-risk AI system is made available.	
3. Where high-risk AI systems are subject to other Union harmonisation legislation which also requires an EU declaration of conformity, a single EU declaration of conformity shall be drawn up in respect of all Union legislations applicable to the high-risk AI system. The declaration shall contain all the information required for identification of the Union harmonisation legislation to which the declaration relates.		
4. By drawing up the EU declaration of conformity, the provider shall assume	4. By drawing up the EU declaration of conformity, the provider shall assume	The reference to title 2, chapter 2 is not correct.

PUBLIC

responsibility for compliance with the requirements set out in Chapter 2 of this Title. The provider shall keep the EU declaration of conformity up-to-date as appropriate.	responsibility for compliance with the requirements laid down in this regulation~~set out in Chapter 2 of this Title.~~ The provider shall keep the EU declaration of conformity up-to-date as appropriate.	
5. The Commission shall be empowered to adopt delegated acts in accordance with Article 73 for the purpose of updating the content of the EU declaration of conformity set out in Annex V in order to introduce elements that become necessary in light of technical progress.		
	(new) Where high-risk AI systems are subject to other Union legislation which also provides for the EU declaration of conformity, the EU declaration of conformity shall indicate that the high-risk AI systems also fulfil the requirements of that other legislation.	Avoid additional EU declaration

PUBLIC

Article 49 *CE marking of conformity*		
	(new) High-risk AI systems that do not have an authorisation referred to Article 47 and that are in conformity with the requirements of this Regulation shall bear the CE marking of conformity.	Consequential amendments of Article 47.
1. **The CE marking of conformity ~~referred to in paragraph 1 of this Article~~ shall be subject to the general principles set out in Article 30 of Regulation (EC) No 765/2008.** ~~The CE marking shall be affixed visibly, legibly and indelibly for high-risk AI systems. Where that is not possible or not warranted on account of the nature of the high-risk AI system, it shall be affixed to the packaging or to the accompanying documentation, as appropriate.~~		
2. ~~The CE marking referred to in paragraph 1 of this Article shall be subject to the general principles set out in Article 30 of Regulation~~	The CE marking shall be affixed before the high-risk AI system is placed on the market or put into service. It may be followed by a	In healthcare, there are some standardised pictogram or any other mark indicating a special risk or use.

PUBLIC

~~(EC) No 765/2008.~~ **The CE marking shall be affixed visibly, legibly and indelibly for high-risk AI systems. Where that is not possible or not warranted on account of the nature of the high-risk AI system, it shall be affixed to the packaging or to the accompanying documentation, as appropriate.**	pictogram or any other mark indicating a special risk or use.	
3. Where applicable, the CE marking shall be followed by the identification number of the notified body responsible for the conformity assessment procedures set out in Article 43. The identification number shall also be indicated in any promotional material which mentions that the high-risk AI system fulfils the requirements for CE marking.		
	(new) Where high-risk AI systems are subject to other Union legislation which also provides for the affixing of the CE marking, the CE marking shall indicate that the high-risk AI systems also fulfil the requirements of that other	Avoid additional CE marking

PUBLIC

	legislation.	
~~*Article 50*~~ ~~*Document retention*~~		
~~The provider shall, for a period ending 10 years after the AI system has been placed on the market or put into service, keep at the disposal of the national competent authorities:~~		
~~(a) the technical documentation referred to in Article 11;~~		
~~(b) the documentation concerning the quality management system referred to Article 17;~~		
~~(c) the documentation concerning the changes approved by notified bodies where applicable;~~		
~~(d) the decisions and other documents issued by the notified bodies where applicable;~~		

PUBLIC

~~(e) the EU declaration of conformity referred to in Article 48.~~		
Article 51 *Registration*		
Before placing on the market or putting into service a high-risk AI system **listed in Annex III** ~~referred to in Article 6(23)~~, the provider or, where applicable, the authorised representative shall register that system in the EU database referred to in Article 60.		There is a fear that the disclosure of all the law enforcement agencies' AI applications in operation or development will facilitate the assessment of an overall picture of the operational capabilities of the respective agencies. This database could potentially be used to identify capability gaps or to create thematic profiles of individual countries. This in itself could pose a security risk and affect the capabilities of the authorities. Do the Commission or other Member States share this view? Please also refer to the separate position paper handed in, proposing necessary diverging regulations for public administration (especially

PUBLIC

		LEAs and migration authorities) „[TITLE]“
	2. Before using an AI system, the relevant public authorities shall register the system used by the public authority in the EU database referred to in Article 60a.	Due to the unique role and responsibility public authorities bear, the sensitive personal data they have access to, the consequential effects their decisions have on individuals, and thus their primary obligation to respect, protect and fulfil fundamental rights, public authorities should be subject to more stringent transparency requirements when using AI systems. Hence, any deployments of AI systems – regardless of their level of risk – by or on behalf of public authorities should be registered within a separate EU database if applicable in addition to the registration as High Risk AI in the database referred to in Article 60. However, in the field of law enforcement, the possible security risk arising from the database must also be considered. Please also refer to the comment

PUBLIC

		aobove (no 276) and the separate position paper handed in, proposing necessary diverging regulations for public administration (especially LEAs and migration authorities) „[TITLE]“. For this purpose it is sufficient that the database contains the name of the AI system, a brief description of its purpose, as well as the name, address and contact information of the deploying authority. We are also still in discussion about the necessity to register AI systems that could have no impact on fundamental rights in the database, or whether these AI systems should be excluded. We are also still discussing this topic under aspects such as operating expenses, especially how to avoid exceeding operating expenses. We also reserve further comment.
TITLE IV		

PUBLIC

TRANSPARENCY OBLIGATIONS FOR CERTAIN AI SYSTEMS	**TRANSPARENCY ~~OBLIGATIONS~~ REQUIREMENTS FOR CERTAIN AI SYSTEMS**	
Article 52 *Transparency obligations for certain AI systems*	*Article 52* *Transparency ~~obligations~~requirements for certain AI systems*	In order to accommodate the AI-specific environmental and sustainability aspects, appropriate changes should be made. DE proposes laying down horizontal transparency rules in Art. 52a in order to enable providers and users to lower the energy and resource consumption caused by the development and the application of AI systems and to contribute to reach the goal of carbon neutrality. This proposal of a horizontal transparency requirement aims at reporting a limited number of easy-to-monitor sustainability indicators of AI systems. These might entail simple, binary statements on whether AI providers follow a

PUBLIC

		good practice regarding energy-efficient programming ('green coding') or whether the computing power originates from certified data centres that, for example, generate own renewable energy, obtain green electricity, use waste heat or employ more sustainable cooling techniques. The definition of sustainability indicators is best left to an expert committee; therefore, no pre-determinations should be made. This committee should also take into account the ease of monitoring and reporting to minimize burdens for AI providers, particularly SME providers. It should be composed of a broad range of experts from science, business, civil society and standardization organisations. It is conceivable that the AI Board may be involved or take over (a part of) the function of the expert committee. While we emphasize that many AI products lead to major environmental benefits, our goal is to ensure that the positive environmental outcome of an AI system is not, as an undesirable side effect, partially negated by poor energy and resource efficiency. The proposed reporting requirement firstly aims at creating incentives for AI providers to raise their sustainability

PUBLIC

		ambitions and in the medium term, increase the demand for more sustainable computing power provision. Even though energy prices spike and chips become scarce, we do not witness significant changes in AI development practices, as other performance criteria than energy efficiency predominate in design and sourcing choices. In addition, it is often not transparent for AI developers, how much energy their models and programs actually consume, due to time-based, flat rate pricing of cloud services providers. Thus, as price signals do not sufficiently incentivize more sustainable practices, transparency requirements present a necessary additional and unrestrictive incentive. To highlight credible sustainability information also offers advantages in the marketing of AI systems. It is only through such information that a distinctiveness, ideally a unique selling proposition, can be established, which gives European providers a competitive advantage in the long run ("sustainable AI made in Europe"). Due to the pace of development and many crossroad decisions on the direction of AI

PUBLIC

		development underway, the AI Act offers a timely and flexible option to address sustainability issues of AI systems, in contrast to the long, complex and detailed procedures under the Ecodesign Regulation. Further clarifications are given in recital 70.
	NEW (1) The Commission is empowered to adopt delegated acts in accordance with Article 73 to amend this Regulation by establishing, after having consulted relevant stakeholders, a common Union scheme for describing and rating the environmental sustainability of AI systems placed on the market or put into service in its territory. The scheme shall in a first step, by one year after the entering into force of this Regulation, establish a definition of AI systems' sustainability and set out a small number of easy-to-monitor indicators related, for example, to good practice through energy-efficient programming or to data centre resource efficiency. In a second step, by 2027, the scheme shall set up a lean methodology to	

PUBLIC

	measure and rate AI systems based on the indicators. The indicators and methodology shall be updated in light of technical progress. The scheme shall only concern direct environmental impacts of AI systems and may allow for exceptions for SMEs.	
1. Providers shall ensure that AI systems intended to interact with natural persons are designed and developed in such a way **that those systems inform** ~~*that*~~ natural persons ~~are informed~~ that they are interacting with an AI system, unless this is obvious **from the point of view of a reasonable person** from the circumstances and the context of use. This obligation shall not apply to AI systems authorised by law to detect, prevent, investigate and prosecute criminal offences, unless those systems are available for the public to report a criminal offence.	~~1.~~ Providers shall ensure that AI systems intended to interact with natural persons are designed and developed in such a way that natural persons are informed that they are interacting with an AI system, unless this is obvious from the circumstances and the context of use. This obligation shall not apply to AI systems authorised by law to detect, prevent, investigate and prosecute criminal offences, unless those systems are available for the public to report a criminal offence.	To increase transparency for all users. In this context, we want to emphasize the particular importance of AI in the area of media as well as in democratic processes. By the use of these applications, public discourse can be manipulated and thus significantly influenced. It is therefore important that this regulation does not preclude further regulation in this area. Furthermore, the information of the user should

PUBLIC

		be as uniform and simple as possible.
	Providers shall ensure that AI systems intended to interact with natural persons are designed and developed in such a way that natural persons are informed that they are interacting with an AI system, ~~unless this is obvious from the circumstances and the context of use~~.	Obviousness is no objective criteria. To guarantee that the interaction with an AI is recognizable for persons with different kinds of disabilities we suggest to delete this addition.
2. Users of ~~an emotion recognition system or~~ a biometric categorisation system shall inform of the operation of the system the natural persons exposed thereto. This obligation shall not apply to AI systems used for biometric categorisation, which are permitted by law to detect, prevent and investigate criminal offences**, subject to appropriate safeguards for the rights and freedoms of third parties**.	~~2. Users of an emotion recognition system or a biometric categorisation system shall inform of the operation of the system the natural persons exposed thereto. This obligation shall not apply to AI systems used for biometric categorisation, which are permitted by law to detect, prevent and investigate criminal offences~~**~~, subject to appropriate safeguards for the rights and freedoms of third parties~~**~~.~~	Proposal for a separate title and paragraph under IVA.
2a. Users of an emotion recognition system	**~~2a. Users of an emotion recognition system~~**	

PUBLIC

shall inform of the operation of the system the natural persons exposed thereto. This obligation shall not apply to AI systems used for emotion recognition which are permitted by law in the context of criminal investigations.	**~~shall inform of the operation of the system the natural persons exposed thereto. This obligation shall not apply to AI systems used for emotion recognition which are permitted by law in the context of criminal investigations.~~**	
3. Users of an AI system that generates or manipulates image, audio or video content that appreciably resembles existing persons, objects, places or other entities or events and would falsely appear to a person to be authentic or truthful ('deep fake'), shall disclose that the content has been artificially generated or manipulated.	~~3. Users of an AI system that generates or manipulates image, audio or video content that appreciably resembles existing persons, objects, places or other entities or events and would falsely appear to a person to be authentic or truthful ('deep fake'), shall disclose that the content has been artificially generated or manipulated.~~	Hinweis: AI systems can also be used to generate fake texts which may resemble the writing style of target person (e.g. GPT-2, -3). This may induce others to falsely believe the respective text has been written by the target person. The term distinguishable should be replaced be accessible. We are still examining/discussing the

PUBLIC

		systematically correct placement of these specifications/this provision.
However, the first subparagraph shall not apply where the use is authorised by law to detect, prevent, investigate and prosecute criminal offences ~~or it is necessary for the exercise of the right to freedom of expression and the right to freedom of the arts and sciences guaranteed in the Charter of Fundamental Rights of the EU, and~~ subject to appropriate safeguards for the rights and freedoms of third parties.	~~However, the first subparagraph shall not apply where the use is authorised by law to detect, prevent, investigate and prosecute criminal offences~~ or it is necessary for the exercise of the right to freedom of expression and the right to freedom of the arts and sciences guaranteed in the Charter of Fundamental Rights of the EU, and ~~subject to appropriate safeguards for the rights and freedoms of third parties.~~	The deleted sentence should be reinserted (in suggested Titel IV A).
3a. The information referred to in paragraphs 1 to 3 shall be provided to natural persons in a clear and ~~visible~~ distinguishable manner at the latest at the time of the first interaction or exposure.	~~**3a. The information referred to in paragraphs 1 to 3 shall be provided to natural persons in a clear and visible distinguishable manner at the latest at the time of the first interaction or exposure.**~~	
4. Paragraphs 1, 2**, 3** and 3**a** shall not affect	~~4. Paragraphs 1, 2 and 3 shall not affect the~~	

PUBLIC

the requirements and obligations set out in Title III of this Regulation~~.~~ **and shall be without prejudice to other transparency obligations for users of AI systems laid down in Union or national law**.	~~requirements and obligations set out in Title III of this Regulation.~~	
	TITLE IVA **INFORMATION TO BE PROVIDED TO NATURAL PERSONS** ***Art. 52a*** ***Information to be provided for emotion recognition and biometric categorisation systems*** 1. Users of an emotion recognition system or a biometric categorisation system shall inform of the operation of the system the natural	Regarding supervision, it would still be necessary to discuss further which authorities should be responsible for enforcing the respective obligations under this Title. Contradictions with the supervisory responsibilities under the GDPR as well as supervisory structures under other Union legislation should be avoided.

PUBLIC

	persons exposed thereto. This obligation shall not apply to AI systems used for biometric categorisation, which are permitted by law to detect, prevent and investigate criminal offences or prevent of a threat to critical infrastructure, life, health or physical safety of natural persons. 2. Providers of an AI system that generates or manipulates image, audio or video content that appreciably resembles existing persons, objects, places or other entities or events and would falsely appear to a person to be authentic or truthful ('deep fake'), shall disclose that the content has been artificially generated or manipulated. However, the first subparagraph shall not apply	We are still discussing if AI systems used for the prevention of a threat to critical infrastructure, life, health, physical safety of natural persons or public safety should also be excluded from the obligations of par. 1 and may comment on this later.

PUBLIC

	where the use is authorised by law to detect, prevent, investigate and prosecute criminal offences or prevent of a threat to critical infrastructure, life, health, or physical safety of natural persons or it is necessary for the exercise of the right to freedom of expression and the right to freedom of the arts and sciences guaranteed in the Charter of Fundamental Rights of the EU, and subject to appropriate safeguards for the rights and freedoms of third parties. ***Art. 52b*** ***Information to be provided for high-risk AI systems*** 1. Users of High Risk-AI systems shall provide the person affected by a decision at least	This obligation of para 2 will not be effectively enforceable if it is addressed to users. Users are usually not clearly identifiable to the enforcing market surveillance authorities. Instead, it seems more sensible to oblige the providers to make it technically possible for users to mark/label the content. We are still examining/discussing the systematically correct placement of these specifications/this provision.

PUBLIC

	partially determined by the output of the AI system ("Affected Person") with standardized information about	One of the primary reasons why AI is being regulated at all is to protect individuals from the risks generated by AI systems to fundamental

PUBLIC

		rights and to create trust. In this context, the need for transparency is one of the main factors explicitly addressed by the AIA. The GDPR already grants certain rights to information to natural persons/data subjects. However, the GDPR does not sufficiently cover constellations where AI systems are involved. For example, Articles 22, 13 (2) (f), 14 (2) (g) and 15 (1) (h) address automated processing, but these provisions only cover cases where natural persons are directly exposed to automated decision making. This would – at least according to the wording of the GDPR - not cover the constellation that AI is used to prepare a decision ultimately made by a human (for example, an AI might provide a credit rating score that a bank employee uses to decide on the granting of a loan to a natural person).This constellation may have consequences for the natural person that can be just as serious as where the natural person is directly exposed to

PUBLIC

		automated processing, and gives therefore rise to a similar need for protection. It is necessary for an affected natural person to understand the risks which they are being subjected to in order to be able to seek redress. Therefore, we consider it necessary to include an obligation of the user to provide the affected natural person with standardized information on the use and general function of the AI system and to include a substantive right for affected persons to request further information on the input data and the relevant data categories, in constellations, where an AI system is used to prepare a human decision. We also consider it necessary to supplement the existing information requirements in the GDPR with some further information that seem necessary specifically in the context of AI systems in order to provide natural persons with all relevant knowledge to understand their

PUBLIC

		situation. With the suggested Article 52b, we aim to avoid any duplication or overlapping with existing rights under the GDPR, but merely to supplement them only to the extent necessary, as it is important to avoid legal uncertainty regarding the relation of this Regulation to the GDPR. In addition to the implementation of Art. 52b new, the following sentence should be added to Recital 43: „Natural persons affected by decisions at least partially determined by high-risk AI systems (this includes decisions that were made after a high-risk AI system provided a recommendation for the decision) placed on the EU market or otherwise put into service should be informed in an appropriate, easily accessible and comprehensible manner about

PUBLIC

		the use of the AI system, the role and purpose of the AI system in the decision-making process, the logic involved and the main parameters of decision making. Such information could be provided in electronic form, for example, when addressed to the public, through a user‘s website while providing the link to this website at the time the decision is communicated to the affected person. For this purpose, with regard to the standardized information to be provided under para. 1 and 2, the user should be able utilise the information received from the provider according to article 13 paragraph 3 letters b and d. With regard to the individual explanation according to para. 3, the affected natural person must be provided with the individual input data relating to the affected natural person and the relevant data categories that serve as the main parameters on the basis of which the output was given.”

PUBLIC

		Furthermore, the term “affected natural person” should be defined in Art. 3 AIA. The rights of the persons affected are limited by the wording to individual persons. This does not include the protection or representation of collective interests. This means that particularly vulnerable groups or groups at risk of discrimination can exercise their rights less effectively. Possibilities for collective enforcement still need to be examined within the federal government. Generally, it has to be made sure that Union or Member State law containing prohibitions of disclosure or relevant restrictions on the affected person’s right of access to the information

PUBLIC

		covered by Art. 52a (new) remains unaffected, especially in the area of law enforcement. For example: In case of suspicion of money laundering, the competent authority (Financial Intelligence Unit, "FIU") is prohibited to reveal information to the affected person (based on Art. 41 para. 4 EU-act). Therefore, we suggest to add para. 4 or a similar provision inspired by Art. 23 GDPR saying that the obligations or rights granted under Art. 52 a (new) can be restricted by Union or Member State law that e.g. prohibits or restricts the user of the AI system to reveal the information, provided that such a prohibition or restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society.

PUBLIC

	(a) the fact that an AI system has been used within the context of the decision-making process; (b) a reference to the EU-data base as referred to in Art 51, 60 and Annex VIII;	

PUBLIC

	(c) the general role and purpose of the AI system in the decision-making-process; (d) the relevant data categories of the input data; (e) information provided to the user pursuant to Article 13 paragraph 3 letters b and d; and (f) the right to receive an explanation upon request according to paragraph 3. The information shall be provided at the time the decision is communicated to the affected natural person.	We are still discussing details on this provision. Paragraph 2 only covers situations that are already covered by automated processing in accordance with Article 22 of the GDPR (i.e.,

PUBLIC

	2. Where a high-risk AI system is used for automated individual decision-making, including profiling, within the meaning of Article 22 of Regulation (EU) 2016/679, information according to Articles 13 (2) (f), 14 (2) (g) and 15 (1) (h) of Regulation (EU) 2016/679 shall also comprise information according to paragraph (1) (b), (d), (e) and (f). 3. Users of high-risk AI systems shall provide the affected natural person upon his or her request in addition to the standardized information provided according to paragraph 1 with concise, complete, correct and clear explanation of the individual input data relating to the affected natural person and the relevant data categories on the basis of which the decision was made.	constellations where a natural person is exposed directly to an AI system). In these constellations, information obligations under the GDPR are extended to certain further, AI specific information according to paragraph 1.

PUBLIC

	4. Paragraph 1 (e),2 insofar as it refers to paragraph 1 lit. (e) and paragraph 3 shall not apply to the use of AI systems that are authorised by law to detect, prevent, investigate and prosecute criminal offences or prevent of a threat to critical infrastructure, life, health or physical safety of natural persons. 5. Paragraph 1 to 3 shall not apply to the use of AI systems (a) for which exceptions from, or restrictions to, the obligations under this Article follow from Union or Member State law (such as a prohibition or restriction to disclose information covered by paragraph 1 and 2 to the affected person), which lays down appropriate other safeguards for the affected person's rights and	We are still discussing if AI systems used for the prevention of a threat to critical infrastructure, life, health, physical safety of natural persons or public safety should also be excluded from the obligations of par. 1-3 and may comment on this later.

PUBLIC

	freedoms and legitimate interests when such an exception or restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society; or (c) that have only minor influence within the decision-making process. 6. Information according to paragraph 1 to 3 shall be given in a concise, transparent, intelligible and easily accessible form appropriate to different kinds of disabilities, using clear and plain language. ***Article 52c*** ***Relation to Title III***	

PUBLIC

	Obligations under this Title shall not affect the requirements and obligations set out in Title III of this Regulation.	This corresponds to the current Article 52(4) and should apply to the entire title.

