Council of the European Union
General Secretariat

Brussels, 18 November 2021

WK 14060/2021 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 - Consolidated table of comments from PT, PL, BG, SK, CZ, IT, MT, LV, AT, EE, DK, NL, BE, ES, FR, SE, FI (Articles 1-29, Annexes I-IV) (doc. 8115/21)

DOCUMENT PARTIALLY ACCESSIBLE TO THE PUBLIC (25.01.2022)

Delegations will find in annex the consolidated table of comments from : PT, PL, BG, SK, CZ, IT, MT, LV, AT, EE, DK, NL, BE, ES, FR, SE, FI on Artificial Intelligence Act (Articles 1-29, Annexes I-IV).

Commission proposal	Drafting Suggestions Comments
2021/0106 (COD) **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**	**DELETED** SK: (Comments):

LEGISLATIVE ACTS	**SK:** Slovakia hereby enters a general scrutiny reservation. Also, the combination of short deadline and high number of articles and annexes under review did not enable Slovakia to prepare and include relevant drafting suggestions (i.e. only comments are submitted). In order to prevent possible succesful court challenges to the validity of the regulation (as was previously the case in the field of data flows and data retention), Slovakia proposes to request CLS to provide an opinion – in light of case-law of CJEU - on - sufficiency of legal bases for the proposal, as it appears to regulate also areas falling under exclusive or shared competence of MSs, e.g. exercise of public powers by national authorites in fields such as justice, education or social benefits; public security (in fields such as law enforcement) and national security (e.g. dual-use of AI systems for military purposes; supply of AI systems to national security bodies by private actors), - limitations of article 290 TFEU for delegated powers of the Commission, especially those proposed under article 4 and 7, - possible implications of article 16 TFEU for institutional independce of national and EU authorities, including areas beyond law enforcement. Slovakia also proposes to invite the EU Fundamental Rights Agency to have a deeper look into the current challenges and limitations of law enforcement in cyberspace and of software assessment and monitoring, and also to identify possible toolbox for adressing these challenges. Lessons learned from application of

	GDPR and EU Medical Device Regulation should be taken into account in the study. Last but not least, the proposal should take equal care of *all* its declared goals, i.e. overriding reasons of public interest as enumerated in recital no. 1: the protection of (1) health, (2) safety and (3) fundamental rights. The regulatory tools for both *ex ante* and *ex post* protection fundamental rights and health need to be as explicit, sophisticated and effective as those related to safety. The current proposal is primarily focused on safety aspects, given that it is built on product safety legislation and conformity assessments, and relies to a significant extent on technical standards created by private entities. The protection of health and fundamental rights should not be reduced to technical standards in situations where this is not feasible or adequate. This is all the more important because the proposal is a full harmonisation measure which implies that all AI deployment and uses not forbidden or restricted by the proposed regulation will be automatically deemed legitimate, lawful and proportionate. CZ: (Comments): The Czech Republic still has doubts about the choice of a horizontal regulatory approach since it was not sufficiently proved that the aim of this proposal cannot be achieved by sectoral regulation. The proposed regulation has an impact on various sectoral policies, some of which are under shared or supporting competences of the EU (public health, employment, transport, civil protection, security, education, law enforcement). The legal basis and regulatory approach of the proposed regulation should take into account

	these sectoral policies and explain how this regulation contributes to their development (for example employment policy – title IX SFEU, law enforcement – title V SFEU, etc.). A relation between the proposed horizontal regulation and sectoral policies is unclear, especially with regards to the division of competencies between EU and the Member States. Impact of the horizontal approach and proposed rules on these sectors must be properly analysed so as to prevent any duplications or negative impacts. The same goes for the interplay with existing sectoral policies and legislative acts. **DELETED** DK: (Comments): We support the aim with the Commission's proposal of establishing a horisontal regulatory framework for AI, as this can facilitate a genuinely single market for trustworthy, human-centric, safe and secure AI. The regulatory framework must follow a risk-based, technology-neutral and proportionate approach where the level of obligations follows the level of possible harmful effects. Against this background, there is a need for a clear and operational regulatory framework that ensures citizens' trust and increases protection in society, without unnecessarily hampering the ability to innovate or impairing competitiveness.