PUBLIC

~~**TITLE IVA**~~		
~~**GENERAL PURPOSE AI SYSTEMS**~~		
~~***Article 52a***~~		
~~***General purpose AI systems***~~		
~~**1. The placing on the market, putting into service or use of general purpose AI systems shall not, by themselves only, make those systems subject to the provisions of this Regulation.**~~		
~~**2. Any person who places on the market or puts into service under its own name or trademark or uses a general purpose AI**~~		

PUBLIC

~~**system made available on the market or put into service for an intended purpose that makes it subject to the provisions of this Regulation shall be considered the provider of the AI system subject to the provisions of this Regulation.**~~		
~~**3. Paragraph 2 shall apply, mutatis mutandis, to any person who integrates a general purpose AI system made available on the market, with or without modifying it, into an AI system whose intended purpose makes it subject to the provisions of this Regulation.**~~		
~~**4. The provisions of this Article shall apply irrespective of whether the general purpose AI system is open source software or not.**~~		
TITLE V		

PUBLIC

MEASURES IN SUPPORT OF INNOVATION		
Article 53 *AI regulatory sandboxes*		We support the establishment of regulatory sandboxes as an important to tool support innovation.
-1a. National competent authorities may establish AI regulatory sandboxes for the development, training, testing and validation of innovative AI systems, before their placement on the market or putting into service. Such regulatory sandboxes may include testing in real world conditions supervised by the national competent authorities.	**-1a. National competent authorities may establish AI regulatory sandboxes for the development, training, testing and validation of innovative AI systems under the direct supervision, guidance and support by the national competent authority, before their placement on the market or putting into service. Such regulatory sandboxes may include testing in real world conditions supervised by the national competent authorities.**	Add "under the direct supervision, guidance [..] by the national competent authority". The key element of supervision and guidance by the national competent authority was deleted by deleting the whole article 53 (1) and should be returned. Add *"support"*: Especially for start-ups it is very important that competent authorities – within their legal possibilities – act as supporters in ensuring compliance, e.g. through

PUBLIC

		mentoring, personal exchange or customized guidance. The impressive examples of data regulatory sandboxes by the French CNIL and the British ICO also explicitly "support" the projects. The term "support" is also used in EU Commission's Better Regulation Toolbox Tool #69 on regulatory sandboxes (page 597).
-1b. In relation to AI systems provided by the EU institutions, bodies and agencies, such AI regulatory sandboxes may be established by the European Data Protection Supervisor.		
-1c Where appropriate, national competent authorities shall cooperate with other relevant national authorities and may allow for the involvement of other actors within the AI ecosystem such as national or European standardisation organisations, notified bodies, testing and experimentation facilities, research and experimentation labs and	**-1c Where appropriate, national competent authorities shall cooperate with other relevant national authorities and may allow for the involvement of other actors within the AI ecosystem such as national or European standardisation organisations, notified bodies, testing and experimentation facilities, research, ~~and~~ experimentation labs, ~~and~~**	

PUBLIC

innovation hubs.	**innovation hubs and civil society organisations.**	
-1d. Paragraphs 1-a and -1b shall not affect other regulatory sandboxes established under national or Union law. Member States shall ensure an appropriate level of cooperation between the authorities supervising those other sandboxes and the national competent authorities.		
1. ~~AI regulatory sandboxes established by one or more Member States competent authorities or the European Data Protection Supervisor shall provide a controlled environment that facilitates the~~**for the** ~~development, testing and validation of innovative AI systems, for a limited time before their placement on the market or putting into service pursuant to a specific plan. This shall take place under the direct supervision and~~		

PUBLIC

~~guidance by the~~ **national** ~~competent authorities~~ **~~and, where appropriate, in cooperation with other relevant national authorities, or by the European Data Protection Supervisor in relation to AI systems provided by the EU institutions, bodies and agencies.~~** ~~with a view to ensuring compliance with the requirements of this Regulation and, where relevant, other Union and Member States legislation supervised within the sandbox.~~		
~~1a. The national competent authority or the European Data Protection Supervisor, as appropriate, may also supervise testing in real world conditions upon the request of participants in the sandbox.~~		
1b. The establishment of AI regulatory sandboxes under this Regulation ~~as defined in paragraph 1~~ shall aim to contribute to one or more of the following objectives:		

PUBLIC

a) foster innovation and competiveness and facilitate the development of an AI ecosystem;		
b) facilitate and accelerate access to the Union market for AI systems, ~~including~~ in particular when provided by small and medium enterprises (SMEs), including ~~and~~ start-ups;		
c) improve legal certainty and contribute to the shareing of best practices through cooperation with the authorities involved in the AI regulatory sandbox with a view to ensuring future compliance with this Regulation and, where appropriate, with other Union and Member States legislation;		
~~d) enhance authorities' understanding of the opportunities and risks of AI systems as~~	**d) enhance authorities' understanding of the opportunities and risks of AI systems as**	To prevent diverging approaches, the key objective of regulatory learning with its

PUBLIC

~~**well as of the suitability and effectiveness of the measures for preventing and mitigating those risks;**~~	**well as of the suitability and effectiveness of the measures for preventing and mitigating those risks;**	different facets (better understanding of opportunities and risks, contribution to effective implementation and development of standards and specification) should be returned. The Council conclusion on regulatory sandboxes (para 10) as well as the Commission's Better regulation toolkit (page 595) highlight regulatory learning as crucial feature of regulatory sandboxes.
~~**e) contribute to the uniform and effective implementation of this Regulation and, where appropriate, its swift adaptation, notably as regards the techniques in Annex I, the high-risk AI systems in Annex III, the technical documentation in Annex IV;**~~	**e) contribute to the uniform and effective implementation of this Regulation and, where appropriate, its evidence based swift adaptation, notably as regards the techniques in Annex I, the high-risk AI systems in Annex III, the technical documentation in Annex IV;**	see comment on d)
~~**f) contribute to the development or update of harmonised standards and common specifications referred to in Articles**~~	**f) contribute to the development or update of harmonised standards and common specifications referred to in Articles**	see comment on d)

PUBLIC

~~**40 and 41 and their uptake by providers.**~~	**40 and 41 and their uptake by providers.**	
	g) contribute to the possible future evidence-based advancement of this Regulation and, where appropriate, of other Union and Member States legislation.	Add new para: The Council conclusion on regulatory sandboxes (para 10) as well as the Commission's Better regulation toolkit (page 595) highlight regulatory learning as crucial feature of regulatory sandboxes. Regulatory sandboxes should contribute to resilient and relevant legislation through facilitating regulatory learning.
2. ~~**The AI regulatory sandboxes may be established upon the decision of the national competent authorities, including jointly with those from other Member States, or by the European Data Protection Supervisor. They may be established upon request of any provider or prospective provider having an interest in participating in the sandbox, or at the sole initiative of the national competent authorities or the European Data Protection Supervisor.**~~		

PUBLIC

~~Member States shall ensure that to the extent the innovative AI systems involve the processing of personal data or otherwise fall under the supervisory remit of other national authorities or competent authorities providing or supporting access to data, the national data protection authorities and those other national authorities are associated to the operation of the AI regulatory sandbox.~~		Why was the involvement of national data protection authorities in the processing of personal data deleted?
~~As appropriate, national competent authorities may allow for the involvement in the AI regulatory sandbox of other actors within the AI ecosystem such as national or European standardisation organisations, notified bodies, testing and experimentation facilities, research and experimentation labs and innovation hubs.~~		
2a. ~~Access to the AI regulatory sandboxes and supervision and guidance by the relevant~~		

PUBLIC

~~authorities shall be free of charge, without prejudice to exceptional costs that national competent authorities may recover in a fair and proportionate manner.~~ ~~It~~ Access to the AI regulatory sandboxes shall be open to any provider or prospective provider of an AI system who fulfils the eligibility and selection criteria referred to in paragraph 6(a) and who has been selected by the national competent authorities or, where applicable, by the European Data Protection Supervisor following the selection procedure referred to in paragraph 6(b). Providers or prospective providers may also submit applications in partnership with users or any other relevant third parties.		
Participation in the AI regulatory sandbox shall be limited to a period that is appropriate to the complexity and scale of the project ~~in any case not longer than a~~		

PUBLIC

~~**maximum period of 2 years, starting upon the notification of the selection decision. The participation may be extended for up to 1 more year**~~**. This period may be extended by the national competent authority.**		
Participation in the AI regulatory sandbox shall be based on a specific plan referred to in paragraph 6 of this Article that shall be agreed between the participant(s) and the national competent authoritie(s) or the European Data Protection Supervisor, as applicable. ~~**The plan shall contain as a minimum the following:**~~	**Participation in the AI regulatory sandbox shall be based on a specific plan referred to in paragraph 6 of this Article that shall be agreed between the participant(s) and the national competent authoritie(s) or the European Data Protection Supervisor, as applicable. The plan shall contain as a minimum the following:**	The requirements to the specific plan should be returned. The lessons from sandboxes are only comparable if there is a common framework. Harmonizing the rules concerning this specific plan of participation helps regulatory learning as well. - It is important to have a clear objective in mind when operating a regulatory sandbox. If the context of participation is documented well, it is easier to compare the results of the sandbox with sandboxes that have taken place under the supervision of other national competent authorities

PUBLIC

~~**a) description of the participant(s) involved and their roles, the envisaged AI system and its intended purpose, and relevant development, testing and validation process;**~~	**a) description of the participant(s) involved and their roles, the envisaged AI system and its intended purpose, and relevant development, testing and validation process;**	See comment above.
~~**b) the specific regulatory issues at stake and the guidance that is expected from the authorities supervising the AI regulatory sandbox;**~~	**b) the specific regulatory issues at stake and the guidance and support that is expected from the authorities supervising the AI regulatory sandbox;**	See comment above; add "*support*": Especially for start-ups it is very important that competent authorities – within their legal possibilities – act as supporters in ensuring compliance, e.g. through mentoring, personal exchange or customized guidance.
	bb) the novelty of the specific regulatory issue, compared to the annual reports referred to in Article 53(5), and whether analyzing this regulatory issue in the regulatory sandbox contributes to the objectives of Article 53(1b)(c) and (d);	Additionally we propose a new provision 2a(bb). Note that this does not require participants to have a novel regulatory issue in order to participate in the sandbox. Whether a regulatory issue is novel can also become clear during the sandbox.

PUBLIC

~~**c) the specific modalities of the collaboration between the participant(s) and the authoritie(s), as well as any other actor involved in the AI regulatory sandbox;**~~	**c) the specific modalities of the collaboration between the participant(s) and the authoritie(s), as well as any other actor involved in the AI regulatory sandbox;**	See comment above.
~~**d) a risk management and monitoring mechanism to identify, prevent and mitigate any risk referred to in Article 9(2)(a);**~~	**d) a risk management and monitoring mechanism to identify, prevent and mitigate any risk referred to in Article 9(2)(a);**	See comment above.
	(dd) obligations for the participants to provide the authority with information needed for the authority's evaluation of the project.	An evaluation on the basis of current and accurate data is crucial in order to enhance authorities' understanding and to allow for regulatory learning. COM's better regulation toolkit p. 597 stresses that the main evaluation criteria (and that includes also the data and data source) should be established ex ante.
e) ~~**the key milestones to be completed by the participant(s) for the AI system to be considered ready to exit from the regulatory sandbox.**~~	**e) the key milestones to be completed by the participant(s) for the AI system to be considered ready to exit from the regulatory sandbox.**	See comment above.
	(2b) After an AI regulatory sandbox has ended, the participant(s) and the national	In various national regulatory sandboxes, it is common practice to issue an exit report after the

PUBLIC

	competent authoritie(s) or the European Data Protection Supervisor, as applicable, shall draw up an exit report. This exit report shall contain as a minimum the following: **a) The plan referred to in paragraph 2a of this Article;** **b) An evaluation of the specific regulatory issues that were at stake during the AI regulatory sandbox, including a problem definition and proposed solutions;** **c) Whether the key milestones referred to in paragraph 2a(e) of this Article have been completed;** **d) A conclusion on the lessons learnt, specified in the following categories of use:** **1. An improved understanding on the implementation of the AI regulatory sandboxes;** **2. Improved methods of supervision by national competent authorities;** **3. A revised or novel interpretation of**	sandbox has concluded. We propose to include this practice in the AI Act as well. The exit reports focus more specifically on the case at hand, instead of the more vaguely drafted 'annual reports' (which also focus on the implementation of sandboxes). In order to truly utilize lessons learnt, they must first be defined. The national competent authorities are in the best position to do this, right after a sandbox has ended. Under paragraph 5a, the exit reports will then be used by the AI Board and Commission to improve interpretation, guidance, communication and amendments regarding this Regulation.

PUBLIC

	this Regulation.	
3. The **participation in the** AI regulatory sandboxes shall not affect the supervisory and corrective powers of the ~~competent~~ authorities **supervising the sandbox**. **Those authorities shall exercice their supervisory powers in a flexible manner within the limits of the relevant legislation, using their discretionary powers when implementing legal provisions to a specific AI sandbox project.~~.~~, with the objective of supporting innovation in AI in the Union** ~~Any significant risks to health and safety and fundamental rights identified during the development and testing of such systems shall result in immediate mitigation and, failing that, in the suspension of the development and testing process until such mitigation takes place.~~	with the objective of supporting innovation in AI in the Union. Any significant risks to health and safety and fundamental rights identified during the development and testing of such systems shall result in immediate mitigation and, failing that, in the suspension of the development and testing process until such mitigation takes place. The authorities shall cooperate with the participants of the sandbox to develop and implement a mitigation plan to enable a resumption of the testing process without undue delay.	The former formulation should be reinserted and amended since significant risks to health and safety and fundamental rights require immediate mitigation (and failing that suspension). The authorities shall support the participants in developing and implementing the mitigation.
~~However, p~~**Provided that the participant(s) respect the sandbox plan and**		We welcome the amendment. However, in order to ensure the protection of fundamental rights,

PUBLIC

the terms and conditions for their participation as referred to in paragraph 6(c) and follow in good faith the guidance given by the authorities, no administrative ~~enforcement action shall be taken~~ fines shall be imposed by the authorities for infringement of applicable Union or Member State legislation, including the provisions of this Regulation.		we remain critical of the fact that fines should continue to be excluded even in the case of infringements that lead to high risks for the rights and freedoms of natural persons. Legal Council Service should verify if with regard to the financial market a sector specific clarification is necessary. The rules and provisions for participation in a sandbox program should not contradict the harmonized financial market regulation. We would therefore advise to consult with COM (DG FISMA) on this specific financial sector related question.
4. **The p**~~P~~articipants ~~in the AI regulatory sandbox~~ remain liable under applicable Union and Member States liability legislation for any ~~harm~~ **damage caused** ~~inflicted~~ ~~on third parties~~		To avoid legal uncertainties, it is necessary to regulate which stakeholder/participant is the controller regarding personal data. If it is correct that the technical infrastructure is established

PUBLIC

in the course of their participation ~~as a result from the experimentation taking place~~ in ~~the~~ **an AI-regulatory** sandbox.		and run by Member States competent authorities or the European Data Protection Supervisor, it should be considered to amend para. 4 correspondingly. In our understanding, compensation for violation of personal data is based exclusively on the GDPR. Is this the purpose of this provision?
4a. Upon request of the provider or prospective provider of the AI system, the national competent authority shall provide, where applicable, a written proof of the activities successfully carried out in the sandbox. Such written proof could be taken into account by market surveillance authorities or notified bodies, as applicable, in the context of conformity assessment procedures or market surveillance checks.		
4b. The AI regulatory sandboxes shall be		

PUBLIC

designed and implemented in such a way that, where relevant, they facilitate cross-border cooperation between the national competent authorities. ~~and synergies with relevant sectoral regulatory sandboxes. Cooperation may also be envisaged with third countries outside the Union establishing mechanisms to support AI innovation.~~		
5. ~~Member States'~~ **~~National~~** ~~competent authorities that have established AI regulatory sandboxes~~ **~~and the European Data Protection Supervisor~~** ~~shall coordinate their activities and cooperate within the framework of the European Artificial Intelligence Board.~~		
~~They~~ **National competent authorities shall make publicly available ~~publish on their websites~~** ~~submit~~ annual reports **on** ~~to the Board and the Commission on the results from~~ the implementation of ~~those~~ **the AI regulatory**	[..] **Those annual reports shall be submitted to the AI Board which shall annually make publicly available ~~publish on its website~~ a summary of all good practices, lessons learnt and recommendations**.	Small addition to ensure regular feedback from the AIB.

PUBLIC

sandboxes, including good practices, lessons learnt and recommendations on their setup and, where relevant, on the application of this Regulation and other Union legislation supervised within the sandbox. **Those annual reports shall be submitted to the AI Board which shall make publicly available ~~publish on its website~~ a summary of all good practices, lessons learnt and recommendations**.		
	5a. **1. After an AI regulatory sandbox has ended, the national competent authority shall share the exit report of that sandbox with the AI Board and the Commission.** **2. The AI Board shall use the annual reports of paragraph 5 of this Article and the exit reports it recieves according to paragraph 1 in the exercise of its tasks as listed in Article 58.**	To ensure that sandboxes will deliver more than vaguely defined annual reports, this paragraph requires the AI Board and Commission to utilize the exit reports that have been drawn by the national competent authorities. As these exit reports may contain sensitive information that should be kept confidential, an explicit reference to Article 70 has been made. This also prevents a situation in which participants may be reluctant to participate in

	3. The Commission shall use the annual reports of paragraph 5 of this Article and the exit reports it recieves according to paragraph 1 in the exercise of its tasks in Articles 4, 7, 11(3) and 58a. **The exit reports shall be shared on a confidential basis and in accordance with Article 70.**	sandboxes because they are afraid that their trade secrets or other sensitive information will be made public.
5b. The Commission shall ensure that information about AI regulatory sandboxes, including about those established under this Article, is available through ~~a~~ the single information platform ~~as~~ referred to in Article 55(3)(b).		
6. The ~~**detailed**~~ modalities and the conditions **for the establishment and** ~~of the~~ operation of the AI regulatory sandboxes **under this Regulation**~~, including the eligibility criteria and the procedure for the application, selection,~~	6. The ~~**detailed**~~ modalities and the conditions **for the establishment and** ~~of the~~ operation of the AI regulatory sandboxes **under this Regulation**, including the eligibility criteria and the procedure for the application, selection,	Add *"including the eligibility criteria..":* we propose to return to the previous text. The lessons from sandboxes are only comparable if there is a common framework for the learning aspect.

PUBLIC

PUBLIC

~~participation and exiting from the sandbox, and the rights and obligations of the participants shall be set out in implementing acts. Those implementing acts~~ shall be adopted **through implementing acts** in accordance with the examination procedure referred to in Article 74(2).	participation and exiting from the sandbox, and the rights and obligations of the participants shall be set out in implementing acts. Those implementing acts shall be adopted **through implementing acts** in accordance with the examination procedure referred to in Article 74(2). These modalities and conditions shall foster innovation and shall take into account particularly the special circumstances of participating small and medium-sized enterprises.	Add *"These modalities and conditions shall foster innovation and shall take into account particularly the special circumstances of participating small and medium-sized enterprises"*: The objectives of the regulatory sandboxes should be to foster AI innovation (recital 71). In order to promote innovation, it is important that the interests of small-scale providers are taken into particular account (recital 73. Both must be reflected in the regulatory sandboxes' modalities and conditions.
Those implementing acts shall include ~~general common rules~~ common main principles on the following issues:	**Those implementing acts shall include ~~general common rules~~ ~~common main principles~~ general common rules on the following issues:**	'Common main principles' may result in differently organised sandboxes throughout Europe.
a) ~~the~~ eligibility and selection ~~criteria~~ for	**a) ~~the~~ eligibility and selection ~~criteria~~**	

PUBLIC

participation in the AI regulatory sandbox;	**criteria for participation in the AI regulatory sandbox, including the capacity to preserve the specific data protection, data security and confidentiality requirements.**	
b) ~~the~~ procedure for the application, ~~selection,~~ participation, monitoring, ~~and~~ exiting from and termination of the AI regulatory sandbox~~, including templates of all relevant documents~~;	**b) ~~the~~ procedure for the application, ~~selection~~ selection~~,~~ participation, monitoring, ~~and~~ exiting from and termination of the AI regulatory sandbox~~, including templates of all relevant documents~~;**	
	(bb) provisions for a possible subsequent introduction into permenant operation	Add *"provisions for a possible subsequent introduction into permanent operation":* In order to provide innovators with transparent and reliable investment conditions, perspectives for scaling the AI systems outside the regulatory sandbox should be set up.
c) the terms and conditions applicable to the participants~~, including in relation to their collaboration with the authorities supervising~~		

PUBLIC

~~**the sandbox, as well as the conditions for suspension and termination of the participation in the sandbox;**~~		
	(cc) The modalities for the evaluation of the sandbox and the transfer of results into legislative process;	As emphasized in recital 72, one objectives of the regulatory sandboxes is to enhance the competent authorities' oversight and understanding. EU Commission's Better Regulation Toolkit (page 595 and 597) and the Council Conclusions on Reg. Sandboxes (para 10) also stress the objective of advancing regulation through regulatory learning. To achieve this overarchingly, clear rules shall be set up.
~~**d) the modalities for the involvement in the AI regulatory sandbox of other national authorities and other actors within the AI ecosystem;**~~		
~~**e) the modalities and procedures for cross-border cooperation, including the establishment and operation by two or more**~~		

PUBLIC

~~**Member States of cross-border AI regulatory sandboxes.**~~		
	(new) The AI regulatory sandboxes do not modify the competencies and regulations regarding the fulfilment of requirements on the clinical evaluation, performance evaluation and clinical evidence for high-risk AI systems which are safety components of devices, or are devices themselves, covered by Regulation (EU) 2017/745 or Regulation (EU) 2017/746. Without prejudice to the requirements on clinical evaluation, performance evaluation and clinical evidence of Regulation 2017/745 and 2017/746, data collected for those devices within regulatory sandboxes may be used with regard to clinical evaluation or performance evaluation and for demonstration of compliance with those regulatory requirements.	Add: *"The AI regulatory sandboxes.."*: Data collected for medical device AI-systems and used for the demonstration of compliance or of the clinical evidence should fulfill the regulatory requirements of Regulation 2017/745 and 2017/746. Add: *"By derogation from paragraphs 1.."*: Given their innovative nature and the resulting effects on the development of advanced military capabilities, AI regulatory sandboxes for purposes of the defence sector or the armed forces should be fully outside the public domain. They also should be controled by Member States' military authorities only since Member States are the sole owners of military capabilities in accordance with Union law (cf.

PUBLIC

	(new) By derogation from paragraphs 1 through 6, only Member States' military authorities may establish, operate, and supervise AI regulatory sandboxes for purposes of the defence sector or the armed forces. Member States' military authorities shall establish the necessary conditions for such developing and testing.	Article 42(3) TEU).
7. When national competent authorities consider authorising testing in real world conditions supervised within the framework of an AI regulatory sandbox established under this Article, they shall specifically agree with the participants on the terms and conditions of such testing and in particular on the appropriate safeguards. Where appropriate, they shall cooperate with other national competent authorities with a view to ensure consistent practices across the Union.	**7. When national competent authorities consider authorising testing in real world conditions supervised within the framework of an AI regulatory sandbox established under this Article, they shall ensure that the testing in real world conditions takes place according to the requirements of Articles 54a and 54b ~~specifically agree with the participants on the terms and conditions of such testing and in particular on the appropriate safeguards.~~ Where appropriate, they shall cooperate with other national**	

PUBLIC

	competent authorities with a view to ensure consistent practices across the Union.	
Article 54 ~~*Further p*~~ ***Further pP****rocessing of personal data for developing certain AI systems in the public interest in the AI regulatory sandbox*		We support the proposal for further processing of personal data in regulatory sandboxes as an important means of promoting innovation, since the further processing would provide significant benefit the development of AI systems in the public interest.
1. In the AI regulatory sandbox personal data **lawfully collected for other purposes** ~~lawfully collected for other purposes~~ ~~shall~~ **may** be processed for the purposes of developing**,** ~~and~~ testing **and training of** ~~certain~~ innovative AI systems in the sandbox under the following **cumulative** conditions:	1. In the AI regulatory sandbox established by the Member States or the European Data Protection Supervisor personal data **lawfully collected for other purposes** ~~lawfully collected for other purposes~~ ~~shall~~ **may** be processed by participants of the sandbox for the purposes of developing**,** ~~and~~ testing **and training of** ~~certain~~ innovative AI systems in the sandbox under the following **cumulative** conditions:	Add: *"established by the Member States or the European Data Protection Supervisor"* and *"by participants of the sandbox":* Amendment to clarify the scope of the legal basis. The privilege to process personal data collected for other purposes is only justified when the data are processed in the sandboxes under the supervision of public authorities, in particular if special categories of personal data (Art. 9, 10 GDPR) are processed.

PUBLIC

(a) the innovative AI systems shall be developed for safeguarding substantial public interest **by a public authority or another natural or legal person governed by public law or by private law and** in one or more of the following areas:	(a) the innovative AI systems shall be developed for ~~safeguarding~~ realizing substantial public interest [..]	Replace *"safeguarding"* by *"realizing"*: Innovative AI systems shall not only serve to conserve but to pursue and realize substantial public interest through new and innovative means.
~~(i) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, under the control and responsibility of the competent authorities. The processing shall be based on Member State or Union law;~~		
(ii) public safety and ~~public~~ health, including ~~disease~~ prevention, control and treatment **of disease and improvement of health care systems**;	(ii) public safety, long-term care and ~~public~~ health, including ~~disease~~ prevention, control and treatment **of disease and improvement of health care systems**;	We support the deletion of "public", since "prevention, control and treatment" is mainly done outside public health. There is a "substantial public interest" in improving AI in health in general. Thus, regulatory sandboxes

PUBLIC

		should enable the processing of personal data within the secure environment with the required safeguards for training AI in healthcare. In the current draft, AI in the field of care cannot be trained and supported in regulatory sandboxes. Therefore we propose the addition of *"term long-term care"*.
(iii) ~~a high level of~~ protection and improvement of the quality of the environment**, including green transition, climate change mitigation and adaptation;**		We support the addition of "including green transition, climate change mitigation and adaptation" since its hightlights the potential of AI to address pressing issues posed by climate change, that go beyond the term environmental protection in its narrow interpretation. For example, AI-assisted climate change adaptation measures such as AI-based extreme heat risk maps for urban planning may exceed the scope of environmental protection.

PUBLIC

		Civil society stakeholders have called for a stronger recognition of AIs positive and negative effects on climate change.
(iv) energy sustainability, transport and mobility;		We support the addition, these sectors should be explicitly included as they are important current and future areas where AI can be of substantial benefit to society and the environment and may provide competitive advantages to companies and the European economy.
(v) ~~a high level of~~ efficiency and quality of public administration and public services~~.~~;	**(v) ~~a high level of~~ efficiency and quality of e-government~~public administration and public services.~~;**	*"public administration and public services"* seems to be far too vague and should be replaced by *"e-government"*. According to the GDPR, a legal basis for the processing of personal data should be clear and precise. The inclusion of the public sector could be ensured by our proposal "e-government".
(vi) cybersecurity and resilience of critical infrastructure.		

PUBLIC

	Add: (vii) ensuring or increasing data protection and data security in AI systems or other technology;	We suggest to add this purpose to the list. There are risks for data protection and security regarding technology in general, but also AI (such as membership attacks), and counter-measures are currently still under research. It would be in the public interest to foster such research as well by providing regulatory sandboxes. This could also help providers increase legal certainty (Art. 53 (1b) (c)) and reduce risks and costs by defining and implementing appropriate mitigation measures.
(b) the data processed are necessary for complying with one or more of the requirements referred to in Title III, Chapter 2 where those requirements cannot be effectively fulfilled by processing anonymised, synthetic or other non-personal data;	(b) the data processed are necessary for complying with one or more of the requirements referred to in Title III, Chapter 2 where those requirements cannot be effectively fulfilled by processing anonymised, synthetic or other non-personal data or at least pseudonymized personal data;	Add "or at least pseudonymized personal data":In line with the GDPR, it should be clarified, that pseudonymized personal data must be the first choice before processing other personal data.
(c) there are effective monitoring mechanisms to identify if any high risks to the ~~fundamental~~		The reference to Art. 35 GDPR is not quite clear to us because the provision does not entail a

PUBLIC

rights and freedoms of the data subjects**, as referred to in Article 35 of Regulation (EU) 2016/679 and in Article 35 of Regulation (EU) 2018/1725,** may arise during the sandbox experimentation as well as response mechanism to promptly mitigate those risks and, where necessary, stop the processing;		definition of "high risks to the rights and freedoms". Is it rather about pointing out the cases, that would require a monitoring, comparable to Art. 35 (3) GDPR?
(d) any personal data to be processed in the context of the sandbox are in a functionally separate, isolated and protected data processing environment under the control of the participants and only authorised persons have access to that data;		
(e) any personal data processed are not **to** be transmitted, transferred or otherwise accessed by other parties **that are not participants in the sandbox, unless such disclosure occurs in compliance with the GDPR or, where applicable, Regulation 2018/725, and all**		We ask for clarification of the implications of these changes. What is the reason that personal data shall be transferred? Shall it be possible that personal data are transferred out of the sandbox or shall the entire sandbox be transferred? From a data protection point of

PUBLIC

participants have agreed to it ~~nor transferred to a third country outside the Union or an international organisation~~;		view, it is of utmost importance that personal data remains in the sandboxes that provide a "safe spaces". Otherwise, it would be impossible for data subjects to follow their data. Individual data protection rights could not be further guaranteed.
(f) any processing of personal data in the context of the sandbox ~~do not lead to measures or decisions affecting the data subjects~~; **shall not affect the application of the rights of the data subjects as provided for under Union law on the protection of personal data, in particular in Article 22 of Regulation (EU) 2016/679 and Article 24 of Regulation (EU) 2018/1725;**		General rights & obligations of the GDPR must be ensured. We support the observance of the rights of the data subject provided for in the GDPR. Why has the provision, that the processing of personal data may not lead to any measures or decisions affecting the data subject, been deleted and been replaced by a reference to the rights after the GDPR, especially Art. 22 GDPR? Which decisions shall be taken inside

PUBLIC

		the sandbox affecting in any way the participating natural persons or the natural persons whose data is used in the sandbox?
(g) any personal data processed in the context of the sandbox are **protected by means of appropriate technical and organisational measures and** deleted once the participation in the sandbox has terminated or the personal data has reached the end of its retention period;		We ask for further clarification with regard to the retention period. When would personal data have to be deleted? The usually used "no longer necessary in relation to the purposes" might be pointless in the context of sandboxes since the data would remain useful. Currently, there seems to be no specific retention period laid down in the Regulation.
(h) the logs of the processing of personal data in the context of the sandbox are kept for the duration of the participation in the sandbox ~~and 1 year after its termination, solely for the purpose of and only as long as necessary for fulfilling accountability and documentation obligations under this Article or other application Union or Member States legislation~~;		From our point of view, the purpose of the logs should be clearly expressed (*"for the purpose of fulfilling accountability and documentation obligations under this Article or other applicable Union or Member States legislation")*

PUBLIC

(i) complete and detailed description of the process and rationale behind the training, testing and validation of the AI system is kept together with the testing results as part of the technical documentation in Annex IV;		
(j) a short summary of the AI project developed in the sandbox, its objectives and expected results published on the website of the competent authorities.	**[..] This provision does not apply to AI systems used for law enforcement purposes.**	For security reasons LEAs cannot be obliged to publish their intended future methods and processes.
1a. For the purpose of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, under the control and responsibility of law enforcement authorities, the processing of personal data in AI regulatory sandboxes shall be based on a specific		

PUBLIC

Member State or Union law and subject to the same cumulative conditions as referred to in paragraph 1.		
2. ~~Paragraph 1 is without prejudice to Union or Member States legislation excluding processing for other purposes than those explicitly mentioned in that legislation.~~ **Paragraph 1 is without prejudice to Union or Member States laws laying down the basis for the processing of personal data which is necessary for the purpose of developing, testing and training of innovative AI systems or any other legal basis, in compliance with Union law on the protection of personal data.**		
Article 54a		
Testing of high-risk AI systems in real world conditions outside AI regulatory sandboxes		We support to include testing in real world conditions as the Council Conclusion on Regulatory Sandboxes (para 8) as well as the

PUBLIC

		Commission's Better regulation toolkit (page 593) emphasize the relevance of a real-world environment for regulatory sandboxes.
1. Testing of AI systems in real world conditions outside AI regulatory sandboxes may be conducted by providers or prospective providers of high-risk AI systems listed in Annex III, in accordance with the provisions of this Article and the real-world testing plan referred to in this Article.		
The detailed elements of the real-world testing plan shall be specified in implementing acts adopted by the Commission in accordance with the examination procedure referred to in Article 74(2).		
This provision shall be without prejudice to Union or Member State		

PUBLIC

legislation for the testing in real world conditions of high-risk AI systems related to products covered by legislation listed in Annex II.		
2. Providers or prospective providers may conduct testing of high-risk AI systems referred to in Annex III in real world conditions at any time before the placing on the market or putting into service of the AI system on their own or in partnership with one or more prospective users.		
~~The testing in real world conditions under this Article may occur in the course of the participation in a AI regulatory sandbox under the conditions specified in Article 53(1a). In such a case, supervision and guidance by the national competent authorities or, where applicable, the European Data Protection Supervisor, may~~		

PUBLIC

~~**be extended to the testing in real world conditions.**~~		
3. The testing of high-risk AI systems in real world conditions under this Article shall be without prejudice to ethical review that may be required by national or Union law.		
4. Providers or prospective providers may conduct the testing in real world conditions only where all of the following conditions are met:		
(a) the provider or prospective provider has drawn up a real-world testing plan and submitted it to the market surveillance authority in the Member State(s) where the testing in real world conditions is to be conducted or the European Data Protection Supervisor, as applicable;		

PUBLIC

(b) the market surveillance authority in the Member State(s) where the testing in real world conditions is to be conducted or to the European Data Protection Supervisor, as applicable, have not objected to the testing within 30 days after its submission;		**Do you have information or experiences from similar cases on how much time it takes the authority to check such submissions?**
(c) the provider or prospective provider has registered the testing in real world conditions in the EU database referred to in Article 60(6) with a Union-wide unique single identification number and the information specified in Annex VIIIa;		
(d) the provider or prospective provider conducting the testing in real world conditions is established in the Union or it has appointed a legal representative for the purpose of the testing in real world conditions who is established in the Union;		

PUBLIC

(e) data collected and processed for the purpose of the testing in real world conditions shall not be transferred to countries outside the Union, unless the transfer and the processing provides equivalent safeguards to those provided under Union law;	**(e) without prejudice to Chapter V of the GDPR and Chapter V of the EU-DPR,** data collected […]"	"equivalent safeguards" are too vague.
(f) the testing in real world conditions does not last longer than necessary to achieve its objectives and in any case not longer than 12 months;		
~~**(g) the testing in real world conditions does not involves persons belonging to vulnerable groups due to their age, physical or mental disability, only when such testing does not exploit any of those vulnerabilities unless that testing is essential with respect to those vulnerable groups insofar as data of comparable validity cannot be obtained**~~		

PUBLIC

~~**through testing in real conditions on other persons or by other methods**~~**; persons belonging to vulnerable groups due to their age, physical or mental disability are appropriately protected;**		
~~(h) the testing in real world conditions is designed to involve as little inconvenience as possible for the subjects of that testing; such possible inconvenience shall be specifically anticipated and defined by the provider or prospective provider in the real-world testing plan, monitored and possibly mitigated in the course of the testing;~~		
(i) where a provider or prospective provider organises the testing in real world conditions in cooperation with one or more prospective users, the latter have been informed of all aspects of the testing that are relevant to their decision to participate,		

PUBLIC

~~including~~ and given the relevant instructions on how to ~~of~~ use ~~of~~ the AI system referred to in Article 13; the provider or prospective provider and the user(s) shall conclude an agreement specifying their roles and responsibilities with a view to ensuring compliance with the provisions for testing in real world conditions under this Regulation and other applicable Union and Member States legislation;		
(j) the subjects of the testing in real world conditions have given informed consent in accordance with Article 64b;	**(j) the subjects of the testing in real world conditions have given informed consent in accordance with Article ~~6~~54b;**	Is the personal data of the persons actively participating in the testing in real world conditions to be collected on the legal basis of consent after Art. 7 GDPR? This should be clarified in this article or in a recital, especially with regard to the relationship to the GDPR. In addition to "informed consent", is consent according to Art. 6 (1) lit a, 7 DSGVO also required when personal data is used in testing

PUBLIC

		high-risk AI systems in the real world?.
(k) the testing in real world conditions is effectively overseen by the provider or prospective provider and user(s) with persons who are suitably qualified in the relevant field and have the necessary capacity, training and authority to perform their tasks;		
(l) the predictions, recommendations or decisions of the AI system can be effectively reversed or disregarded.		
5. Any subject of the testing in real world conditions, or his or her legally designated representative, as appropriate, may, without any resulting detriment and without having to provide any justification, withdraw from the testing at any time by revoking his or her informed consent. The withdrawal of the		We kindly ask for further information regarding the relationship of this para. to the GDPR. We suggest that the possibility to revoke the informed consent will be included directly in the definition in Art. 3 (51).

PUBLIC

informed consent shall not affect the activities already carried out and the use of data obtained based on the informed consent before its withdrawal.		
6. Any serious incident ~~or malfunctioning~~ identified in the course of the testing in real world conditions shall be reported to the national market surveillance authority in accordance with Article 62 of this Regulation. The provider or prospective provider shall adopt immediate mitigation measures or, failing that, suspend the testing in real world conditions until such mitigation takes place or otherwise terminate it. The provider or prospective provider shall establish a procedure for the prompt recall of the AI system upon such termination of the testing in real world conditions.		
7. Providers or prospective providers shall		

PUBLIC

notify the national market surveillance authority in the Member State(s) where the testing in real world conditions is to be conducted or the European Data Protection Supervisor, as applicable, of the suspension or termination of the testing in real world conditions and the final outcomes.		
8. The provider and prospective provider shall be liable under applicable Union and Member States liability legislation for any damage caused to the subjects by reason of their participation in the testing in real world conditions.		
Article 54b		
Informed consent to participate in testing in real world conditions outside AI regulatory sandboxes		If Art. 54b should not be understood as a consent given under the GDPR, we wonder under which legal basis data processing under real world conditions would take place. Could

PUBLIC

		you provide further information on the relationship between Art. 54b and the GDPR Depending on the requested clarification, we suggest including an explicit clarification in this article or in a recital that "informed consent" in the meaning of Art. 54b is not meant to be consent to the processing of personal data within the meaning of the GDPR.
1. For the purpose of testing in real world conditions under Article 54a, informed consent shall be freely given by the subject of testing prior to his or her participation in such testing and after having been duly informed with concise, clear, relevant, and understandable information regarding:		
(i) the nature and objectives of		

PUBLIC

the testing in real world conditions and the possible inconvenience that may be linked to his or her participation;		
(ii) the conditions under which the testing in real world conditions is to be conducted, including the expected duration of the subject's participation;		
(iii) the subject's rights and guarantees regarding participation, in particular his or her right to refuse to participate in and the right to withdraw from the field testing at any time without any resulting detriment and without having to provide any justification;		
(iv) the modalities for requesting the reversal or the disregard of the predictions, recommendations or decisions of the AI system;		

PUBLIC

(v) the Union-wide unique single identification number of the testing in real world conditions in accordance with Article 54a(c) and the contact details of the provider or its legal representative from whom further information can be obtained.		
2. The informed consent shall be dated and documented and a copy shall be given to the subject or his or her legal representative.		
Article 55 ***Support m~~M~~easures for operators, in particular SMEs, including start-ups*** *~~small-scale providers and users~~*		
1. Member States shall undertake the following actions:		
(a) provide ~~small-scale~~ SME**s** ~~providers~~**,**		

PUBLIC

including ~~and~~ start-ups**,** with priority access to the AI regulatory sandboxes to the extent that they fulfil the eligibility ~~conditions~~ **and selection criteria**;		
(b) organise specific awareness raising **and training** activities about the application of this Regulation tailored to the needs of the ~~small-scale~~ **SMEs** ~~providers and users~~**, including start-ups**;	(b) organise specific awareness raising **and training** activities about the application of this Regulation tailored to the needs of the ~~small-scale~~ **SMEs** ~~providers and users~~**, including start-ups**; Where possible, the goal should be to use existing structures for awareness rising an training activities.	We welcome the suggestions of the Presidency to support SMEs. Awareness rising and training activities are important instruments to support SMEs. Simultaneously and where possible, the goal should be to use existing structures and known contact points for SME in order to avoid the establishment of parallel structures and new contact points and to the minimize search effort for SMEs. Are the MS going to get support at organising training activities?
(c) where appropriate, establish a dedicated channel for communication with ~~small-scale~~ **SMEs** ~~providers and user~~**, including start-ups,**	(c) ~~where appropriate~~, establish a dedicated channel for communication with ~~small-scale~~ **SMEs** ~~providers and user~~**, including start-ups,**	Delete *"where appropriate"* and add *"and provide assistance for participation in AI regulatory sandboxes"*: Numerous companies,

PUBLIC

~~and other innovators~~ to provide ~~guidance~~ **advice** and respond to queries about the implementation of this Regulation.	~~and other innovators~~ to provide ~~guidance~~ **advice** and respond to queries about the implementation of this Regulation, and provide assistance for participation in AI regulatory sandboxes.	especially startups, have told us about the need for a contact point. Especially for the access to the novel instrument of the regulatory sandbox, low-threshold and practice-oriented information offers are necessary.
2. The specific interests and needs of the ~~small-scale~~ **SME** providers**, including start-ups,** shall be taken into account when setting the fees for conformity assessment under Article 43, reducing those fees proportionately to their size**,** ~~and~~ market size **and other relevant indicators**.	The specific interests and needs of the ~~small-scale~~ **SME** providers**, including start-ups,** shall be taken into account when setting the fees for conformity assessment under Article 43, reducing those fees proportionately to their size**,** ~~and~~ and market size. Member states can apply **other relevant indicators**.	We welcome that fees should be reduced for smaller companies. Which other indicators should be considered here? The MS should be free to set the indicators.
3. The Commission shall undertake the following actions:		
(a) **upon request of the AI Board, provide standardised ~~documents~~ templates for the areas covered by this Regulation;**		

PUBLIC

(b) **develop and maintain a single information platform providing easy to use information in relation to this Regulation for all operators across the Union;**		
(c) **organise appropriate communication campaigns to raise awareness about the obligations arising from this Regulation;**		
(d) **evaluate and promote the convergence of best practices in public procurement procedures in relation to AI systems.**		
Article 55a	~~***Article 55a***~~	
Derogations for specific operators	~~***Derogations for specific operators***~~	
1. The obligations laid down in Article 17 of this Regulation shall not apply to microenterprises as defined in Article 2(3) of Commission Recommendation 2003/361/EC	~~**The obligations laid down in Article 17 of this Regulation shall not apply to microenterprises as defined in Article 2(3) of Commission Recommendation 2003/361/EC**~~	The derogation for micro entreprises raises the question, how these providers should ensure the quality of their AI-applications. The risks posed by an AI system are not related to the size of its

PUBLIC

concerning the definition of micro, small and medium-sized enterprises.	~~**concerning the definition of micro, small and medium-sized enterprises.**~~	provider, so a sound quality management should remain necessary even for micro enterprises. Furthermore, it would be helpful, to know how many micro enterprises are affected.
2. Paragraph 1 shall not be interpreted as exempting those operators from fulfilling any other requirements and obligations laid down in this Regulation, including those established in Articles 9, 61 and 62.		
3. Requirements and obligations for general purpose AI systems laid down in Article 4b shall not apply to micro, small and medium-sized enterprises.		
TITLE VI		
GOVERNANCE		

PUBLIC

CHAPTER 1		
EUROPEAN ARTIFICIAL INTELLIGENCE BOARD		
		WE CONTINUE TO SUGGEST AN ORIENTATIONAL DEBATE REGARDING THE AI BOARD. THIS DEBATE SHOULD INCLUDE THE GENERAL ALIGNEMENT OF THE BOARD AND THE SCOPE, ITS MEMEBERS AND POSSIBLE RULES OF PROCEDURE. WE WOULD LIKE TO RESERVE THE OPPORTUNITY TO MAKE FURTHER COMMENTS AFTER THAT PROPOSED DEBATE.
Article 56 *Establishment **and structure** of the European Artificial Intelligence Board*		
1. A 'European Artificial Intelligence Board' (the 'Board') is established.		
~~2. The Board shall provide advice and~~		

PUBLIC

~~assistance to the Commission in order to:~~		
~~(a) contribute to the effective cooperation of the national supervisory authorities and the Commission with regard to matters covered by this Regulation;~~		
~~(b) coordinate and contribute to guidance and analysis by the Commission and the national supervisory authorities and other competent authorities on emerging issues across the internal market with regard to matters covered by this Regulation;~~		
~~(c) assist the national supervisory authorities and the Commission in ensuring the consistent application of this Regulation.~~		
~~*Article 57*~~ ~~*Structure of the Board*~~		

PUBLIC

~~1~~**2**. The Board shall be composed of **one representative per Member State** ~~the national supervisory authorities, who shall be represented by the head or equivalent high-level official of that authority,~~ ~~**and of eight independent experts representing SMEs and start-ups, large enterprises, academia and civil society, in equal proportions of 2 members per category.**~~ ~~and~~ ~~t~~**T**he European Data Protection Supervisor **shall participate as an observer**. **The Commission shall also attend the Board's meetings without taking part in the votes.**	and of eight independent experts representing SMEs and start ups, large enterprises, academia and civil society in equal proportions of 2 members per category The European Data Protection Supervisor and the European Supervisory Authorities	To ensure consistency with comprehensive financial market legislation it is essential to include the European Supervisory Authorities in the AI Board Eight independent experts representing SMEs and start-ups, large enterprises, academia and civil society, in equal proportions of 2 members per category should be again included in the AI Act. The Board shall give advice and assistance to the COM. The Board itself is not deciding. Because of the advisory nature of the board, it is important to get as many expert views on the topic of AI. To fully incorporate the views of experts in the recommendations for the COM, the experts need to be represented on the board and not in a second advisory body to the advisory board.
Other national **and Union** authorities**, bodies or**		