	Therefore, we need to establish an approach, where innovation and trustworthiness are two sides of the same coin. This means striking the balance between setting the right requirements and safeguards in order to achieve trustworthy AI, while at the same time facilitating and promoting innovation. In this regard, the regulatory framework must create an internal market with coherent rules, taking into account existing legislation and not creating unnecessary administrative and financial burdens for providers and users. Further work and discussion are needed on some of the key elements of the proposal in order to achieve the proportionate, risk-based approach. In our view, we should start out by finding common ground in terms of the scope as well as the definition of AI. A common understanding on these aspects will be essential for reaching an agreement on the content of the rest of the proposal. We have therefore prioritised these elements in our written remarks. Our following comments and proposals will be of a preliminary nature, as we still have a scrutiny reservation on the proposal. Furthermore, as article 1-29 contain some of the most complex articles, national coordination is still ongoing and we reserve the right to submit further comments and proposals concerning these articles at a later stage. NL: (Comments): General comments: NL appreciates the opportunity provided bythe Slovenian Presidency to submit input on Chapter I, II and III of the proposal for a Artificial Intelligence Act (hereinafter AI Act), as well as its corresponding Annexes I, II, III and IIII. Please note, that the drafting suggestions and/or comments provided below are non-exhaustive: We are currently still analysing the proposal in -depth which is why at this point we are only able tp share general

	comments; the NL comments below hone in on issues considered to be most pertinent. We urge, as also mentioned during the Telecom Council of October 14th, that thoroughness and quality takes precedence over speed in the process of coming to a common position. This is a complex file with potentially far-reaching implications. Furthermore, at the time of writing, the formation of a new Dutch government is ongoing. Our current government is under resignation 1) The Netherlands calls for strengther involvement of Member States to amend Annex I and III in the proposed AI Act, and therefore the flexibility to react to the fast technological developtments of AI. In our opinion, these annexes are essential elements of the proposed regulation and we propose to change art 7 into implementing acts. Moreover The Netherlands would like to have removed high risk areas in Annex III, as menioned in prior draft proposals in this final one it has been removed. Finally, NL calls for the incorporation of a consultation procedure to harvest perspectives of non-governmental stakeholders such as civil society and enterprises that have expertise about developments with regards to techniques, approaches and areas of high-risk AI, based on best practices. 2) The Netherlands takes the position that the AI-Act should be without prejudice to both EU and national rules governing the context in which the AI-system is used. For instance, according to the principles of fair trial and good administration, certain decisions that are unilaterally binding must be duly justified. This motivation principle should apply to any AI system used by the public sector and cannot be overridden by the AI Act if this act does not contain provisions regarding this principle. 3) The Netherlands worries about the current definition of "AI system" as used in Article 3 and Annex I, as it may create an overbroad scope of application for this regulation. We suggest specifying the scope to AI systems that because of their specific characteristics warrant the extra measures this regulation prescribes. Our concern is that the combination of this broad definition of an AI-system, the extensive list of techniques (annex I) and

	the broad definitions of the high-risk areas, (annex III) may result in regulating algorithmic systems with minimum risk for fundamental rights. This bears the risk to be disproportionate, to overburden organizations (particularly SMEs), to stifle innovation and needs to be considered carefully. 4) Regarding the definitions in article 3 and the obligations in articles 16-29: more attention should be given to clarifying the different roles and responsibilities organizations have when taking on more than one role (provider, user, etc). This applies particularly to the responsibilities government organizations have when developing in house and when using AI systems in house. 5) The NL supports a risk-based approach in which the requirements are proportional to the risk. Extensive requirements apply to high-risk AI systems to prevent or mitigate the risks (article 9, Chapter II), such as the obligation to carry out an ex ante conformity assessment or have it carried out (article 19, Chapter III). Although we agree that a certain level of requirements and obligations should be imposed by the actors, we strongly ask for more guidance especially to help SMEs, start-ups and small scale providers and users. This is important because those involved do not always have the right expertise in their companies available. It is important to guide them as much as possible, especially for instance with the conformity assessment and administration burdens. For instance guidance can be given in the form of tools, roadmaps or checklists. 6) The Netherlands is carefully considering the role of those affected by AI systems: This draft regulation focuses on economic and institutional actors that provide or use AI systems, and focuses on governance. We are currently researching whether those affected by AI systems in its provisions have sufficient access to legal protection under this regulation combined with other legislation. 7) The Netherlands is carefully considering the harms in article 5, and whether we have to include (alternative) measures to further avoid unlawful breaches of human rights, democracy and the rule of law. 8) Align AI Act with the GDPR : The AI Act overall currently lacks clear references to the existing provisions in the GDPR. The AIA would benefit from clearer references to the GDPR, to increase legal certainty and clarity.

	9) Exclude national security: Please explicietly exclude national security from the scope of this regulation as it is an exclusive member state competence. 10) By the use of the word 'students' in Annex III the Cion proposal could suggest only to refer to vocational and higher education, and lifelong learning. AI systems are also applied, and perhaps even more, in primary and secondary education, and children in this age group (minors up to 17 years) are even more vulnerable. In the understanding that the AI Act should be applicable to all educational sectors we suggest a minor redrafting to clarify this. Secondly, the AI Act should take into account that in education developments take place such as flexibilisation, with as a consequence a shift from 'summative assessment' (evaluation of what has been learned, i.e. learning outcomes) to 'formative assessment' (assessment with a view to steer the learning process), as well as predictive use of AI, with impact on equal opportunities. (b) AI systems intended to be used for the purpose of assessing **pupils and** students in educational and vocational training institutions **at all levels with a view to assessing learning outcomes, steering the learning process** and for assessing participants in tests commonly required for admission to educational institutions. BE: (Comments): - Belgium acknowledges the fact that the choice for a horizontal approach certainly has its advantages, but nevertheless we must not forget that AI systems can be repurposed for various uses with their own specificities. Hence, a balance between specialization and consistency is needed regarding some specific sectors, e.g. the law enforcement sector.

	- Furthermore, because this Proposal is a first-of-its-kind initiative and will affect companies and users who are already fully engaged with this technology, Belgium wants to emphasize the importance to test this Proposal in practice via policy prototyping. This can be done by the European Commission, the Member States and/or other actors who will ultimately have to enforce this pioneering horizontal legislation when it enters into force. We believe that testing this Proposal engaging (some or all) operators of AI systems identified in the AIA and subsequently taking into account the conclusions of these tests will improve the actual feasibility and enforceability of the AIA. - Also, a reference can be made to GDPR compliancy of the AIA. Article 22 of the GDPR is also important (automated individualized decision-making (e.g. profiling)). - We understand that the Commission is possibly preparing a complementary EU act to cover specific AI related liability issues. Belgium can definitely support this initiative as we believe it is crucial to have clear and comprehensive rules on liability in the context of AI. However, to prevent fragmentation of AI liability rules in the EU, we would like to stress that as the revision work is still ongoing (public consultation until 10 January 2022), clear delineation of liability rules for harm caused by AI should already be considered in this Proposal. Some questions are raised in this matter: Who is responsible for elimination or lowering the risk (e.g. adaption in AI model – take ownership rights into account – risks of lock-ins), for recovery-actions, actions in case of damage? The user, the developer, the supplier, …? Can this be agreed by contract (with the danger that all responsibilities will then be transferred to the user)?