PUBLIC

experts may be invited to the meetings **by the Board on a case by case basis**, where the issues discussed are of relevance for them.		
2a. Each representative shall be designated by their Member State for a period of 3 years, renewable once. ~~The eight independent experts referred to paragraph 2 shall be selected by the Member States national representatives in a fair and transparent selection process established in the Board's rules of procedure, for a period of 3 years, renewable once.~~	**2a. Each representative shall be designated by their Member State for a period of 3 years, renewable once. The eight independent experts referred to paragraph 2 shall be selected by the Member States national representatives in a fair and transparent selection process established in the Board's rules of procedure, for a period of 3 years, renewable once.**	
2aa. Member States shall ensure that their representatives in the Board:		We would like to emphasize the importance of the EU Gender Equality Strategy. We therefore suggest working towards gender parity in the composition of the AI Board.
(i) have the relevant competences and powers in their Member State so as to		

PUBLIC

contribute actively to the achievement of the board's tasks referred to in Article 58;		
(ii) are designated as a single contact point vis-à-vis the Board and, where appropriate, taking into account Member States' needs, as a single contact point for stakeholders;		
(iii) are empowered to facilitate consistency and coordination between national competent authorities in their Member State as regards the implementation of this Regulation, including through the collection of relevant data and information for the purpose of fulfilling their tasks on the Board.		
~~2~~**3**. The ~~Board~~ **designated representatives of the Member States** shall adopt ~~its~~ **the Board's** rules of procedure by a ~~simple~~ **two-thirds**		

PUBLIC

majority ~~of its members, following the consent of the Commission~~. ~~The rules of procedure shall also contain the operational aspects related to the execution of the Board's tasks as listed in Article 58.~~		
The rules of procedure shall, in particular, lay down procedures for ~~the selection process for the eight independent experts referred to in paragraph 1, as well as~~ the selection process, duration of mandate and specifications of the tasks of the Chair, the voting modalities, and the organisation of the Board's activities.		
The Board shall establish a standing subgroup serving as a platform for stakeholders to advise the Board on all issues related to the implementation of this Regulation, including on the preparation of implementing and delegated acts. To this		We do support the inclusion of stakeholders in the tasks of the AI board. However, we miss provisions on the specific role of this subgroup and its tasks in the current proposal. We therefore would welcome a more formal approach regarding the advisory role of this

PUBLIC

purpose, organisations representing the interests of the providers and users of AI systems, including SMEs and start-ups, as well as civil society organisations, representatives of affected persons, researchers, standardisation organisations, notified bodies, laboratories and testing and experimentation facilities shall be invited to participate to this sub-group.		subgroup.
The Board may establish **other standing or temporary** sub-groups as appropriate for the purpose of examining specific ~~questions~~ **issues**. **Where appropriate, ~~organisations representing the interests of the providers and users of AI systems, including SMEs and start-ups, as well as civil society organisations, representatives of affected persons, researchers, standardisation organisations, notified bodies, laboratories and testing and experimentation facilities~~**		

PUBLIC

stakeholders referred to in the previous subparagraph may be invited to such sub-groups in the capacity of observers.		
3a. The Board shall be organised and operated so as to safeguard the objectivity and impartiality of its activities.		
~~3~~**4**. The Board shall be chaired by **one of the representatives of the Member States.** ~~the Commission~~. **Upon request of the Chair,** ~~T~~the Commission shall convene the meetings and prepare the agenda in accordance with the tasks of the Board pursuant to this Regulation and ~~with~~ its rules of procedure. The Commission shall provide administrative and analytical support for the activities of the Board pursuant to this Regulation.		
~~4~~**5**. ~~The Board may invite external experts and observers to attend its meetings and may hold~~		

PUBLIC

~~exchanges with interested third parties to inform its activities to an appropriate extent. To that end the Commission may facilitate exchanges between the Board and other Union bodies, offices, agencies and advisory groups.~~		
Article 58 *Tasks of the Board*		
~~When providing advice and assistance to the Commission in the context of Article 56(2),~~ **The Board shall advice and assist the Commission and the Member States in order to facilitate the consistent and effective application of this Regulation. For this purpose** the Board **may** ~~shall~~ in particular:		
(a) collect and share **technical and regulatory** expertise and best practices among Member States;		

PUBLIC

(b) contribute to ~~uniform~~ **the harmonisation of** administrative practices in the Member States, including **in relation to** ~~for~~ **the derogation from the conformity assessment procedures referred to in Article 47,** the functioning of regulatory sandboxes and **testing in real world conditions** referred to in Article 53**, 54 and 54a**;		
(c) **upon the request of the Commission or on its own initiative,** issue ~~opinions, recommendations or~~ written **opinions** ~~contributions~~ **on any relevant** matters related to the implementation of this Regulation **and to its consistent and effective application**, **including:** ~~in particular~~		
(i) on technical specifications or existing standards regarding the requirements set out in Title III, Chapter 2,		

PUBLIC

(ii) on the use of harmonised standards or common specifications referred to in Articles 40 and 41,		
(iii) on the preparation of guidance documents, including the guidelines concerning the setting of administrative fines referred to in Article 71.**;**		
(d) ~~issue an advisory opinion on the need for amendment of Annex I and Annex III, including in light of available evidence.~~ advise the Commission on the potential need for amendment of Annexes I and III in accordance with Articles 4 and 7, taking into account relevant available evidence and the latest develoments in technology		
(e) advise the Commission during the preparation of delegated or implementing act pursuant to this Regulation;		

PUBLIC

f) cooperate, as appropriate, with relevant EU bodies, experts groups and networks in particular in the fields of product safety, cybersecurity, competition, digital and media services, financial services, cryptocurrencies, consumer protection, data and fundamental rights protection;		
g) contribute and provide relevant advice to the Commission in the development of the guidance referred to in Article 58a or request the development of such guidance;		
(h) to assist the work of market surveillance authorities and, in cooperation and subject to agreement of the concerned market surveillance authorities, promote and support cross-border market surveillance investigations;		
(i) contribute to the assessment of training		

PUBLIC

needs for staff of Member States involved in implementing this Regulation;		
(j) advise the Commission in relation to international matters on artificial intelligence.		
	Where the tasks concern high-risk AI systems covered by Annex II Section A, the Board shall be preceded by a consultation with the relevant expert group established under a legal act listed in Annex II Section A.	Expert groups established under a legal act listed in Annex II should be consulted as soon as possible, e. g. the Medical Device Coordination Group (MDCG) under Regulation (EU) 2017/745.
CHAPTER 1A		
GUIDELINES FROM THE COMMISSION		
Article 58a ***Guidelines from the Commission on the implementation of this Regulation***		
1. Upon the request of the Member States		

PUBLIC

or the Board, or on its own initiative, the Commission shall issue guidelines on the practical implementation of this Regulation, and in particular on		
(i) the application of the requirements referred to in Articles 8 - 15;		
(ii) the prohibited practices referred to in Article 5;		
(iii) the practical implementation of the provisions related to substantial modification;		
(iv) the practical implementation of uniform conditions referred to in Article 6, paragraph 3, including examples ~~identification and application of criteria and~~ in relation to ~~use cases related~~ high risk AI systems referred to in Annex III;		

PUBLIC

(v) the practical implementation of transparency obligations laid down in Article 52;		
(vi) the relationship of this Regulation with other relevant Union legislation.		
When issuing such guidelines, the Commission shall pay particular attention to the needs of SMEs including start-ups and sectors most likely to be affected by this Regulation.	~~including start-ups~~	The explicit reference to start-ups is not necessary when SMEs are mentioned. It contradicts the general principles that have been applied e.g. to financial market regulation to date (same business, same risk, same rule). The reference to "start-ups" should therefore also be deleted elsewhere in the AI Regulation.
CHAPTER 2		
NATIONAL COMPETENT AUTHORITIES		

PUBLIC

Article 59 *Designation of national competent authorities*		
~~1. National competent authorities shall be established or designated by each Member State for the purpose of ensuring the application and implementation of this Regulation. National competent authorities shall be organised so as to safeguard the objectivity and impartiality of their activities and tasks.~~		
2. Each Member State shall **establish or** designate ~~a national supervisory authority~~**, and at least one notifying authority and at least one market surveillance authority for the purpose of this Regulation as** ~~among the~~ national competent authorities. **These national competent authorities shall be organised so as to safeguard the priniciples of objectivity and impartiality of their activities and tasks.**		If the "national supervisory authority" would act as notifying authority and market surveillance authority **at the same time**, the independency is not guaranteed because they are part of the same authority. To prevent conflicting interests we propose to establish a "national AI board" instead of a "national supervisory authority". The "national

PUBLIC

Provided that those prinicples are respected, such activities and tasks may be performed by one or several designated authorities, in accordance with the organisational needs of the Member State. ~~The national supervisory authority shall act as notifying authority and market surveillance authority unless a Member State has organisational and administrative reasons to designate more than one authority.~~		AI board" would consists of the national competent authority, notifying authority, market surveillance authority, which are all independent from each other. **This change is necessary to ensure the independency of the different authorities in each Member State.**
3. Member States shall inform the Commission of their designation or designations ~~and, where applicable, the reasons for designating more than one authority~~.		
4. Member States shall ensure that national competent authorities are provided with adequate financial **resources, technical equipment and well qualified** ~~and~~ human resources to **effectively** fulfil their tasks under this Regulation. ~~In particular, national~~		

PUBLIC

~~competent authorities shall have a sufficient number of personnel permanently available whose competences and expertise shall include an in-depth understanding of artificial intelligence technologies, data and data computing, fundamental rights, health and safety risks and knowledge of existing standards and legal requirements.~~		
5. **By *[one year after entry into force of this Regulation]* and afterwards six months before the deadline referred to in Article 84(2)** Member States shall ~~report to~~ **inform** the Commission ~~on an annual basis~~ on the status of the financial **resources, technical equipment and** ~~and~~ human resources of the national competent authorities with an assessment of their adequacy. The Commission shall transmit that information to the Board for discussion and possible recommendations.		

PUBLIC

6. The Commission shall facilitate the exchange of experience between national competent authorities.		
7. National competent authorities may provide ~~guidance and~~ advice on the implementation of this Regulation, including **tailored** to ~~small-scale~~ **SME** providers. Whenever national competent authorities intend to provide guidance and advice with regard to an AI system in areas covered by other Union legislation, the competent national authorities under that Union legislation shall be consulted, as appropriate. Member States may also establish one central contact point for communication with operators.	7. National ~~competent authorities~~ AI board (…)	Editorial adjustment necessary due to the proposed change of Art. 59 (2).
8. When Union institutions, agencies and bodies fall within the scope of this Regulation, the European Data Protection Supervisor shall act as the competent authority for their		

PUBLIC

supervision.		
TITLE VII		
EU DATABASE FOR ~~STAND-ALONE~~ HIGH-RISK AI SYSTEMS LISTED IN ANNEX III		
Article 60 *EU database for ~~stand-alone~~ high-risk AI systems* ***listed in Annex III***		There is a fear that the disclosure of all the law enforcement agencies' AI applications in operation or development will facilitate the assessment of an overall picture of the operational capabilities of the respective agencies. This database could potentially be used to identify capability gaps or to create thematic profiles of individual countries. This in itself could pose a security risk and affect the capabilities of the authorities. Do the Commission or other Member States share this view? Please also refer to the separate position

PUBLIC

		paper handed in, proposing necessary diverging regulations for public administration (especially LEAs and migration autoritiess) „[TITLE]“.
1. The Commission shall, in collaboration with the Member States, set up and maintain a EU database containing information referred to in paragraph 2 concerning high-risk AI systems **listed in Annex III** ~~referred to in Article 6(2)~~ which are registered in accordance with Article**s** 51 **and 54a**.	The Commission shall, in collaboration with the Member States, set up, ~~and~~ maintain and manage a EU database to enable the public to be adequately informed about high-risk AI systems placed on the market and containing information referred to in paragraph 2 concerning high-risk AI systems listed in Annex III which are registered in accordance with Article 51 and 54a.	Clarification and addition of the scope of the database.
	(new) The Commission, in collaboration with the Member States, shall set up the functional and non-functional requirements of the EU database. (new) The Commission, in collaboration with the Member States, shall draw up annaul	Clarification of the development process. determining needed material and human resources. Given their nature as advanced miliatry capacities, AI systems developed or used for

PUBLIC

	activity plans and allocate a sufficient number of material and competent human resources in order to carry activities taking into account the requirements set out in this Article.	purposes of the defence sector or the armed forces should be fully outside the public domain. They also should be controled by the Member States military authorities only since Member States are the sole owners of military capabilities in accordance with Union law (cf. Article 42(3) TEU).
2. The data listed in Annex VIII shall be entered into the EU database by the providers, **or where applicable by the authorised representative, in accordance with Article 51. The data listed in Annex VIIIa shall be entered into the database by the prospective providers or providers in accordance with Article 54a**. ~~The Commission shall provide them with technical and administrative support.~~	The data listed in Annex VIII points 1 to 5 and 8 to 12 shall be entered into the EU database by the providers, or where applicable by the authorised representative, in accordance with Article 51. The data listed in Annex VIII point 6 and 7 shall be entered into the EU database by the notified body. The Commission shall provide them with technical and administrative support. The data listed in Annex VIIIa shall be entered into the database by the prospective providers or	Amendment to clarify, that the list of data mentioned in Annex VIIII is exhaustive. Furthermore, we examine whether obligation to register should also be upon users of AI systems, rather than just on providers. Can Commission clarify the reasons why it has chosen to address only the provider and not the user? Data referred to notified bodies shall be entered by the notified body.

PUBLIC

	providers in accordance with Article 54a. **The EU database shall contain personal data only insofar as necessary for collecting and processing information in accordance with this Regulation.** The Commission shall provide them with technical and administrative support.	
3. ~~Information contained in the EU database shall be accessible to the public~~.		
4. The EU database shall contain **no** personal data**, except for the information listed in Annex VIII** ~~only insofar as necessary for collecting and processing information in accordance with this Regulation. That information shall include the names and contact details of natural persons who are responsible for registering the system and have the legal authority to represent the provider~~.	Deletion	See amendment in para 2.

PUBLIC

5. The Commission shall be the controller of the EU database. It shall ~~also~~ ~~**ensure**~~ **make available** to providers **and prospective providers** adequate technical and administrative support.	The Commission shall be the controller and the operator of the EU database. It shall make available to providers ~~and~~, prospective providers and users adequate technical and administrative support.	Clarification.
5a. Information contained in the EU database registered in accordance with Article 51 shall be accessible to the public. The information registered in accordance with Article 54a shall be accessible only to market surveillance authorites and the Commission, unless the prospective provider or provider has given consent for making this information also accessible the public.		
	Article 60a *EU database for stand-alone AI systems used by public authorities* 1. The Commission shall, in collaboration with the Member States, set up, maintain and manage	Due to the unique role and responsibility public authorities bear, the sensitive personal data they have access to, the consequentional effects their decisions have on individuals, and thus their primary obligation to respect, protect and fulfil fundamental rights, public authorities should be

PUBLIC

	a EU database to enable the public to be adequately informed about AI systems placed on the market and containing information referred to in paragraph 2 concerning AI systems used by the public authorities registered in accordance with Article 51 (2). 2. The data listed in Annex VIIIb shall be entered into the EU database by the public authorities. The Commission shall provide them with technical and administrative support. 3. Art. 60 par. 3-5a shall apply accordingly.	subject to more stringent transparency requirements when using AI systems. Hence, any deployments of AI systems – regardless of their level of risk – by or on behalf of public authorities should be registrered within a separate EU database in addition to the registration as High Risk AI in the database referred to in Article 60. We refrain from drafting up an Annex VIIIb for this comment. However, the data base should include the name of the AI system and a short description of its intended purpose as well as the name, address and contact details of the public authority by whom or on whose behalf it is used. However, in the field of law enforcement, the possible security risk arising from the database must also be considered. Please also refer to the comment above (no. 130) and the separate position paper handed in, proposing

PUBLIC

		necessary diverging regulations for public administration (especially LEAs and migration authorities) „[TITLE]“. We are also still discussing this topic under aspects such as operating expenses, especially how to avoid exceeding operating expenses.
TITLE VIII		
POST-MARKET MONITORING, INFORMATION SHARING, MARKET SURVEILLANCE		
CHAPTER 1		
POST-MARKET MONITORING		

PUBLIC

Article 61 *Post-market monitoring by providers and post-market monitoring plan for high-risk AI systems*		
1. Providers shall establish and document a post-market monitoring system in a manner that is proportionate to ~~the nature of the artificial intelligence technologies and~~ the risks of the high-risk AI system.	Providers shall plan, establish, ~~and~~ document, implement, maintain and update a post market monitoring system in a manner that is proportionate to the risks of the high-risk AI system. That system shall be an integral part of the provider's quality management system referred to in Article 17(1).	Clarification.
2. **In order to allow the provider to evaluate the compliance of AI systems with the requirements set out in Title III, Chapter 2 throughout their life cycle,** ~~T~~the post-market monitoring system shall ~~actively and systematically~~ collect, document and analyse relevant data**, which may be** provided by users or **which may be** collected through other sources on the performance of high-risk AI	In order to allow the provider to evaluate the compliance of AI systems with the requirements set out in Title III, Chapter 2 throughout their life cycle, the post-market monitoring system shall be suited to actively and systematically collect, document and analyse relevant data on the quality, performance, safety and security which may be provided by users or which may be collected through other sources on the	Clarification. There is concern that the mere disclosure of all law enforcement agencies' AI applications in operation or development will facilitate an assessment of an overall picture of the relevant agencies' operational capabilities. Should an exception be included in Articles 61, which

PUBLIC

systems**.** ~~throughout their life time and allow the provider to evaluate the continuous compliance of AI systems with the requirements set out in Title III, Chapter 2.~~	performance.	would allow the Member State concerned, under conditions to be defined in more detail, to refrain from publication in individual cases if and to the extent that confidentiality interests conflict with this? DEU security authorities are in favor of this.
3. The post-market monitoring system shall be based on a post-market monitoring plan. The post-market monitoring plan shall be part of the technical documentation referred to in Annex IV. The Commission shall adopt an implementing act laying down detailed provisions establishing a template for the post-market monitoring plan and the list of elements to be included in the plan.		
4. For high-risk AI systems covered by the legal acts referred to in Annex II, where a post-market monitoring system and plan is already established under that legislation, ~~the elements~~	For high-risk AI systems covered by the legal acts referred to in Annex II, where a post-market monitoring system and plan is already established under that legislation, ~~the elements~~	The post-market monitoring documentation covered by legal acts referred to in Annex II should take into account the information of the template referred to para 3.

PUBLIC

~~described in paragraphs 1, 2 and 3 shall be integrated into that system and plan as appropriate~~ **the post-market monitoring documentation as prepared under that legislation shall be deemed sufficient, provided that the template referred to paragraph 3 is used**.	~~described in paragraphs 1, 2 and 3 shall be integrated into that system and plan as appropriate~~ **the post-market monitoring documentation as prepared under that legislation shall be deemed sufficient, provided that the template referred to paragraph 3 is taken into account~~used~~**.	
The first subparagraph shall also apply to high-risk AI systems referred to in point 5(b) of Annex III placed on the market or put into service by credit institutions regulated by Directive 2013/36/EU.		Please specify in which specific existing plan credit institutions should include the elements described in paragraph 1 to 3. Moreover, similar procedures exist for entities regulated by Directive 2009/183/EC, Directive (EU) 2016/2341, Directive 2014/65/EU resp. Directive (EU) 2015/2366, Directive 2009/65/EG and Directive 2011/61/EU which should be referended here. It remains unclear whether the AI Act poses additional requirements for entities already regulated by comprehensive financial sector

PUBLIC

		regulation. Please specify how the AI Act does avoid double regulation for the highly regulated financial sector.
CHAPTER 2		
SHARING OF INFORMATION ON SERIOUS INCIDENTS ~~AND MALFUNCTIONING~~		
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~~		If a serious incident according to Art. 3 para 44 AIA entails a personal data breach, providers of high-risk AI systems are obliged to report the incident to both the market surveillance authorities as well as to data protection supervisory authorities. We suggest to add a clarifying sentence and added a draft paragraph

PUBLIC

occurred.		8 in in Art. 2 but would be open to move it to another location. Corresponding Recital XY: This Regulation is without prejudice to Regulation (EU) 2016/679 and Directive 2002/58/EC of the European Parliament and of the Council and therefore should in particular not affect the tasks and powers of the independent supervisory authorities competent to monitor compliance with the respective Union data protection law.
Such notification shall be made immediately after the provider has established a causal link between the AI system and the **serious** 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~~.		Why is the deadline set to max. 15 days? The analogue deadline in GDRP is max. 72 hours?

PUBLIC

2. Upon receiving a notification related to a **serious incident referred to in Article 3(44)(c)** ~~a breach of obligations under Union law intended to protect fundamental rights~~, the **relevant** market surveillance authority shall inform the national public authorities or bodies referred to in Article 64(3). The Commission shall develop dedicated guidance to facilitate compliance with the obligations set out in paragraph 1. That guidance shall be issued 12 months after the entry into force of this Regulation, at the latest.		
3. For high-risk AI systems referred to in point 5~~(b)~~ of Annex III which are placed on the market or put into service by providers that are ~~credit~~ **financial** institutions **that are subject to requirements regarding their internal governance, arrangements or processes under Union financial services legislation** ~~regulated by Directive 2013/36/EU and for~~	~~For high-risk AI systems referred to in point 5(b) and 5 (d) of Annex III which are placed on the market or put into service by providers that are credit institutions regulated by Directive 2013/36/EU and entities regulated by Directive 2009/138/EC, Directive (EU) 2016/2341, Directive 2014/65/EU, Directive (EU) 2015/2366, Directive 2009/65/EG resp.~~	Moved exception of medical devices to a new paragraph It remains unclear whether the AI Act poses additional requirements for entities already regulated by comprehensive financial sector regulation. Please specify how the AI Act does avoid double regulation for the highly regulated

PUBLIC

~~high-risk AI systems which are safety components of devices, or are themselves devices, covered by Regulation (EU) 2017/745 and Regulation (EU) 2017/746~~, the notification of serious incidents ~~or malfunctioning~~ shall be limited to those **referred to in Article 3(44)(c)**~~that that constitute a breach of obligations under Union law intended to protect fundamental rights~~.	~~Directive 2011/61/EU and~~ ~~for high-risk AI systems which are safety components of devices, or are themselves devices, covered by Regulation (EU) 2017/745 and Regulation (EU) 2017/746, the notification of serious incidents shall be limited to those referred to in Article 3(44)(c).~~	financial sector.
4. **For high-risk AI systems which are safety components of devices, or are themselves devices, covered by Regulation (EU) 2017/745 and Regulation (EU) 2017/746 the notification of serious incidents shall be limited to those referred to in Article 3(44)(c) and be made to the national ~~supervisory~~ competent authority chosen for this purpose by ~~of~~ the Member States where that incident occurred.**	**For high-risk AI systems which are safety components of devices, or are themselves devices, covered by Regulation (EU) 2017/745 and Regulation (EU) 2017/746 the notification of serious incidents shall be ~~limited to those referred to in Article 3(44)(c) and be~~ made to the national ~~supervisory~~ competent authority ~~chosen for this purpose by of the Member States where that incident occurred~~ under this legislation. If the serious incidents is limited to those referred to in**	In the Regulation (EU) 2017/745 and Regulation (EU) 2017/746 there are serious incidents that directly or indirectly led into death of patient, user or other persons. It is important that every notification of serious incident is reported to the competent authority for Medical Devices or IVD. If the serious incident is limited to those referred to in Article 3(44)c the national competent authority for Medical Devices or IVD forward the notification of serious incidents to the

PUBLIC

	Article 3(44)c the national competent authority referred to in the precending sentence shall be forward the notification of serious incidents to the competent authority for this purpose.	competent authority for this purpose.
	CHAPTER 2A DATA ACCESS FOR VETTED RESEARCHERS *Article 62a* *Data Access for vetted Researchers* 1 Upon a reasoned request from a public or private body to be determined by each member state, providers shall within a reasonable period, as specified in the request, provide access to	Regarding the data access for vetted researchers, in the field of law enforcement, the possible security risk arising from data access must also be considered. Therefore, there is a need for exemptions from the requests laid down in article 62a. These exemptions are still under discussion. We may provide further comments.

PUBLIC

	training, validation and test-ing datasets used by the provider to vetted researchers who meet the requirements in para-graph 2 of this article for the sole purpose of conducting research that contributes to the development, training, validation and testing of AI systems within the existing legal framework, in particular with regards to bias monitoring, detection and correction of such systems and that is related to a public interest. Access to personal data shall be provided in anonymised or at least pseudonymised form as long as this is possible without jeopardizing the research pur-pose. 2 Upon a duly substantiated application from researchers, the responsible body shall award them the status of vetted researchers and issue data access re-quests pursuant to paragraph 1, where the researchers demonstrate that they	

PUBLIC

	meet all of the following conditions: (a) researchers shall be affiliated to a research organisation as defined in Article 2 (1) of Di-rective (EU) 2019/790 of the European Parliament and of the Council (c) the application submitted by the researchers justifies the necessity and proportionality for the purpose of their research of the data requested and the timeframes within which they re-quest access to the data, and they demonstrate the contribution of the expected research results to the purposes laid down in paragraph 1, () the planned research activities will be carried out only for the purposes laid down in para-graph 1, (f) shall commit and be in a capacity to preserve the specific data security and confidentiali-ty	

PUBLIC

	requirements corresponding to each request. In particular, a protection concept shall be provided with the request, containing a description of the research purpose, the intended use of the information, measures taken to protect the interests of the data subject and tech-nical and organisational measures taken to protect personal data. 3 The provider may refuse the requested information, if trade secrets are affected and the public interest in the research does not outweigh the interest in confidentiality. The provid-er may refuse access to personal data, if the legitimate interests of the data subject outweigh the public interest in the research. Where the data holder claims compensation for making data available, such compensation shall not exceed the technical and organisational costs incurred to comply with the request including,	

PUBLIC

	where necessary, the costs of anonymisation and of technical adaptation. 4 The public or private body that awarded the status of vetted researcher and issued the access request in favour of a vetted researcher shall issue a decision terminating the ac-cess if it determines, following an investigation either on its own initiative or on the basis in-formation received from third parties, that the vetted researcher no longer meets the condi-tions set out in paragraph 2. Before terminating the access, the body shall allow the vetted researcher to react to the findings of its investigation and its intention to terminate the access. As soon as the vetted researcher no longer meets the conditions set out in paragraph 2, the vetted researcher shall report this circumstance to the market surveil-lance authority.	

PUBLIC

CHAPTER 3		
ENFORCEMENT		
Article 63 *Market surveillance and control of AI systems in the Union market*		
1. Regulation (EU) 2019/1020 shall apply to AI systems covered by this Regulation. However, for the purpose of the effective enforcement of this Regulation:		Our understanding is that the Regulation 2017/745 and 2017/746 are lex specialis and provide more specific provisions for market surveillance and control of AI systems so that the Regulation 2019/1020 are not apply to AI systems, covered by Regulation 2017/745 and 2017/746.
(a) any reference to an economic operator under Regulation (EU) 2019/1020 shall be understood as including all operators identified		

PUBLIC

in ~~Title III, Chapter 3~~ **Article 2** of this Regulation;		
(b) any reference to a product under Regulation (EU) 2019/1020 shall be understood as including all AI systems falling within the scope of this Regulation.		
2. **As part of their reporting obligations under Article 25(6) of Regulation (EU) 2019/1020, the Member States** ~~national supervisory authority~~ shall report to the Commission ~~on a regular basis~~ **about** the outcomes of relevant market surveillance activities **under this Regulation**. ~~The national supervisory authority shall report, without delay, to the Commission and relevant national competition authorities any information identified in the course of market surveillance activities that may be of potential interest for the application of Union law on competition rules.~~	2. The national AI board ~~supervisory~~ authority shall report to the Commission on a regular basis the outcomes of relevant market surveillance activities. The national ~~supervisory authority~~ AI board shall report, without delay, to the Commission and relevant national competition authorities any information identified in the course of market surveillance activities that may be of potential.	Clarification. Legal acts listed in Annex II already established reports to the COM. Editorial adjustment necessary due to the proposed change of Art. 59 (2).

PUBLIC

3. For high-risk AI systems, related to products to which legal acts listed in Annex II, section A apply, the market surveillance authority for the purposes of this Regulation shall be the authority responsible for market surveillance activities designated under those legal acts **or, in justified circumstances and provided that coordination is ensured, another relevant authority identified by the Member State.**		
The procedures referred to in Articles 65, 66, 67 and 68 of this Regulation shall not apply to AI systems related to products, to which legal acts listed in Annex II, section A apply, when such legal acts already provide for procedures having the same objective. In such a case, these sectoral procedures shall apply instead.		

PUBLIC

4. For **high-risk** AI systems placed on the market, put into service or used by financial institutions regulated by Union legislation on financial services, the market surveillance authority for the purposes of this Regulation shall be the relevant **national** authority responsible for the financial supervision of those institutions under that legislation~~.~~ **in so far as the placement on the market, putting into service or the use of the AI system is in direct connection with the provision of those financial services. When the placement on the market, putting into service or the use of the AI system is not in direct connection with the provision of financial services, or in justified circumstances and provided that coordination is ensured, another relevant authority may be identified by the Member State. National market surveillance authorities supervising regulated credit institutions shall report, without delay, to the**		

PUBLIC

European Central Bank any information identified in the course of their market surveillance activities that may be of potential interest for the European Central Bank's prudential supervisory tasks as specified in Council Regulation (EU) No 1204/2013 establishing the Single Supervisory Mechanism (SSM).		
5. For **high-risk** AI systems listed in point 1(a) in so far as the systems are used for law enforcement purposes, points 6~~,~~ ~~and~~ 7 and 8 of Annex III, Member States shall designate as market surveillance authorities for the purposes of this Regulation either **the national authorities supervising the activities of the law enforcement, immigration or asylum authorities** ~~systems~~, or the competent data protection supervisory authorities under Directive (EU) 2016/680, or Regulation 2016/679 ~~or the national competent authorities~~	points 6 and~~,~~ ~~and~~ 7 ~~**and 8**~~ of Annex III	Oversight of AI used in the judiciary should rest with state judicial administrations, not with the "national authority supervising the activities of the law enforcement, immigration or asylum authorities". Clearer separation of immigration and asylum authorities from law enforcement authorities is

PUBLIC

~~supervising the activities of the law enforcement, immigration or asylum authorities putting into service or using those systems~~.	**the national authorities supervising the activities of the law enforcement authorities, immigration or asylum authorities**	imperative, as different purposes are pursued.
	5a. For AI systems developed or used for purposes of the defence sector or the armed forces Member States shall designate a military authority to perform the functions assigned to market surveillance authorities under this Regulation.	
6. Where Union institutions, agencies and bodies fall within the scope of this Regulation, the European Data Protection Supervisor shall act as their market surveillance authority.		

PUBLIC

	6a. Paragraph 6 shall not apply to the European Union Military Committee, the European Union Military Staff, the Military Planning and Conduct Capability within the European External Action Service, the European Defence Agency, and any missions or operations established in the framework of the Common Security and Defence Policy.	The military uses of AI systems as well as related activities of the institutions, agencies and bodies is not suited for surveillance by the European Data Protection Supervisor.
7. Member States shall facilitate the coordination between market surveillance authorities designated under this Regulation and other relevant national authorities or bodies which supervise the application of Union harmonisation legislation listed in Annex II or other Union legislation that might be relevant for the high-risk AI systems referred to in Annex III.		
8. Without prejudice to powers provided under Regulation (EU) 2019/1020, and where relevant and limited to what is necessary to		

PUBLIC

fulfil their tasks, the market surveillance authorities shall be granted full access by the provider to the documentation as well as the training, validation and testing datasets used for the development of the high-risk AI system, including, where appropriate and subject to security safeguards, through application programming interfaces ('API') or other relevant technical means and tools enabling remote access.		
9. Market surveillance authorities shall be granted access to the source code of the high-risk AI system upon a reasoned request and only when the following cumulative conditions are fulfilled:		
a) Access to source code is necessary to assess the conformity of a high-risk AI system with the requirements set out in Title III, Chapter 2, and		

PUBLIC

b) testing/auditing procedures and verifications based on the data and documentation provided by the provider have been exhausted or proved insufficient.		
Article 63a		
Supervision of testing in real world conditions by market surveillance authorities		
1. Market surveillance authorities shall have the competence and powers to ensure that testing in real world conditions is in accordance with this Regulation.		
2. Where testing in real world conditions is conducted for AI systems that are supervised within an AI regulatory sandbox under Article 54, the market surveillance authorities or the European Data protection		

PUBLIC

Supervisor, as appropriate, shall verify the compliance with the provisions of Article 54a as part of their supervisory role for the AI regulatory sandbox. Those authorities may, as appropriate, allow the testing in real world conditions to be conducted by the provider or prospective provider in derogation to the conditions set out in Article 54a(4) (f) and (g).		
3. Where a market surveillance authority has been informed by the prospective provider, the provider or any third party of a serious incident or has other grounds for considering that the conditions set out in Articles 54a and 54b are not met, it may take any of the following decisions on its territory, as appropriate:		
(a) suspend or terminate the testing in real world conditions;		

PUBLIC

(b) require the provider or prospective provider and user(s) to modify any aspect of the testing in real world conditions.		
4. Where a market surveillance authority has taken a decision referred to in paragraph 3 of this Article or has issued an objection within the meaning of Article 54a(4)(b), the decision or the objection shall indicate the grounds thereof and the modalities and conditions for the provider or prospective provider to challenge the decision or objection.		
5. Where applicable, where a market surveillance authority has taken a decision referred to in paragraph 3 of this Article, it shall communicate the grounds therefor to the market surveillance authorities of the other Member States in which the AI system has been tested in accordance with the testing		

PUBLIC

plan.		
Article 64 ***Powers of authorities protecting fundamental rights*** ~~*Access to data and documentation*~~		
~~1. Access to data and documentation in the context of their activities, the market surveillance authorities shall be granted full access to the training, validation and testing datasets used by the provider, including through application programming interfaces ('API') or other appropriate technical means and tools enabling remote access.~~		
~~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.~~		

PUBLIC

3. National public authorities or bodies which supervise or enforce the respect of obligations under Union law protecting fundamental rights in relation to the use of high-risk AI systems referred to in Annex III shall have the power to request and access any documentation created or maintained under this Regulation when access to that documentation is necessary for the fulfilment of the competences under their mandate within the limits of their jurisdiction. The relevant public authority or body shall inform the market surveillance authority of the Member State concerned of any such request.	3. National public authorities or bodies which supervise or enforce the respect of obligations under Union law protecting fundamental rights, including the right to non-discrimination, in relation to the use of high-risk AI systems referred to in Annex III, shall have the power to request and access any documentation created or maintained under this Regulation when access to that documentation is necessary for the fulfilment of the competences under their mandate within the limits of their jurisdiction. The relevant public authority or body shall inform the market surveillance authority of the Member State concerned of any such request.	In the field of law enforcement, there is an ongoing discussion, how confidentiality requirements for LEAs can be met in regards to this provision. Please also refer to the separate position paper handed in, proposing necessary diverging regulations for public administration (especially LEAs and migration autorities) „[TITLE]“.
4. By 3 months after the entering into force of this Regulation, each Member State shall identify the public authorities or bodies referred to in paragraph 3 and make ~~a~~ **the** list publicly available ~~on the website of the national~~	4. By 3 months after the entering into force of this Regulation, each Member State shall identify the public authorities or bodies referred to in paragraph 3 and make a list publicly available on the website of the ~~national~~	Editorial adjustment necessary due to the proposed change of Art. 59(2).

PUBLIC

~~supervisory authority~~. Member States shall notify the list to the Commission and all other Member States and keep the list up to date.	~~supervisory authority~~AI board. Member States shall notify the list to the Commission and all other Member States and keep the list up to date.	
5. Where the documentation referred to in paragraph 3 is insufficient to ascertain whether a breach of obligations under Union law intended to protect fundamental rights has occurred, the public authority or body referred to paragraph 3 may make a reasoned request to the market surveillance authority to organise testing of the high-risk AI system through technical means. The market surveillance authority shall organise the testing with the close involvement of the requesting public authority or body within reasonable time following the request.	5. Where the documentation referred to in paragraph 3 is insufficient to ascertain whether a breach of obligations under Union law intended to protect fundamental rights, including the right to non-discrimination, has occurred, the public authority or body referred to paragraph 3 may make a reasoned request to the market surveillance authority to organise testing of the high-risk AI system through technical means. The market surveillance authority shall organise the testing with the close involvement of the requesting public authority or body within reasonable time following the request.	
6. Any information and documentation obtained by the national public authorities or		Regarding the confidentiality obligations set out in Article 70 we refer to the separate position

PUBLIC

bodies referred to in paragraph 3 pursuant to the provisions of this Article shall be treated in compliance with the confidentiality obligations set out in Article 70.		paper handed in, proposing necessary diverging regulations for public administration (especially LEAs and migration autorities) „[TITLE]“.
Article 65 *Procedure for dealing with AI systems presenting a risk at national level*		
	(new*)* For high-risk AI systems which are safety components of devices, or are themselves devices, covered by Regulation (EU) 2017/745 and Regulation (EU) 2017/746, shall apply procedures for dealing with risks under those legal acts.	Dealing with serious incidents and other incidents (field safety corrective action, other non compliance) are more specifically regulated in the Regulations 2017/745 and 2017/746 (e. g. vigilance system).
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.	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 or to environmental protection are concerned.	Following the definition in Article 3, point 19 of Regulation (EU) 2019/1020 we propose not to exclude environmental aspects of product-related risks. This would benefit a strong “Sustainable AI – Made in Europe” brand as previously endorsed by DEU.

PUBLIC

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 **identified** ~~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		

PUBLIC

shall without **undue** 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~~, **within a period** ~~as~~ it may prescribe.		
The market surveillance authority shall inform the relevant notified body accordingly. Article 18 of Regulation (EU) 2019/1020 shall apply to the measures referred to in the second subparagraph.		
3. Where the market surveillance authority considers that non-compliance is not restricted to its national territory, it shall inform the Commission and the other Member States **without undue delay** of the results of the evaluation and of the actions which it has required the operator to take.		

PUBLIC

4. The operator shall ensure that all appropriate corrective action is taken in respect of all the AI systems concerned that it has made available on the market throughout the Union.		
5. Where the operator of an AI system does not take adequate corrective action within the period referred to in paragraph 2, the market surveillance authority shall take all appropriate provisional measures to prohibit or restrict the AI system's being made available on its national market, to withdraw the product from that market or to recall it. That authority shall ~~inform~~ **notify** the Commission and the other Member States, without **undue** delay, of those measures.		
6. The ~~information~~ **notification** referred to in paragraph 5 shall include all available details, in particular the ~~data~~ **information** necessary for the identification of the non-compliant AI		

PUBLIC

system, the origin of the AI system, the nature of the non-compliance alleged and the risk involved, the nature and duration of the national measures taken and the arguments put forward by the relevant operator. In particular, the market surveillance authorities shall indicate whether the non-compliance is due to one or more of the following:		
(-a) non-compliance with the prohibition of the artificial intelligence practices referred to in Article 5;		
(a) a failure of **a high-risk** AI system to meet requirements set out in Title III, Chapter 2;	a failure of **a high-risk** AI system to meet requirements set out in ~~Title III, Chapter 2~~ this Regulation;	Taking into account other requirements, e. g. quality management system, post-market-surveillance system, etc..
(b) shortcomings in the harmonised standards or common specifications referred to in Articles 40 and 41 conferring a presumption of conformity.		

PUBLIC

(c) non-compliance with provisions set out in Article 52;		
(d) non-compliance of general purpose AI systems with the requirements and obligations referred to in Article 4a;		
7. The market surveillance authorities of the Member States other than the market surveillance authority of the Member State initiating the procedure shall without **undue** delay inform the Commission and the other Member States of any measures adopted and of any additional information at their disposal relating to the non-compliance of the AI system concerned, and, in the event of disagreement with the notified national measure, of their objections.		
8. Where, within three months of receipt of		

PUBLIC

the ~~information~~ **notification** referred to in paragraph 5, no objection has been raised by either a Member State or the Commission in respect of a provisional measure taken by a Member State, that measure shall be deemed justified. This is without prejudice to the procedural rights of the concerned operator in accordance with Article 18 of Regulation (EU) 2019/1020. **The period referred to in the first sentence of this paragraph shall be reduced to 30 days in the case of non-compliance with the prohibition of the artificial intelligence practices referred to in Article 5.**		
9. The market surveillance authorities of all Member States shall **then** ensure that appropriate restrictive measures are taken in respect of the ~~product~~ **AI system** concerned, such as withdrawal of the product from their market, without **undue** delay.		

PUBLIC

Article 66 *Union safeguard procedure*		
1. Where, within three months of receipt of the notification referred to in Article 65(5), **or 30 days in the case of non-compliance with the prohibition of the artificial intelligence practices referred to in Article 5,** objections are raised by a Member State against a measure taken by another Member State, or where the Commission considers the measure to be contrary to Union law, the Commission shall without **undue** delay enter into consultation with the relevant Member State**'s market surveillance authority** and operator or operators and shall evaluate the national measure. On the basis of the results of that evaluation, the Commission shall decide whether the national measure is justified or not within 9 months, **or 60 days in the case of non-compliance with the prohibition of the**		

PUBLIC

artificial intelligence practices referred to in Article 5, **starting** from the notification referred to in Article 65(5). **It shall** and notify such decision to the Member State concerned. **The Commission shall also inform all other Member States of such decision.**		
2. If the ~~national~~ **measure taken by the relevant Member State's market surveillance authority** is considered justified **by the Commission, the market surveillance authorities of** all Member States **shall ensure that appropriate restrictive measures are taken in respect of the AI system concerned, such as withdrawal of the AI system from their market without undue delay,** ~~shall take the measures necessary to ensure that the non-compliant AI system is withdrawn from their market,~~ and shall inform the Commission accordingly. If the national measure is considered unjustified **by the Commission, the**		

PUBLIC

market surveillance authority of the Member State concerned shall withdraw the measure **and inform the Commission accordingly**.		
3. Where the national measure is considered justified and the non-compliance of the AI system is attributed to shortcomings in the harmonised standards or common specifications referred to in Articles 40 and 41 of this Regulation, the Commission shall apply the procedure provided for in Article 11 of Regulation (EU) No 1025/2012.		
Article 67 *Compliant **high-risk or general purpose** AI systems which present a risk*		
1. Where, having performed an evaluation under Article 65, the market surveillance authority of a Member State finds that although ~~an~~ **high-risk or general purpose** AI system is	Where, having performed an evaluation under Article 65, the market surveillance authority of a Member State finds that although an AI system is in compliance with this Regulation, it presents	The definition of a relevant risk should extend to environmental risks, as described regarding Article 65 (1).

PUBLIC

in compliance with this Regulation, it presents a risk to the health or safety of persons~~,~~ **or** to ~~the compliance with obligations under Union or national law intended to protect~~ fundamental rights ~~or to other aspects of public interest protection~~, it shall require the relevant operator to take all appropriate measures to ensure that the AI system concerned, when placed on the market or put into service, no longer presents that risk, to withdraw the AI system from the market or to recall it **without undue delay** ~~within a reasonable period, commensurate with the nature of the risk~~, **within a period** it may prescribe.	a risk to the health or safety of persons **or to fundamental rights or** to the environment (…)	Given the large differences across the Union in terms of geographies, infrastructures, landscapes, climatic conditions and many other factors influencing the functioning of an AI system, it is possible that systems developed and proven compliant in one location represents a risk in a different context.
2. The provider or other relevant operators shall ensure that corrective action is taken in respect of all the AI systems concerned that they have made available on the market throughout the Union within the timeline prescribed by the market surveillance authority of the Member		

PUBLIC

State referred to in paragraph 1.		
3. The Member State shall immediately inform the Commission and the other Member States. That information shall include all available details, in particular the data necessary for the identification of the AI system concerned, the origin and the supply chain of the AI system, the nature of the risk involved and the nature and duration of the national measures taken.		
4. The Commission shall without **undue** delay enter into consultation with the Member States **concerned** and the relevant operator and shall evaluate the national measures taken. On the basis of the results of that evaluation, the Commission shall decide whether the measure is justified or not and, where necessary, propose appropriate measures.		