	FR: (Drafting): **(New) This Regulation is without prejudice to Article 4(2) of the TEU.** **(New) This Regulation recognises the importance of justified, proportionate and controlled use of AI for important objectives of general public interest of the Union or of a Member State, such as the protection of the public and security. The use of AI for such objectives should be allowed.** **(New) The transparency and compliance obligations established by this Regulation should not lead to the publication of information the secrecy of which is necessary for the preservation of the public interest .** **(New) This Regulation do not intend to prevent homeland security forces from adapting their AI tools in light of the use of such tools by criminal groups.** (9) For the purposes of this Regulation the notion of publicly accessible space should be understood as referring to any physical place that is accessible to the public, irrespective of whether the place in question is privately or publicly owned. Therefore, the notion does not cover places that are private in nature and normally not freely accessible for third parties, including law enforcement authorities, unless those parties have been specifically invited or authorised, such as homes, private clubs, offices, warehouses and factories. Online spaces are not covered

	either, as they are not physical spaces. **This wording does not extend to correctional institutions.** 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. (12) This Regulation should also apply to Union institutions, offices, bodies and agencies when acting as a provider or user of an AI system. ~~**AI systems exclusively developed or used for military purposes should be excluded from the scope of 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)**~~**. DELETED** 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]. FR: (Comments):

	COM replied to FR's question about correctional institutions, saying that it did not consider them to be publicly accessible spaces. It is believed that this exclusion needs to appear at least in the recitals. We suggest either "*correctional institutions*" or "*prison premisces*".

	According to COM, national security is out of the regulations's scope by nature. However, several institutions fear that ECJ would interpret it differently if this is not expressly mentioned. We could also be open to another phrasing SE: (Comments): SE would like to add that there might be need to clarify the relationship to GDPR and LED in an article. It is in many parts difficult to see how the regulations relate to each other. This in turn may result in difficulties to comply with both sets of rules.

	There is a need to review the proposal to ascertain that the obligations aimed at the targeted stakeholders (eg. companies, public authorities etc) are proportionate to the aim of the legislation. Many of the articles contain in themselves or in combination with other articles and the annexes far reaching and detailed demands on the targeted stakeholders. As a consequence these stakeholders (providers, users etc.) will be subject to a significantly increased administrative burden and other types of costs. Other aspects of concern are e.g. the wide definition of AI in combination with the wide definition of what encompasses high-risk AI and the procedure (e.g. through delegated acts) for adding to the areas covered by the regulation. SE also have concerns regarding the extensive reporting requirements and the handling of this information which include confidential and other proprietory information. Art. 70 might not be enough to secure confidentiality which will effect all prior articles that stipulate stakeholders need for documentation and sharing of information. It is of great importance that the regulation is predictable and easy to apply. FI: (Comments): Please note that these views are still preliminary as we have not yet received the official Finnish position on the AI Act. Finland supports the Commission's human-centered approach and its objective of striving to harmonise the development of the union, respecting its common values, and to improve citizens' participation and

	trust in society and the development of democracy. It is important to ensure compliance with fundamental rights and, in particular, provisions on the protection of personal data. Finland supports the Commission's objective of defining a common European approach that takes into account the interests of citizens, companies, municipalities and society, with the aim of avoid-ing the fragmentation of the internal market. A clear regulatory framework and legal certainty will help increase the trust of consumers, the public sector and businesses in AI and thus accelerate the uptake of AI. The regulatory environ-ment must encourage innovations and support the development of new technologies, business and services. Finland supports the risk-based approach proposed by the Commission. This ensures the pro-portionality of the regulation. In general, Finland emphasizes the possibility of using self-regula-tion and sharing best practices. Before the implementation of the proposed regulatory framework, we must ensure that it will not impose unnecessary regulatory burden on businesses and consumers and that it complies with the principles of better regulation in other respects. In addition, uunnecessary administrative burden should be avoided.
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	PL: (Drafting): and the use of artificial intelligence systems (‘AI systems’) in the Union~~;~~ as also the developing of AI systems in only the porpose of science excluded from the rules harmonisted for placing on the market; PL: (Comments): As alternative it is to be considered to include a minimum a recital in the preamble to the regulation,