PUBLIC

5. The Commission shall address its decision to the Member States **concerned, and inform all other Member States**.		
Article 68 *Formal non-compliance*		
1. Where the market surveillance authority of a Member State makes one of the following findings, it shall require the relevant provider to put an end to the non-compliance concerned, **within a period it may prescribe**:	Where, having performed an evaluation under Article 65, the market surveillance authority of a Member State makes one of the following findings, it shall require the relevant provider to put an end to the non-compliance concerned, within a period it may prescribe:	Clarification.
(a) the conformity marking has been affixed in violation of Article 49;		
(b) the conformity marking has not been affixed;		
(c) the EU declaration of conformity has not		

PUBLIC

been drawn up;		
(d) the EU declaration of conformity has not been drawn up correctly;		
(e) the identification number of the notified body, which is involved in the conformity assessment procedure, where applicable, has not been affixed;		
2. Where the non-compliance referred to in paragraph 1 persists, the Member State concerned shall take all appropriate measures to restrict or prohibit the high-risk AI system being made available on the market or ensure that it is recalled or withdrawn from the market.		
Article 68a ***Union testing facilities in the area of artificial intelligence***		

PUBLIC

1. The Commission shall designate one or more Union testing facilities pursuant to Article 21 of Regulation (EU) 1020/2019 in the area of artificial intelligence.		
2. Without prejudice to the activities of Union testing facilities referred to in Article 21(6) of Regulation (EU) 1020/2019, Union testing facilities referred to in paragraph 1 shall also provide independent technical or scientific advice at the request of the Board or market surveillance authorities.		
Article 68b ***Central pool of independent experts***		
1. The Commission may, by means of an implementing act, make provisions on the creation, maintenance and financing of a central pool of independent experts to support the enforcement activities under this		

PUBLIC

Regulation.		
2. Experts shall be selected by the Commission and included in the central pool on the basis of up-to-date scientific or technical expertise in the field of artificial intelligence, having due regard to the technical areas covered by the requirements and obligations in this Regulation and the activities of market surveillance authorities pursuant to Article 11 of Regulation (EU) 1020/2019. The Commission shall determine the number of experts in the pool in accordance with the required needs.		
3. Experts may have the following tasks:		
(a) provide advice to and support the work of market surveillance authorities, at their request;		

PUBLIC

(b) support cross-border market surveillance investigations as referred to in Article 58(h);		
(c) advise and support the Commission when carrying out its duties in the context of the safeguard clause pursuant to Article 66.		
4. The experts shall perform their tasks with impartiality, objectivity and ensure the confidentiality of information and data obtained in carrying out their tasks and activities. Each expert shall draw up a declaration of interests, which shall be made publicly available. The Commission shall establish systems and procedures to actively manage and prevent potential conflicts of interest.		
5. The Member States may be required to pay fees for the advice and support by the		

PUBLIC

experts. The structure and the level of fees as well as the scale and structure of recoverable costs shall be adopted by the Commission by means of the implementing act referred to in paragraph 1, taking into account the objectives of the adequate implementation of this Regulation, cost-effectiveness and the necessity to ensure an effective access to experts by all Member States.		
6. The Commission shall facilitate timely access to the experts by the Member States, as needed, and ensure that the combination of support activities carried out by Union testing facilities pursuant to Article 70 and experts pursuant to this Article is efficently organised and provides the best possible added value.		

PUBLIC

TITLE IX		
CODES OF CONDUCT		
Article 69 *Codes of conduct* ***for voluntary application of specific requirements***		
1. The Commission, and the Member States shall ~~encourage and~~ facilitate the drawing up of codes of conduct intended to ~~foster~~ **encourage** the voluntary application to AI systems other than high-risk AI systems **of one or more of** the requirements set out in Title III, Chapter 2 **of this Regulation to the best extent possible**, **taking into account the available, technical solutions allowing for the application of such requirements.** ~~on the basis of technical specifications and solutions that are appropriate means of ensuring compliance with such~~	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 of **this Regulation** on the basis of harmonised standards or common ~~technical~~ specifications and solutions that are appropriate means of ensuring compliance with such requirements in light of the intended purpose of the systems.	Taking into account other requirements, e. g. quality management system, post-market-surveillance system, etc. Not “specifications” should be used, but the existing harmonised standards or common specifications

PUBLIC

~~requirements in light of the intended purpose of the systems.~~		
2. The Commission and the ~~Board~~ **Member States** shall ~~encourage and~~ facilitate the drawing up of codes of conduct intended to **encourage** ~~foster~~ the voluntary application to **all** AI systems of **specific** requirements related**,** for example**,** to environmental sustainability, accessibility for persons with a disability, stakeholders participation in the design and development of the AI systems and diversity of development teams on the basis of clear objectives and key performance indicators to measure the achievement of those objectives. **The Commission and the Member States shall also facilitate, where appropriate, the drawing of codes of conduct applicable on a voluntary basis with regard to users' obligations in relation to AI systems.**	(…) to **all** AI systems of **specific** requirements related for example to **security by design and security by default, explainability by design,** environmental sustainability, e.g. energy-efficient programming, accessibility for persons with a disability, stakeholders participation in the design and development of the AI systems and diversity of development teams on the basis of clear objectives and key performance indicators to measure the achievement of those objectives.(…)	Clarification. Codes of conduct should set requirements for AI systems for ecological sustainability and thus contribute to a strong brand "Sustainable AI - Made in Europe". A strong signal should be sent to make the opportunities of sustainable AI systems, e.g. for the environment and climate, even more visible as a competitive advantage. The term ‘environmental sustainability’ encompasses a broad range of aspects, such as environmental impact assessments, life cycle analysis, or reusability and recyclability of hardware. The proposed addition ‘energy-

PUBLIC

		efficient programming' not only gives a precise example of an environmental concern, it also supports the broader call for a more energy-efficient AI development, e.g. expressed in debates on 'Green AI' complementing 'Red AI', that would allow for more inclusivity and diversity in the corporate AI landscape as the high costs for computing power keep small actors out of the market. Security relevant aspects should be considered by default
		At this point we underline that accessibility for persons with disabilities shouldn´t be a voluntary requirement but an obligation. We refer to the Convention of the United Nations on the rights of persons with disabilities ratified by the EU.

PUBLIC

3. Codes of conduct **applicable on a voluntary basis** may be drawn up by individual providers of AI systems or by organisations representing them or by both, including with the involvement of users and any interested stakeholders and their representative organisations, **or, where appropriate, by users with regard to their obligations**. Codes of conduct may cover one or more AI systems taking into account the similarity of the intended purpose of the relevant systems.		
4. The Commission and the Board shall take into account the specific interests and needs of ~~the small-scale~~ **SME** providers, including ~~and~~ start-ups**,** when encouraging and facilitating the drawing up of codes of conduct **referred to in this Article**.		
TITLE X		

PUBLIC

CONFIDENTIALITY AND PENALTIES		
Article 70 *Confidentiality*		In DEU, there is discussion on whether further requirements on secrecy and the guarantee of confidentiality and data protection are necessary. For example, Art. 70(2) of the AI Regulation provides only few concrete requirements for confidentiality and only for the case that authorities from the law enforcement sector are themselves developers or providers of AI applications. We refer to the separate position paper handed in, proposing necessary diverging regulations for public administration (especially LEAs and migration authorities) [TITLE].
1. National competent authorities**,** ~~and~~ notified bodies**, the Commission, the Board,**		

PUBLIC

and any other natural or legal person involved in the application of this Regulation shall**, in accordance with Union or national law, put appropriate technical and organisational measures in place to ensure** ~~respect~~ the confidentiality of information and data obtained in carrying out their tasks and activities in such a manner as to protect, in particular:		
(a) intellectual property rights, and confidential business information or trade secrets of a natural or legal person, including source code, except the cases referred to in Article 5 of Directive 2016/943 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure apply.		
(b) the effective implementation of this Regulation, in particular for the purpose of		

PUBLIC

inspections, investigations or audits;		
(c) public and national security interests;		
~~(c)~~ **(d)** integrity of criminal or administrative proceedings.		
	(e) the integrity of information classified in accordance with Member States' respective laws as well EU classified information.	
2. Without prejudice to paragraph 1, information exchanged on a confidential basis between the national competent authorities and between national competent authorities and the Commission shall not be disclosed without the prior consultation of the originating national competent authority and the user when high-risk AI systems referred to in points 1, 6 and 7 of Annex III are used by law enforcement, immigration or asylum authorities, when such	shall not be disclosed without the prior ~~consultation~~ **approval (…)** used by law enforcement authorities, immigration or asylum authorities	Consultation is not sufficient Clearer separation of immigration and asylum authorities from law enforcement authorities is imperative, as different purposes are pursued. More detailed explanation required: What is meant by the phrase "when such disclosure

PUBLIC

disclosure would jeopardise public and national security interests.		would jeopardize public and national security interests"? What requirements/obstacles must be met/overcome for this?
When the law enforcement, immigration or asylum authorities are providers of high-risk AI systems referred to in points 1, 6 and 7 of Annex III, the technical documentation referred to in Annex IV shall remain within the premises of those authorities. Those authorities shall ensure that the market surveillance authorities referred to in Article 63(5) and (6), as applicable, can, upon request, immediately access the documentation or obtain a copy thereof. Only staff of the market surveillance authority holding the appropriate level of security clearance shall be allowed to access that documentation or any copy thereof.	shall not be disclosed without the prior ~~consultation~~ **approval (…)** law enforcement authorities, immigration or asylum authorities	Consultation is not sufficient Clearer separation of immigration and asylum authorities from law enforcement authorities is imperative, as different purposes are pursued.

PUBLIC

3. Paragraphs 1 and 2 shall not affect the rights and obligations of the Commission, Member States and notified bodies with regard to the exchange of information and the dissemination of warnings, nor the obligations of the parties concerned to provide information under criminal law of the Member States.		What is meant by the term "information under criminal law of the Member States"? If and to the extent that immigration and asylum authorities are affected by this, it must be explained in more detail which data records are forwarded to which authorities and for what purposes.
Article 71 *Penalties*		Art. 71 stipulates administrative fines in case of violations of the provisions of the regulation. According to Art. 25 (2) (a) and (b) and 27 (5), representatives, importers and distributors are obliged to provide certain information to the authorities. This raises the question regarding compliance with the nemo tenetur principle. What is the Commission’s assessment? Should a right to withhold information be added in the legal text or should Member States at least be explicitly allowed to introduce a right to

PUBLIC

		withhold information in their national laws?
1. In compliance with the terms and conditions laid down in this Regulation, Member States shall lay down the rules on penalties, including administrative fines, applicable to infringements of this Regulation and shall take all measures necessary to ensure that they are properly and effectively implemented. The penalties provided for shall be effective, proportionate, and dissuasive. They shall take into particular account the **size and** interests of ~~small-scale~~ **SME** providers**,** **including** ~~and~~ start-up**s,** and their economic viability.		
2. The Member States shall **without delay** notify the Commission of those rules and of those measures and ~~shall notify it, without delay,~~ of any subsequent amendment affecting them.		

PUBLIC

3. ~~The following infringements~~ **Non-compliance with any of the prohibitions of the artificial intelligence practices referred to in Article 5** shall be subject to administrative fines of up to 30 000 000 EUR or, if the offender is company, up to 6 % of its total worldwide annual turnover for the preceding financial year, ~~whichever is higher~~ **whichever is higher.** ~~**and**~~ **In case of SMEs, including** ~~**and**~~ **start-ups, these fines shall be up to 3% of their** ~~**its**~~ **worldwide annual turnover for the preceding financial year**~~**, whichever is higher.**~~**:**		
~~(a) non-compliance with the prohibition of the artificial intelligence practices referred to in Article 5;~~		
~~(b) non-compliance of the AI system with the requirements laid down in Article 10.~~		

PUBLIC

4. The non-compliance of the AI system with any requirements or obligations under this Regulation **on operators or notified bodies**, other than those laid down in Article~~s~~ 5 ~~and 10~~, shall be subject to administrative fines of up to 20 000 000 EUR or, if the offender is a company, up to 4 % of its total worldwide annual turnover for the preceding financial year, ~~whichever is higher~~ **whichever is higher. ~~and~~ In case of SMEs, ~~and~~ including start-ups, these fines shall be up to 2% ~~3%~~ of their ~~its~~ worldwide annual turnover for the preceding financial year~~, whichever is higher~~**.		
5. The supply of incorrect, incomplete or misleading information to notified bodies and national competent authorities in reply to a request shall be subject to administrative fines of up to 10 000 000 EUR or, if the offender is a company, up to 2 % of its total worldwide		

PUBLIC

annual turnover for the preceding financial year, ~~whichever is higher~~ **whichever is higher. ~~and~~ In case of SMEs, ~~and~~ including start-ups, these fines shall be up to 1% ~~3%~~ of their ~~its~~ worldwide annual turnover for the preceding financial year~~, whichever is higher~~.**		
6. When deciding on the amount of the administrative fine in each individual case, all relevant circumstances of the specific situation shall be taken into account and due regard shall be given to the following:		
(a) the nature, gravity and duration of the infringement and of its consequences;		
(b) whether administrative fines have been already applied by other market surveillance authorities **in other Member States** to the same operator for the same infringement.		

PUBLIC

(c) the size**, the annual turnover** and market share of the operator committing the infringement;		
7. Each Member State shall lay down rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State.		
8. Depending on the legal system of the Member States, the rules on administrative fines may be applied in such a manner that the fines are imposed by competent national courts ~~of~~ **or** other bodies as applicable in those Member States. The application of such rules in those Member States shall have an equivalent effect.		
9. The exercise by the market surveillance authority of its powers under this Article shall be subject to appropriate procedural safeguards in accordance with Union and		

PUBLIC

Member State law, including effective judicial remedy and due process.		
Article 72 *Administrative fines on Union institutions, agencies and bodies*		
1. The European Data Protection Supervisor may impose administrative fines on Union institutions, agencies and bodies falling within the scope of this Regulation. When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case, all relevant circumstances of the specific situation shall be taken into account and due regard shall be given to the following:		
(a) the nature, gravity and duration of the infringement and of its consequences;		

PUBLIC

(b) the cooperation with the European Data Protection Supervisor in order to remedy the infringement and mitigate the possible adverse effects of the infringement, including compliance with any of the measures previously ordered by the European Data Protection Supervisor against the Union institution or agency or body concerned with regard to the same subject matter;		
(c) any similar previous infringements by the Union institution, agency or body;		
2. ~~The following infringements~~ **Non-compliance with any of the prohibitions of the artificial intelligence practices referred to in Article 5** shall be subject to administrative fines of up to 500 000 EUR~~.:~~		
~~(a) non-compliance with the prohibition of the artificial intelligence practices referred to in~~		

PUBLIC

~~Article 5;~~		
~~(b) non-compliance of the AI system with the requirements laid down in Article 10.~~		
3. The non-compliance of the AI system with any requirements or obligations under this Regulation, other than those laid down in Articles 5 and 10, shall be subject to administrative fines of up to 250 000 EUR.		
4. Before taking decisions pursuant to this Article, the European Data Protection Supervisor shall give the Union institution, agency or body which is the subject of the proceedings conducted by the European Data Protection Supervisor the opportunity of being heard on the matter regarding the possible infringement. The European Data Protection Supervisor shall base his or her decisions only on elements and circumstances on which the		

PUBLIC

parties concerned have been able to comment. Complainants, if any, shall be associated closely with the proceedings.		
5. The rights of defense of the parties concerned shall be fully respected in the proceedings. They shall be entitled to have access to the European Data Protection Supervisor's file, subject to the legitimate interest of individuals or undertakings in the protection of their personal data or business secrets.		
6. Funds collected by imposition of fines in this Article shall be the income of the general budget of the Union.		
	7. This article shall not apply to the European Union Military Committee, the European Union Military Staff, the Military Planning and Conduct Capability within the European External Action Service, the European Defence	

PUBLIC

	Agency, and any missions or operations established in the framework of the Common Security and Defence Policy.	
TITLE XI		
DELEGATION OF POWER AND COMMITTEE PROCEDURE		
Article 73 *Exercise of the delegation*		
1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.		
	"(new [NR]) Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with the principles laid down in the Interinstitutional Agreement of [13 April 2016] on Better Law-Making."	

PUBLIC

2. The delegation of power referred to in Article 4, Article 7(1), Article 11(3), Article 43(5) and (6) and Article 48(5) shall be conferred on the Commission for ~~an~~ **a** ~~indeterminate~~ period of ~~time~~ **five years** from [*entering into force of the Regulation*].	2. The delegation of power referred to in Article 4, Article 7(1) **and (3)**, Article 11(3), Article 43(5) and (6) and Article 48(5) shall be conferred on the Commission for ~~an~~ **a** ~~indeterminate~~ period of ~~time~~ **five years** from [*entering into force of the Regulation*]	If the proposed Art 7 (3) is adopted, Art. 73 should reflect this.
The Commission shall draw up a report in respect of the delegation of power not later than nine months before the end of the 5 year period. The delegation of power shall be tacitly extended for periods of an identical duration, unless the European Parliament or the Council opposes such extension not later than three months before the end of each period.		
3. The delegation of power referred to in Article 4, Article 7(1), Article 11(3), Article 43(5) and (6) and Article 48(5) may be revoked at any time by the European Parliament or by	The delegation of power referred to in Article 4, Article 7(1) **and (3),** Article 11(3), Article 43(5) and (6) and Article 48(5).	See above

PUBLIC

the Council. A decision of revocation shall put an end to the delegation of power specified in that decision. It shall take effect the day following that of its publication in the *Official Journal of the European Union* or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.		
4. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.		
5. Any delegated act adopted pursuant to Article 4, Article 7(1), Article 11(3), Article 43(5) and (6) and Article 48(5) shall enter into force only if no objection has been expressed by either the European Parliament or the Council within a period of three months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have	5. Any delegated act adopted pursuant to Article 4, Article 7(1) **and (3)**, Article 11(3), Article 43(5) and (6) and Article 48(5) shall enter into force only if no objection has been expressed by either the European Parliament or the Council within a period of ~~three~~ five months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament	See above The regulatory matters that are provided for in this regulation for delegated acts, especially regarding Art. 3 and Art. 7, are very complex,

PUBLIC

both informed the Commission that they will not object. That period shall be extended by three months at the initiative of the European Parliament or of the Council.	and the Council have both informed the Commission that they will not object. That period shall be extended by three months at the initiative of the European Parliament or of the Council.	so that a regularly longer consulting time is required to deal with a possible objection.
Article 74 *Committee procedure*		
1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.		
2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.		
TITLE XII		

PUBLIC

FINAL PROVISIONS		
Article 75 *Amendment to Regulation (EC) No 300/2008*		
In Article 4(3) of Regulation (EC) No 300/2008, the following subparagraph is added:		
"When adopting detailed measures related to technical specifications and procedures for approval and use of security equipment concerning Artificial Intelligence systems in the meaning of Regulation (EU) YYY/XX [on Artificial Intelligence] of the European Parliament and of the Council*, the requirements set out in Chapter 2, Title III of that Regulation shall be taken into account."		
_____		

PUBLIC

* Regulation (EU) YYY/XX [on Artificial Intelligence] (OJ …).”		
Article 76 *Amendment to Regulation (EU) No 167/2013*		
In Article 17(5) of Regulation (EU) No 167/2013, the following subparagraph is added:		
“When adopting delegated acts pursuant to the first subparagraph concerning artificial intelligence systems which are safety components in the meaning of Regulation (EU) YYY/XX [on Artificial Intelligence] of the European Parliament and of the Council*, the requirements set out in Title III, Chapter 2 of that Regulation shall be taken into account.		
_____		
* Regulation (EU) YYY/XX [on Artificial		

PUBLIC

Intelligence] (OJ …).”		
Article 77 *Amendment to Regulation (EU) No 168/2013*		
In Article 22(5) of Regulation (EU) No 168/2013, the following subparagraph is added:		
“When adopting delegated acts pursuant to the first subparagraph concerning Artificial Intelligence systems which are safety components in the meaning of Regulation (EU) YYY/XX on [Artificial Intelligence] of the European Parliament and of the Council*, the requirements set out in Title III, Chapter 2 of that Regulation shall be taken into account.		
_____		
* Regulation (EU) YYY/XX [on Artificial Intelligence] (OJ …).”		

PUBLIC

Article 78 *Amendment to Directive 2014/90/EU*		
In Article 8 of Directive 2014/90/EU, the following paragraph is added:		
"4. For Artificial Intelligence systems which are safety components in the meaning of Regulation (EU) YYY/XX [on Artificial Intelligence] of the European Parliament and of the Council*, when carrying out its activities pursuant to paragraph 1 and when adopting technical specifications and testing standards in accordance with paragraphs 2 and 3, the Commission shall take into account the requirements set out in Title III, Chapter 2 of that Regulation.		
_____		
* Regulation (EU) YYY/XX [on Artificial		

PUBLIC

Intelligence] (OJ …).”.		
Article 79 *Amendment to Directive (EU) 2016/797*		
In Article 5 of Directive (EU) 2016/797, the following paragraph is added:		
“12. When adopting delegated acts pursuant to paragraph 1 and implementing acts pursuant to paragraph 11 concerning Artificial Intelligence systems which are safety components in the meaning of Regulation (EU) YYY/XX [on Artificial Intelligence] of the European Parliament and of the Council*, the requirements set out in Title III, Chapter 2 of that Regulation shall be taken into account.		
_____		
* Regulation (EU) YYY/XX [on Artificial		

PUBLIC

Intelligence] (OJ …).”.		
Article 80 *Amendment to Regulation (EU) 2018/858*		
In Article 5 of Regulation (EU) 2018/858 the following paragraph is added:		
“4. When adopting delegated acts pursuant to paragraph 3 concerning Artificial Intelligence systems which are safety components in the meaning of Regulation (EU) YYY/XX [on Artificial Intelligence] of the European Parliament and of the Council *, the requirements set out in Title III, Chapter 2 of that Regulation shall be taken into account.		
_____		
* Regulation (EU) YYY/XX [on Artificial Intelligence] (OJ …).”.		

PUBLIC

Article 81 *Amendment to Regulation (EU) 2018/1139*		
Regulation (EU) 2018/1139 is amended as follows:		
(1) In Article 17, the following paragraph is added:		
"3. Without prejudice to paragraph 2, when adopting implementing acts pursuant to paragraph 1 concerning Artificial Intelligence systems which are safety components in the meaning of Regulation (EU) YYY/XX [*on Artificial Intelligence*] of the European Parliament and of the Council*, the requirements set out in Title III, Chapter 2 of that Regulation shall be taken into account.		
_____		

PUBLIC

* Regulation (EU) YYY/XX [on Artificial Intelligence] (OJ …).”		
(2) In Article 19, the following paragraph is added:		
“4. When adopting delegated acts pursuant to paragraphs 1 and 2 concerning Artificial Intelligence systems which are safety components in the meaning of Regulation (EU) YYY/XX [on Artificial Intelligence], the requirements set out in Title III, Chapter 2 of that Regulation shall be taken into account.”		
(3) In Article 43, the following paragraph is added:		
“4. When adopting implementing acts pursuant to paragraph 1 concerning Artificial Intelligence systems which are safety components in the		

PUBLIC

meaning of Regulation (EU) YYY/XX [on Artificial Intelligence], the requirements set out in Title III, Chapter 2 of that Regulation shall be taken into account."		
(4) In Article 47, the following paragraph is added:		
"3. When adopting delegated acts pursuant to paragraphs 1 and 2 concerning Artificial Intelligence systems which are safety components in the meaning of Regulation (EU) YYY/XX [on Artificial Intelligence], the requirements set out in Title III, Chapter 2 of that Regulation shall be taken into account."		
(5) In Article 57, the following paragraph is added:		
"When adopting those implementing acts concerning Artificial Intelligence systems which		

PUBLIC

are safety components in the meaning of Regulation (EU) YYY/XX [on Artificial Intelligence], the requirements set out in Title III, Chapter 2 of that Regulation shall be taken into account.”		
(6) In Article 58, the following paragraph is added:		
“3. When adopting delegated acts pursuant to paragraphs 1 and 2 concerning Artificial Intelligence systems which are safety components in the meaning of Regulation (EU) YYY/XX [on Artificial Intelligence] , the requirements set out in Title III, Chapter 2 of that Regulation shall be taken into account.”.		
Article 82 *Amendment to Regulation (EU) 2019/2144*		
In Article 11 of Regulation (EU) 2019/2144, the		

PUBLIC

following paragraph is added:		
"3. When adopting the implementing acts pursuant to paragraph 2, concerning artificial intelligence systems which are safety components in the meaning of Regulation (EU) YYY/XX [on Artificial Intelligence] of the European Parliament and of the Council*, the requirements set out in Title III, Chapter 2 of that Regulation shall be taken into account.		
	Article 82 new **Amendments to Directive 2020/1828/EC on Representative Actions for the Protection of the Collective Interests of Consumers** **3.The following is added to Annex I of the Directive 2020/1828/EC on Representative Actions for the Protection of the Collective Interests of Consumers:**	The AI Act must allow representative actions to be used to defend natural person's rights collectively. This should apply in the case of illegal commercial practices, or in obtaining compensation in case of harm suffered by a group of natural persons. Natural persons must be able via authorised organisations to jointly bring a court case to obtain compensation for damages arising from the same source (e.g. multiple consumers harmed by the same non-compliant AI system

PUBLIC

	"Regulation xxxx/xxxx of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts"	or practice). In the absence of adding the AI Act to the RAD Annex I, consumers would have no way of exercising their rights collectively.
_____		
* Regulation (EU) YYY/XX [on Artificial Intelligence] (OJ …).".		
Article 83 *AI systems already placed on the market or put into service*		DEU further suggests to exclude large-scale IT systems established by the legal acts listed in Annex IX from obligations of users of high-risk AI systems set forth in Art. 29 (in connection with Art. 12 and Art. 11) regardless of the date the systems have been placed on the market or put into service, since these systems are already regulated with regard to those obligations and the obligations laid down in the AI act may conflict with the obligation laid down in the

PUBLIC

		existing legislation. If the amendment of those legal acts leads to a significant change in the design or intended purpose of the AI system, it then should be considered as a question of legal technique if any obligations of users of high-risk AI systems under the AI Act should be implemented directly within the legal acts listed in Annex IX itself. Furthermore, the suggested exemption is without prejudice to Art. 83 (2) of the Commission's proposal, according to which the requirements laid down in this Regulation shall be taken into account, in the evaluation of each large-scale IT systems established by the legal acts listed in Annex IX to be undertaken as provided for in those respective acts. Please also refer to the separate position paper handed in, proposing necessary diverging

PUBLIC

		regulations for public administration (especially LEAs) „[TITLE]“.
1. This Regulation shall not apply to the AI systems which are components of the large-scale IT systems established by the legal acts listed in Annex IX that have been placed on the market or put into service before *[12 months after the date of application of this Regulation referred to in Article 85(2)]*, unless the replacement or amendment of those legal acts leads to a significant change in the design or intended purpose of the AI system or AI systems concerned.		
The requirements laid down in this Regulation shall be taken into account, where applicable, in the evaluation of each large-scale IT systems established by the legal acts listed in Annex IX to be undertaken as provided for in those respective acts.		

PUBLIC

2. This Regulation shall apply to the high-risk AI systems, other than the ones referred to in paragraph 1, that have been placed on the market or put into service before [*date of application of this Regulation referred to in Article 85(2)*], only if, from that date, those systems are subject to significant changes in their design or intended purpose.		
Article 84 *Evaluation and review*		
~~1. The Commission shall assess the need for amendment of the list in Annex III once a year following the entry into force of this Regulation.~~		
1a. The Commission shall assess the need for amendment of the list in Annex I every 24 months following the entry into force of this Regulation and until the end of the period of		

PUBLIC

the delegation of power. The findings of that assessment shall be presented to the European Parliament and the Council.		
1b. The Commission shall assess the need for amendment of the list in Annex III every 24 months following the entry into force of this Regulation and until the end of the period of the delegation of power. The findings of that assessment shall be presented to the European Parliament and the Council.		
2. By [*three years after the date of application of this Regulation referred to in Article 85(2)*] and every four years thereafter, the Commission shall submit a report on the evaluation and review of this Regulation to the European Parliament and to the Council. The reports shall be made public.		

PUBLIC

3. The reports referred to in paragraph 2 shall devote specific attention to the following:		
(a) the status of the financial **resources, technical equipment and** ~~and~~ human resources of the national competent authorities in order to effectively perform the tasks assigned to them under this Regulation;		
(b) the state of penalties, and notably administrative fines as referred to in Article 71(1), applied by Member States to infringements of the provisions of this Regulation.	the state of penalties, and notably administrative fines as referred to in Article 71(1), applied by Member States to infringements of the provisions of this Regulation~~.~~;	
	(new) the status of the EU database for stand-alone high-risk AI systems and planned developments; (new) the state of measures in support of	

PUBLIC

	innovation, in particular measures for SME providers; (new) the state of the code of conduct and the application to AI systems other than high-risk AI systems.	
4**.** Within [*three years after the date of application of this Regulation referred to in Article 85(2)*] and every four years thereafter**,** **where appropriate**, the Commission shall evaluate the impact and effectiveness of **voluntary** codes of conduct to foster the application of the requirements set out in Title III, Chapter 2 and possibly other additional requirements for AI systems other than high-risk AI systems.		
5. For the purpose of paragraphs 1**a** to 4 the Board, the Member States and national competent authorities shall provide the		

PUBLIC

Commission with information on its request.		
6. In carrying out the evaluations and reviews referred to in paragraphs 1**a** to 4 the Commission shall take into account the positions and findings of the Board, of the European Parliament, of the Council, and of other relevant bodies or sources.		
7. The Commission shall, if necessary, submit appropriate proposals to amend this Regulation, in particular taking into account developments in technology and in the light of the state of progress in the information society.		
Article 85 *Entry into force and application*		
1. This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the*		

PUBLIC

European Union.		
2. This Regulation shall apply from [~~24~~ **36** months following the entering into force of the Regulation].		
3. By way of derogation from paragraph 2:		
(a) Title III, Chapter 4 and Title VI shall apply from [~~three~~ **twelve** months following the entry into force of this Regulation];		
(b) Article 71 shall apply from [twelve months following the entry into force of this Regulation].		
This Regulation shall be binding in its entirety and directly applicable in all Member States.		
Done at Brussels,		

PUBLIC

For the European Parliament For the Council		
The President The President		
~~**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;~~		

PUBLIC

~~**(c)** Statistical approaches, Bayesian estimation, search and optimization methods.~~		
ANNEX II **LIST OF UNION HARMONISATION LEGISLATION** **Section A – List of Union harmonisation legislation based on the New Legislative Framework**		
1. Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC (OJ L 157, 9.6.2006, p. 24) [as repealed by the Machinery Regulation];		
2. Directive 2009/48/EC of the European Parliament and of the Council of 18 June 2009 on the safety of toys (OJ L 170, 30.6.2009, p. 1);		

PUBLIC

3. Directive 2013/53/EU of the European Parliament and of the Council of 20 November 2013 on recreational craft and personal watercraft and repealing Directive 94/25/EC (OJ L 354, 28.12.2013, p. 90);		
4. Directive 2014/33/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to lifts and safety components for lifts (OJ L 96, 29.3.2014, p. 251);		
5. Directive 2014/34/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to equipment and protective systems intended for use in potentially explosive atmospheres (OJ L 96, 29.3.2014, p. 309);		

PUBLIC

6. Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC (OJ L 153, 22.5.2014, p. 62);		
7. Directive 2014/68/EU of the European Parliament and of the Council of 15 May 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of pressure equipment (OJ L 189, 27.6.2014, p. 164);		
8. Regulation (EU) 2016/424 of the European Parliament and of the Council of 9 March 2016 on cableway installations and repealing Directive 2000/9/EC (OJ L 81, 31.3.2016, p. 1);		

PUBLIC

9. Regulation (EU) 2016/425 of the European Parliament and of the Council of 9 March 2016 on personal protective equipment and repealing Council Directive 89/686/EEC (OJ L 81, 31.3.2016, p. 51);		
10. Regulation (EU) 2016/426 of the European Parliament and of the Council of 9 March 2016 on appliances burning gaseous fuels and repealing Directive 2009/142/EC (OJ L 81, 31.3.2016, p. 99);		
11. Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (OJ L 117, 5.5.2017, p. 1;		
12. Regulation (EU) 2017/746 of the		

PUBLIC

European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU (OJ L 117, 5.5.2017, p. 176).		
(1)		
Section B. List of other Union harmonisation legislation		
1. Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002 (OJ L 97, 9.4.2008, p. 72).		
2. Regulation (EU) No 168/2013 of the European Parliament and of the Council of 15 January 2013 on the approval and market surveillance of two- or three-wheel vehicles and quadricycles (OJ L 60, 2.3.2013, p. 52);		

PUBLIC

3. Regulation (EU) No 167/2013 of the European Parliament and of the Council of 5 February 2013 on the approval and market surveillance of agricultural and forestry vehicles (OJ L 60, 2.3.2013, p. 1);		
4. Directive 2014/90/EU of the European Parliament and of the Council of 23 July 2014 on marine equipment and repealing Council Directive 96/98/EC (OJ L 257, 28.8.2014, p. 146);		
5. Directive (EU) 2016/797 of the European Parliament and of the Council of 11 May 2016 on the interoperability of the rail system within the European Union (OJ L 138, 26.5.2016, p. 44).		
6. Regulation (EU) 2018/858 of the European Parliament and of the Council of 30		

PUBLIC

May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles, amending Regulations (EC) No 715/2007 and (EC) No 595/2009 and repealing Directive 2007/46/EC (OJ L 151, 14.6.2018, p. 1);		
7. Regulation (EU) 2019/2144 of the European Parliament and of the Council of 27 November 2019 on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users, amending Regulation (EU) 2018/858 of the European Parliament and of the Council and repealing Regulations (EC) No 78/2009, (EC) No 79/2009 and (EC) No 661/2009 of the European Parliament and of the Council and Commission		

PUBLIC

Regulations (EC) No 631/2009, (EU) No 406/2010, (EU) No 672/2010, (EU) No 1003/2010, (EU) No 1005/2010, (EU) No 1008/2010, (EU) No 1009/2010, (EU) No 19/2011, (EU) No 109/2011, (EU) No 458/2011, (EU) No 65/2012, (EU) No 130/2012, (EU) No 347/2012, (EU) No 351/2012, (EU) No 1230/2012 and (EU) 2015/166 (OJ L 325, 16.12.2019, p. 1);		
8. Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the	Add the following references to Annex II B: 9. DIRECTIVE 2014/45/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 3 April 2014 on periodic roadworthiness tests for motor vehicles and their trailers and repealing Directive 2009/40/EC (OJ L 127, 29.4.2014, p. 51); 10. Commission Delegated Directive (EU) 2021/1717 of 9 July 2021 amending Directive 2014/45/EU of the European Parliament and of the Council as regards	

PUBLIC

European Parliament and of the Council and Council Regulation (EEC) No 3922/91 (OJ L 212, 22.8.2018, p. 1), in so far as the design, production and placing on the market of aircrafts referred to in points (a) and (b) of Article 2(1) thereof, where it concerns unmanned aircraft and their engines, propellers, parts and equipment to control them remotely, are concerned.	the updating of certain vehicle category designations and the addition of eCall to the list of test items, methods, reasons for failure and assessment of deficiencies in Annex I and Annex III to that Directive (OJ L 342, 27.9.2021, p. 48); 11. Commission Implementing Regulation (EU) 2019/621 of 17 April 2019 on the technical information necessary for roadworthiness testing of the items to be tested, on the use of the recommended test methods, and establishing detailed rules concerning the data format and the procedures for accessing the relevant technical information (OJ L 108, 23.4.2019, p. 5).	
ANNEX III **HIGH-RISK AI SYSTEMS REFERRED TO IN ARTICLE 6(~~2~~3)**		
In each of the areas listed under points 1-8, the AI systems specifically mentioned under		

PUBLIC

each letter are considered to be h~~H~~High-risk AI systems pursuant to Article 6(~~2~~3) ~~are the AI systems listed in any of the following areas~~:		
1. Biometric**s** ~~**systems** identification and categorisation of natural persons~~:		
(a) ~~AI systems~~ **Biometric identification systems** ~~intended to be used for the 'real-time' and 'post' remote biometric identification of natural persons~~ ~~**without their agreement**~~;		DEU reserves the right to an in-depth comment regarding biometric identification systems at a later stage, final discussions are still ongoing.
	(b) emotion recognition systems, **(c) biometric categorisation systems.**	DEU asks that biometric categorization systems and emotion recognition systems be included in Annex III no. 1, as these systems pose comparable risks to fundamental rights as biometric identification systems.
2. ~~Management and operation of c~~**C**ritical infrastructure ~~**and protection of environment**~~:	2. ~~Management and operation of c~~**C**ritical infrastructure ~~**and protection of environment**~~ and emmission intensive industries	Addition in reference to proposed high risk area 2.b)

PUBLIC

(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**;**	(a) AI systems intended to be used as safety components in the management and operation of ~~road traffic and~~ critical infrastructure used for the supply of water, gas, heating and electricity and the collection, treatment and discharge of wastewater**;**	Remove road traffic here from the list and add separate point 2 (aaa) because of other EU sector regulation to be referenced there in general terms, e.g. ITS RL. AI use in sanitation may be conceivable especially concerning wastewater disposal. Failure or malfunction of such AI may cause detrimental effects on health and hygiene on a larger scale. Hence, the functioning of wastewater disposal is essential to public health and as such to public infrastructure and should be regarded as high-risk.
(aa) AI systems intended to be used ~~to control or~~ as safety components in the management and operation of critical digital infrastructure;	**AI systems intended to be used ~~to control or~~ as safety components in the management and operation of critical digital infrastructure with the exception of process optimisation methods for complex machines and plants, virtual digital assistants, predictive mainte-**	We only consider AI systems used as safety components in the management and operation of critical digital infrastructures (such as process optimation methods for complex machines and plants, virtual digital assistants, predictive

PUBLIC

	nance, programmable logic controllers (PLCs);	maintenance, programmable logic controllers (PLCs)) to be high risk AI if their results actually lead directly - i.e. without human validation - to implementation (i.e. autonomously operating systems) or where the results are the only basis for the relevant action or decision to be taken by a human. Therefore, process optimisation methods for complex machines and plants, virtual digital assistants, predictive maintenance, programmable logic controllers (PLCs) should not fall under 2 (aa). It is our understanding that AI systems which do not pose a significant risk to the health, safe-ty or fundamental rights are not considered high risk. We ask the COM to integrate a recital that clear-ly states which systems are considered critical (digital) infrastructures and to give concrete examples.
	(aaa) AI systems intended to be used as	Road traffic is highly regulated, e.g. ITS

PUBLIC

	safety components in the management and operation of critical infrastructure used for road traffic if not regulated in sector-specific acts. (aaaa) AI systems intended to be used in the management and operation of public warning systems as well as AI systems intended to be used as safety components in the management and operation of technical systems for the protection against extreme weather events such as floods and droughts.	directive incl. delegated acts and road safety regulation. Those more specific acts (existing and new ones) should prevail. It is also our understanding that AI systems which do not pose a significant risk to the health, safety or fundamental rights are not considered high risk. Public warning systems may, for instance, alert the population based on AI-steered predictions about cases of extreme weather such as floods. With a view to possible, large-scale ramifications especially to human health as well as property, such stand-alone systems should be regarded as posing a high risk. The failure or malfunction of safety components in protection systems against extreme weather systems may also result in serious harms. Such systems could encompass e.g. systems for the opening/closing of locks or of transport networks adjacent to water in cases of floods or reservoirs and

PUBLIC

		barrage dams in cases of droughts.
(b) ~~**AI systems intended to be used to control emissions and pollution**~~.	(b) AI systems intended to be used to control industrial activities of energy industries or processing of metals, mineral industry, chemical industry and waste management referred to in the Industrial Emission Directive (IED) 2010/75/EU	AI systems deployed to control activities of emmission intensive industries, which affect the release of the substantial amounts of emmissions and pollution pose significant risks of harm to the environment, therefore infringing the fundamental right to a high level of environmental protection and resulting in immediate or mediate risks to health and safety.In particular technical errors of AI systems which are used to monitor and control operational processes in industrial plants may lead to malfunctions resulting in major environmental damage, such as the release of toxic substances.
3. Education and vocational training:		In the view of DEU it is necessary to sharpen the wording of the use case.

PUBLIC

		For example, what is meant by "educational training institutions"? Does this include both privat and public institutions? What exactly is meant by "institution"?
(a) AI systems intended to be used for the purpose of determining access**, admission** or assigning natural persons to educational and vocational training institutions **or programmes at all levels**;		
(b) AI systems intended to be used for ~~the purpose of~~ **the purpose of assessing** ~~assessing students~~ **natural persons** ~~in~~ **with the view to evaluating learning outcomes or steering the learning process in educational and vocational training institutions or programmes at all levels** ~~educational and vocational training institutions and for assessing~~		What constitutes a "steering learning process"? For instance, does this include mobile applications for learning languages? What are "programmes" in this context?

PUBLIC

~~participants in tests commonly required for admission to educational institutions~~.		
4. Employment, workers management and access to self-employment:		
(a) AI systems intended to be used for recruitment or selection of natural persons, notably for advertising vacancies, screening or filtering applications, evaluating candidates ~~in the course of interviews or tests~~;		
(b) AI intended to be used for making decisions on promotion and termination of work-related contractual relationships, for task allocation **based on individual behavior or personal traits or characteristics** and for monitoring and evaluating performance and behavior of persons in such relationships.	AI intended to be used for making decisions on promotion and termination of work-related contractual relationships, for task allocation that is **based on individual behavior, or personal traits or characteristics** or potentially affects a natural person's health, safety, fundamental rights or legitmate interests and for monitoring and evaluating performance and behavior of persons in such relationships.	The addition of "task allocation based on individual behavior or personal traits or characteristics" limits the scope of this use case too much. If only task allocation based on individual traits of a single person is regulated, essentially only discriminatory cases are likely to be covered. However, AI systems for task allocation can also pose other dangers. For example, decisions of AI systems used in

PUBLIC

		warehouses or by transportation platforms can be based on (from a worker's perspective) external factors like customer needs, the type of goods to be transported, traffic, weather or efficiency. If an AI systems micro-manages workers with granular instructions, it can lead to a loss of autonomy and dignity for the workers while performing their work. Demanding instructions and shift-schedules based on such external factors can be exhaustive and stressful for workers.
5. Access to and enjoyment of **essential** ~~essential~~ private services and public services and benefits:		
(a) AI systems intended to be used by public authorities or on behalf of public authorities to evaluate the eligibility of natural persons for public assistance benefits and services, as well		In our opinion statutory social insurance schemes (e.g. pension insurance, health and long-term care insurance) are covered by Annex III,5a. Also covered are insurance

PUBLIC

as to grant, reduce, revoke, or reclaim such benefits and services;		policies, in which property-like entitlements to social benefits are acquired. Does COM agree?
(b) AI systems intended to be used to evaluate the creditworthiness of natural persons or establish their credit score, with the exception of AI systems put into service by small scale providers for their own use;		It is our understanding that AI systems used by credit agencies to establish a credit score for natural persons which will be used for other purposes than the evaluation of their creditworthiness (e.g. access to essential services such as housing, electricity, and telecommunication services) do fall under No. 5(b) and are therefore considered high-risk. This is important to us because these systems have a significant impact on the lives of natural persons. Flawed systems pose a significant threat to people's ability to participate fully in society. In that sense, we ask the Pres/COM to further specify which processes are precisely covered by the use cases evaluation of creditworthiness and establishment of credit scores (e.g. access to Buy-Now-Pay-Later offerings) as well as to clarify which entities are

PUBLIC

		subject to this high-risk use case. On the other hand entities already regulated by comprehensive financial sector regulation should only be included insofar as the AI act pose additional requirements, e.g. reporting provisions on fundamental rights issues, the EU data base or (potential) obligations towards affected persons (see Art. 52a and 52b). Concerning Annex III point 5 (b) and (d), we ask the Pres/COM to thoroughly analyse and present to the WP whether, and which areas, the existing European Financial and insurance sector regulatory sufficiently covers the regulatory areas covered by the AI act, to avoid regulatory gaps and duplication with exisiting regulation.
(c) AI systems intended to be used to dispatch, or to establish priority in the		

PUBLIC

dispatching of emergency first response services, including by firefighters and medical aid**;**~~.~~		
~~**(d) AI systems intended to be used for insurance premium setting, underwritings and claims assessments.**~~	**(d) AI systems not covered under (a) intended to be used for health insurance and long term care insurance premiums setting, underwriting and claim assessment or for decision on provision of benefits and services**	AI systems for health insurances and long-term care insurances must be added as cases for high-risk AI. Highly sensitive data is processed in this area, and decisions in this area can have particularly far-reaching consequences. This is necessary despite the fact that - AI systems used by institutions covered by Union and Member State financial market regulation for insurance premium setting, underwriting and claims assessment are subject to extensive regulation and strict supervision, and - insurance services provided by insurance companies covered by sector-specific financial market regulation should in principle not be

PUBLIC

		included in the AI Act, as also stated by EIOPA. Concerning Annex III point 5 (b) and (d), we ask the Pres/COM to thoroughly analyse and present to the WP whether, and which areas, the existing European Financial and insurance sector regulatory sufficiently covers the regulatory areas covered by the AI act, to avoid regulatory gaps and duplication with exisiting regulation.
	New (e) AI systems intended to be used in access to housing.	**Housing is correctly named as an essential service in the recitals and should therefore be included here. It is an area where EU anti-discrimination legislation applies, and also objectively one of the main areas where discrimination occurs, and where robust protections are needed. This justifies classfying AI used in this area as high-risk.** new e) These systems could be potential

PUBLIC

	e) AI systems intended for or used in the context of debt collection services **new f)** AI systems intended for personalised pricing within the meaning of Article 6 (1) (ea) of Directive 2011/83/EU	harmful for vulnerable persons that are indebted. If the AI systems makes an mistake in this context, this could exclude the indebted person from participation in the economy. new f) AI Systems used for personalising prices could potentially discriminiate consumers based on ethnicity, income and othe variables. This could lead to a divide between consumers on the market and decreases economic price transparency.
6. Law enforcement:		

PUBLIC

(a) AI systems intended to be used by law enforcement authorities **or on their behalf** for making individual risk assessments of natural persons in order to assess the risk of a natural person for offending or reoffending or the risk for for **a natural person to become a** potential victim~~s~~ of criminal offences;		
(b) AI systems intended to be used by law enforcement authorities **or on their behalf** as polygraphs and similar tools or to detect the emotional state of a natural person;		
(c) ~~AI systems intended to be used by law enforcement authorities **or on their behalf** for law enforcement purposes to detect deep fakes as referred to in article 52(3);~~		
(d) AI systems intended to be used by law enforcement authorities **or on their behalf** for		We ask for further clarification. The description

PUBLIC

evaluation of the reliability of evidence in the course of investigation or prosecution of criminal offences;		of AI systems covered by lit. (d) should be clear-cut. It must be ensured that systems without risk to health, safety or fundamental rights are not covered. For DEU, it is very important that lit. (d) is defined more narrowly in this respect. At the same time, systems that pose a risk to the above-mentioned protected interests must remain covered.
(e) AI systems intended to be used by law enforcement authorities **or on their behalf** for predicting the occurrence or reoccurrence of an actual or potential criminal offence based on profiling of natural persons as referred to in Article 3(4) of Directive (EU) 2016/680 or assessing personality traits and characteristics or past criminal behaviour of natural persons or groups;		
(f) AI systems intended to be used by law		DEU discusses whether the definition provided

PUBLIC

enforcement authorities **or on their behalf** for profiling of natural persons as referred to in Article 3(4) of Directive (EU) 2016/680 in the course of detection, investigation or prosecution of criminal offences;		in Article 3 (4) of Directive (EU) 2016/680 is too broad for the classification as a high-risk CI, and whether a definition should be included in the regulation itself or a concrete description of the facts deemed critical in Annex III. For DEU, for example, it is important in this context that this definition does not include in particular the tasks of an FIU in the sense of "The core function of an FIU is the receipt, analysis and transmitting of suspicious transaction reports identified and filed by the private sector". This is especially true if these suspicious transaction reports are related to financial transactions of natural persons. What do the Commission or other Member States think about the need to clarify (f)?
~~(g) AI systems intended to be used **by law enforcement authorities or on their behalf** for crime analytics regarding natural persons, allowing law enforcement authorities to search~~		

PUBLIC

~~complex related and unrelated large data sets available in different data sources or in different data formats in order to identify unknown patterns or discover hidden relationships in the data.~~		
7. Migration, asylum and border control management:		
(a) AI systems intended to be used by competent public authorities **or on their behalf** as polygraphs and similar tools or to detect the emotional state of a natural person;		
(b) AI systems intended to be used by competent public authorities **or on their behalf** to assess a risk, including a security risk, a risk of irregular immigration, or a health risk, posed by a natural person who intends to enter or has entered into the territory of a Member State;		

PUBLIC

~~(c) AI systems intended to be used by competent public authorities **or on their behalf** for the verification of the authenticity of travel documents and supporting documentation of natural persons and detect non-authentic documents by checking their security features;~~		
(d) AI systems intended to ~~assist~~ **to be used by** competent public authorities **or on their behalf** for the examination of applications for asylum, visa and residence permits and associated complaints with regard to the eligibility of the natural persons applying for a status.		We ask for further clarification. The description of AI systems covered by lit (d) should be clear-cut. It must be ensured that systems without risk to health, safety or fundamental rights are not covered. For DEU, it is very important that lit. (d) is defined more narrowly in this respect. At the same time, systems that pose a risk to the above-mentioned protected interests must remain covered.
8. Administration of justice and democratic processes:		
(a) AI systems intended to ~~assist~~ **be used by** a	applying the law to a concrete set of facts	In order to more clearly distinguish AI systems

PUBLIC

judicial authority **or on their behalf** ~~in~~ **for** ~~researching and~~ interpreting facts ~~and~~ **or** the law ~~and in~~ **for** applying the law to a concrete set of facts.	whenever these systems provide predictions, recommendations or suggestions to the user with respect to a specific case.	that are classified as high-risk from AI systems that are intended for purely ancillary activities and that therefore have no direct impact on the decision of a specific case, we suggest a further addition in Annex III no. 8(a). Alternatively, this could be added in recital 40.
ANNEX IV **TECHNICAL DOCUMENTATION referred to in Article 11(1)**		
The technical documentation referred to in Article 11(1) shall contain at least the following information, as applicable to the relevant AI system:		
1. A general description of the AI system including:		
(a) its intended purpose, the person/s		

PUBLIC

developing the system the date and the version of the system;		
(b) how the AI system interacts or can be used to interact with hardware or software that is not part of the AI system itself, where applicable;		
(c) the versions of relevant software or firmware and any requirement related to version update;		
(d) the description of all forms in which the AI system is placed on the market or put into service **(e.g. software package embedded into hardware, downloadable, API etc.)**;		
(e) the description of hardware on which the AI system is intended to run;		
(f) where the AI system is a component of		

PUBLIC

products, photographs or illustrations showing external features, marking and internal layout of those products;		
(g) instructions of use for the user and, where applicable installation instructions;		
2. A detailed description of the elements of the AI system and of the process for its development, including:		
(a) the methods and steps performed for the development of the AI system, including, where relevant, recourse to pre-trained systems or tools provided by third parties and how these have been used, integrated or modified by the provider;		
(b) the design specifications of the system, namely the general logic of the AI system and of the algorithms; the key design choices	and the relevance of the different ~~parameters~~ features;	The choice of the term parameter is probably not indended and should read instead:

PUBLIC

including the rationale and assumptions made, also with regard to persons or groups of persons on which the system is intended to be used; the main classification choices; what the system is designed to optimise for and the relevance of the different parameters; the decisions about any possible trade-off made regarding the technical solutions adopted to comply with the requirements set out in Title III, Chapter 2;		"relevance of the different features". In ML (see, e.g., Goodfellow et al., Deep Learning, 2016, 3, 117, 292 f.): parameter = learnable variables in the model (used in this way in Recital 6a and Article 3(29)), such as coefficients in a regression, or weights and biases in a neural network feature = input information the model considers
(c) the description of the system architecture explaining how software components build on or feed into each other and integrate into the overall processing; the computational resources used to develop, train, test and validate the AI system;	(c) the description of the system architecture explaining how software components build on or feed into each other and integrate into the overall processing; the computational resources including the specific hardware and its runtime used to develop, train, test and validate the AI system;	The proposed specification of the term "computational resources" warrants that the technical documentation may serve to estimate the energy consumption of the respective AI system and with few additional information also its carbon footprint. While posing little additional effort for developers, this information could greatly contribute to understand AI's energy-related impacts.

PUBLIC

(d) where relevant, the data requirements in terms of datasheets describing the training methodologies and techniques and the training data sets used, **including a general description of these data sets**, ~~including~~ information about ~~the~~ **their** provenance ~~of those data sets~~, ~~their~~ scope and main characteristics; how the data was obtained and selected; labelling procedures (e.g. for supervised learning), data cleaning methodologies (e.g. outliers detection);		
(e) assessment of the human oversight measures needed in accordance with Article 14, including an assessment of the technical measures needed to facilitate the interpretation of the outputs of AI systems by the users, in accordance with Articles 13(3)(d);		
(f) where applicable, a detailed description of pre-determined changes to the AI system and its performance, together with all the relevant		

PUBLIC

information related to the technical solutions adopted to ensure continuous compliance of the AI system with the relevant requirements set out in Title III, Chapter 2;		
(g) the validation and testing procedures used, including information about the validation and testing data used and their main characteristics; metrics used to measure accuracy, robustness, cybersecurity and compliance with other relevant requirements set out in Title III, Chapter 2 as well as potentially discriminatory impacts; test logs and all test reports dated and signed by the responsible persons, including with regard to pre-determined changes as referred to under point (f).		
3. Detailed information about the monitoring, functioning and control of the AI system, in particular with regard to: its capabilities and limitations in performance,	Detailed information about the monitoring, functioning and control of the AI system, in particular with regard to: its capabilities and limitations in performance, including the	Unintended outcomes and sources of risks to the environment may include environmental damages provoked by the foreseeable misrecognition of e.g. technical defects due to

PUBLIC

including the degrees of accuracy for specific persons or groups of persons on which the system is intended to be used and the overall expected level of accuracy in relation to its intended purpose; the foreseeable unintended outcomes and sources of risks to health and safety, fundamental rights and discrimination in view of the intended purpose of the AI system; the human oversight measures needed in accordance with Article 14, including the technical measures put in place to facilitate the interpretation of the outputs of AI systems by the users; specifications on input data, as appropriate;	degrees of accuracy for specific persons or groups of persons on which the system is intended to be used and the overall expected level of accuracy in relation to its intended purpose; the foreseeable unintended outcomes and sources of risks to health and safety, fundamental rights, the environment and discrimination in view of the intended purpose of the AI system; (…)	imperfect accuracy. As illustration, the introduction of an AI-based defect detection system in chemicals production plants may entail a reduction of workforce to monitor plant behavior as well as a heavier reliance on the AI system. If the AI system would now miss to correctly identify a defect such as the leakage of harmful chemicals, the leakage might remain unnoticed for longer as less people are charged with monitoring tasks. While AI systems can significantly improve the detection of plant malfunctioning and the intended purpose of such a system presents a large benefit to the environment, the foreseable unintented outcome should nevertheless be thought through beforehand and idealy be complemented by precautionary measures.
4. A detailed description of the risk management system in accordance with Article 9;		

PUBLIC

5. A description of ~~any~~ **relevant** change**s made by the provider** to the system through its lifecycle;		
6. A list of the harmonised standards applied in full or in part the references of which have been published in the Official Journal of the European Union; where no such harmonised standards have been applied, a detailed description of the solutions adopted to meet the requirements set out in Title III, Chapter 2, including a list of other relevant standards and technical specifications applied;		
7. A copy of the EU declaration of conformity;		
8. A detailed description of the system in place to evaluate the AI system performance in the post-market phase in accordance with		

PUBLIC

Article 61, including the post-market monitoring plan referred to in Article 61(3).		
ANNEX V **EU DECLARATION OF CONFORMITY**		
The EU declaration of conformity referred to in Article 48, shall contain all of the following information:		
1. AI system name and type and any additional unambiguous reference allowing identification and traceability of the AI system;		
2. Name and address of the provider or, where applicable, their authorised representative;		
3. A statement that the EU declaration of conformity is issued under the sole responsibility of the provider;		

PUBLIC

4. A statement that the AI system in question is in conformity with this Regulation and, if applicable, with any other relevant Union legislation that provides for the issuing of an EU declaration of conformity;		
5. References to any relevant harmonised standards used or any other common specification in relation to which conformity is declared;		
6. Where applicable, the name and identification number of the notified body, a description of the conformity assessment procedure performed and identification of the certificate issued;		
7. Place and date of issue of the declaration, name and function of the person who signed it as well as an indication for, and on behalf of		

PUBLIC

whom, that person signed, signature.		
ANNEX VI **CONFORMITY ASSESSMENT PROCEDURE BASED ON INTERNAL CONTROL**		
1. The conformity assessment procedure based on internal control is the conformity assessment procedure based on points 2 to 4.		
2. The provider verifies that the established quality management system is in compliance with the requirements of Article 17.		
3. The provider examines the information contained in the technical documentation in order to assess the compliance of the AI system with the relevant essential requirements set out in Title III, Chapter 2.		

PUBLIC

4. The provider also verifies that the design and development process of the AI system and its post-market monitoring as referred to in Article 61 is consistent with the technical documentation.		
ANNEX VII **CONFORMITY BASED ON ASSESSMENT OF QUALITY MANAGEMENT SYSTEM AND ASSESSMENT OF TECHNICAL DOCUMENTATION**		
1. Introduction		
Conformity based on assessment of quality management system and assessment of the technical documentation is the conformity assessment procedure based on points 2 to 5.		
2. Overview		

PUBLIC

The approved quality management system for the design, development and testing of AI systems pursuant to Article 17 shall be examined in accordance with point 3 and shall be subject to surveillance as specified in point 5. The technical documentation of the AI system shall be examined in accordance with point 4.		
3. Quality management system		
3.1. The application of the provider shall include:		
(a) the name and address of the provider and, if the application is lodged by the authorised representative, their name and address as well;		
(b) the list of AI systems covered under the same quality management system;		
(c) the technical documentation for each AI		

PUBLIC

system covered under the same quality management system;		
(d) the documentation concerning the quality management system which shall cover all the aspects listed under Article 17;		
(e) a description of the procedures in place to ensure that the quality management system remains adequate and effective;		
(f) a written declaration that the same application has not been lodged with any other notified body.		
3.2. The quality management system shall be assessed by the notified body, which shall determine whether it satisfies the requirements referred to in Article 17.		
The decision shall be notified to the provider or		

PUBLIC

its authorised representative.		
The notification shall contain the conclusions of the assessment of the quality management system and the reasoned assessment decision.		
3.3. The quality management system as approved shall continue to be implemented and maintained by the provider so that it remains adequate and efficient.		
3.4. Any intended change to the approved quality management system or the list of AI systems covered by the latter shall be brought to the attention of the notified body by the provider.		
The proposed changes shall be examined by the notified body, which shall decide whether the modified quality management system continues to satisfy the requirements referred to in point		

PUBLIC

3.2 or whether a reassessment is necessary.		
The notified body shall notify the provider of its decision. The notification shall contain the conclusions of the examination of the changes and the reasoned assessment decision.		
4. Control of the technical documentation.		
4.1. In addition to the application referred to in point 3, an application with a notified body of their choice shall be lodged by the provider for the assessment of the technical documentation relating to the AI system which the provider intends to place on the market or put into service and which is covered by the quality management system referred to under point 3.		
4.2. The application shall include:		
(a) the name and address of the provider;		

PUBLIC

(b) a written declaration that the same application has not been lodged with any other notified body;		
(c) the technical documentation referred to in Annex IV.		
4.3. The technical documentation shall be examined by the notified body. ~~To this purpose,~~ **Where relevant and limited to what is necessary to fulfil their tasks,** the notified body shall be granted full access to the training, **validation,** and testing datasets used ~~by the provider~~, including, **where appropriate and subject to security safeguards,** through application programming interfaces (API) or other ~~appropriate~~ **relevant technical** means and tools enabling remote access.		
4.4. In examining the technical documentation,		

PUBLIC

the notified body may require that the provider supplies further evidence or carries out further tests so as to enable a proper assessment of conformity of the AI system with the requirements set out in Title III, Chapter 2. Whenever the notified body is not satisfied with the tests carried out by the provider, the notified body shall directly carry out adequate tests, as appropriate.		
4.5. ~~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 notified body shall also be granted access to the source code of the AI system~~.		
Notified bodies shall be granted access to the source code of the AI system upon a reasoned request and only when the following cumulative conditions are fulfilled:		

PUBLIC

a) Access to source code is necessary to assess the conformity of the high-risk AI system with the requirements set out in Title III, Chapter 2, and		
b) testing/auditing procedures and verifications based on the data and documentation provided by the provider have been exhausted or proved insufficient.		
4.6. The decision shall be notified to the provider or its authorised representative. The notification shall contain the conclusions of the assessment of the technical documentation and the reasoned assessment decision.		
Where the AI system is in conformity with the requirements set out in Title III, Chapter 2, an EU technical documentation assessment certificate shall be issued by the notified body.		

PUBLIC

The certificate shall indicate the name and address of the provider, the conclusions of the examination, the conditions (if any) for its validity and the data necessary for the identification of the AI system.		
The certificate and its annexes shall contain all relevant information to allow the conformity of the AI system to be evaluated, and to allow for control of the AI system while in use, where applicable.		
Where the AI system is not in conformity with the requirements set out in Title III, Chapter 2, the notified body shall refuse to issue an EU technical documentation assessment certificate and shall inform the applicant accordingly, giving detailed reasons for its refusal.		
Where the AI system does not meet the requirement relating to the data used to train it,		

PUBLIC

re-training of the AI system will be needed prior to the application for a new conformity assessment. In this case, the reasoned assessment decision of the notified body refusing to issue the EU technical documentation assessment certificate shall contain specific considerations on the quality data used to train the AI system, notably on the reasons for non-compliance.		
4.7. Any change to the AI system that could affect the compliance of the AI system with the requirements or its intended purpose shall be approved by the notified body which issued the EU technical documentation assessment certificate. The provider shall inform such notified body of its intention to introduce any of the above-mentioned changes or if it becomes otherwise aware of the occurrence of such changes. The intended changes shall be assessed by the notified body which shall decide whether		

PUBLIC

those changes require a new conformity assessment in accordance with Article 43(4) or whether they could be addressed by means of a supplement to the EU technical documentation assessment certificate. In the latter case, the notified body shall assess the changes, notify the provider of its decision and, where the changes are approved, issue to the provider a supplement to the EU technical documentation assessment certificate.		
5. Surveillance of the approved quality management system.		
5.1. The purpose of the surveillance carried out by the notified body referred to in Point 3 is to make sure that the provider duly fulfils the terms and conditions of the approved quality management system.		
5.2. For assessment purposes, the provider		It is suggested to specify that this applies only to

PUBLIC

shall allow the notified body to access the premises where the design, development, testing of the AI systems is taking place. The provider shall further share with the notified body all necessary information.		the final AI system, as AI systems currently consist of different components developed internationally so that uniform access is not possible. In addition, leading AI companies sometimes operate 'remote', i.e. without open premises.
5.3. The notified body shall carry out periodic audits to make sure that the provider maintains and applies the quality management system and shall provide the provider with an audit report. In the context of those audits, the notified body may carry out additional tests of the AI systems for which an EU technical documentation assessment certificate was issued.		

PUBLIC

ANNEX VIII **INFORMATION TO BE SUBMITTED UPON THE REGISTRATION OF HIGH-RISK AI SYSTEMS IN ACCORDANCE WITH ARTICLE 51**		
The following information shall be provided and thereafter kept up to date with regard to high-risk AI systems to be registered in accordance with Article 51.	The following information shall be provided and thereafter kept up to date with regard to ~~high-risk~~ AI systems to be registered in accordance with Article 51.	
1. Name, address and contact details of the provider;		
	~~1. a) Name, address and contact details of the public authority using an AI system;~~	To ensure greater public oversight of AI-systems and to access information about in which contexts AI-systems are put in operation, the framework must be complemented by the information, which public authority is deploying

PUBLIC

		the high risk AI-system.
2. Where submission of information is carried out by another person on behalf of the provider, the name, address and contact details of that person;		
3. Name, address and contact details of the authorised representative, where applicable;		
4. AI system trade name and any additional unambiguous reference allowing identification and traceability of the AI system;		
5. Description of the intended purpose of the AI system; **for high-risk AI systems in the areas of law enforcement and migration, asylum and border control management referred to in Annex III, points 1, 6 and 7, this information shall not include the specific context and conditions of use.**		

PUBLIC

6. Status of the AI system (on the market, or in service; no longer placed on the market/in service, recalled);		
7. Type, number and expiry date of the certificate issued by the notified body and the name or identification number of that notified body, when applicable;		
8. A scanned copy of the certificate referred to in point 7, when applicable;		
9. Member States in which the AI system is or has been placed on the market, put into service or made available in the Union;		
10. A copy of the EU declaration of conformity referred to in Article 48;		
11. Electronic instructions for use; this information shall not be provided for high-risk		

PUBLIC

AI systems in the areas of law enforcement and migration, asylum and border control management referred to in Annex III, points 1, 6 and 7.		
12. URL for additional information (optional).		
ANNEX VIIIa		
INFORMATION TO BE SUBMITTED UPON THE REGISTRATION OF HIGH-RISK AI SYSTEMS LISTED IN ANNEX III IN RELATION TO TESTING IN REAL WORLD CONDITIONS IN ACCORDANCE WITH ARTICLE 54a		
The following information shall be provided and thereafter kept up to date with regard to testing in real world conditions to be registered in accordance with Article 54a:		

PUBLIC

1. Union-wide unique single identification number of the testing in real world conditions;		
2. Name and contact details of the provider or prospective provider and users involved in the testing in real world conditions;		
3. A brief description of the AI system, its intended purpose and other information necessary for the identification of the system;		
4. A summary of the main characteristics of the plan for testing in real world conditions;		
5. Information on the suspension or termination of the testing in real world conditions.		
ANNEX IX **UNION LEGISLATION ON LARGE-SCALE IT SYSTEMS IN THE AREA OF**		

PUBLIC

FREEDOM, SECURITY AND JUSTICE		
1. Schengen Information System		
(a) Regulation (EU) 2018/1860 of the European Parliament and of the Council of 28 November 2018 on the use of the Schengen Information System for the return of illegally staying third-country nationals (OJ L 312, 7.12.2018, p. 1).		
(b) Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006 (OJ L 312, 7.12.2018, p. 14)		

PUBLIC

(c) Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU (OJ L 312, 7.12.2018, p. 56).		
2. Visa Information System		
(a) Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EC) No 767/2008, Regulation (EC) No 810/2009, Regulation (EU) 2017/2226, Regulation (EU) 2016/399, Regulation XX/2018 [Interoperability Regulation], and Decision 2004/512/EC and		

PUBLIC

repealing Council Decision 2008/633/JHA - COM(2018) 302 final. To be updated once the Regulation is adopted (April/May 2021) by the co-legislators.		
3. Eurodac		
(a) Amended proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the establishment of 'Eurodac' for the comparison of biometric data for the effective application of Regulation (EU) XXX/XXX [Regulation on Asylum and Migration Management] and of Regulation (EU) XXX/XXX [Resettlement Regulation], for identifying an illegally staying third-country national or stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes and amending Regulations (EU) 2018/1240 and (EU)		

PUBLIC

2019/818 – COM(2020) 614 final.		
4. Entry/Exit System		
(a) Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011 (OJ L 327, 9.12.2017, p. 20).		
5. European Travel Information and Authorisation System		
(a) Regulation (EU) 2018/1240 of the		

PUBLIC

European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226 (OJ L 236, 19.9.2018, p. 1).		
(b) Regulation (EU) 2018/1241 of the European Parliament and of the Council of 12 September 2018 amending Regulation (EU) 2016/794 for the purpose of establishing a European Travel Information and Authorisation System (ETIAS) (OJ L 236, 19.9.2018, p. 72).		
6. European Criminal Records Information System on third-country nationals and stateless persons		
(a) Regulation (EU) 2019/816 of the European Parliament and of the Council of 17		

PUBLIC

April 2019 establishing a centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons (ECRIS-TCN) to supplement the European Criminal Records Information System and amending Regulation (EU) 2018/1726 (OJ L 135, 22.5.2019, p. 1).		
7. Interoperability		
(a) Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa (OJ L 135, 22.5.2019, p. 27).		
(b) Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information		

PUBLIC

systems in the field of police and judicial cooperation, asylum and migration (OJ L 135, 22.5.2019, p. 85).		
	End	End