Union;	which would confirm the possibility of working (research) on such systems without meeting these requirements, in relation to systems that will not be traded (economic activity), unless we assume that prohibitions, specific requirements , including transparency, always applies. It that case clarification is needed in this section. SK: (Comments): CZ: (Drafting): (a) harmonised rules that define the minimum requirements for the placing on the market, the putting into service and the use of artificial intelligence systems ('AI systems') in the Union; CZ: (Comments): The EU legislation on AI should set only a minimum requirements or standards of AI regulation for providers and manufacturers. We need to prevent an unnecessary administrative burden.
(a) prohibitions of	PT:

certain artificial intelligence practices;	(Drafting): (b) prohibitions of certain artificial intelligence practices; BE: (Drafting): (b) prohibitions of certain artificial intelligence practices; BE: (Comments): Practical comment: the numbered list in Article 1 is faulty numbered: see (a) followed by another (a) instead of (b) and so on.
(b) specific requirements for high-risk AI systems and obligations for operators of such systems;	PT: (Drafting): (c) specific requirements for high-risk AI systems and obligations for operators of such systems; BE: (Drafting):

	(c) specific requirements for high-risk AI systems and obligations for operators of such systems;
(c) harmonised transparency rules for 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;	PT: (Drafting): (d) harmonised transparency rules for AI systems intended to interact with natural persons, including emotion recognition systems and biometric categorisation systems, and AI systems used to generate or manipulate image, audio or video content, and automatic decision systems/algorithms (credit assignment, social benefits, insurances, etc.) that have a considerable impact in people's lives; BE: (Drafting): (d) harmonised transparency rules for 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; FI: (Comments): FI considers the obligations of artificial intelligence systems covered by the transparency obligation of the

	proposed regulation and notes that the impact of the proposal needs to be carefully assessed.
(d) rules on market monitoring and surveillance.	PT: (Drafting): (e) rules on market monitoring and surveillance. PL: (Drafting): rules on market monitoring and surveillance including remedial measures those come from the updated state of the knowledge of AI systems life-cycle referring to technology, good practices and standards in the firld of AI systems application PL: (Comments): Alternative is to supplementing The Recital 51 by this expression. BE: (Drafting): (e) rules on market monitoring and surveillance.

	ES: (Drafting): (d) rules on market monitoring, surveillance and the establishment of a governance system. ES: (Comments): For the purpose of being complete on what the Regulation covers. FI: (Comments): Reference to “artificial intelligence” missing.
	PL: (Drafting): (e) conditions and reasons of administrative penalties for breaking the rules of the Regulation PL: (Comments): The partial reference to the question of liability in recital 53 seems insufficient and may raise numerous doubts as to whether it is only administrative or also civil liability? There is a need to clearly udeline that

	the Regulation's scope include only administrative respnsibility. ES: (Drafting): (e) Measures in support of responsible innovation in the field of artificial intelligence. (f) Confidentiality rules and a general frame for penalties and sanctions ES: (Comments): For the purpose of being complete on what the Regulation covers. FR: (Drafting): **New article** **This Regulation is without prejudice to Regulation (EU) 2020/852 of the European Parliament and of the Council of 18 June 2020 on the establishment of a framework to facilitate sustainable investment and amending Regulation (EU) 2019/2088** FR: (Comments):

	The regulation gives a framework and sets criteria to determine if aaaand how an economica financial activity can be qualified as "*environmentally sustainable*".is "green" or not. The chapter II of this regulation targets environmentally sustainable economic activities and specifically climate change.
Article 2 Scope	PL: (Drafting): The Regulation does not establish additional conflict-of-law rules under private international law and jurisdiction national. PL: (Comments): In order to clarify the relationship with EU rules of private international law, in particular with the Rome II Regulation on the law applicable to non-contractual obligations, consideration should be given to adding the following sentence as a minium to the relevant recital in the preamble to the scope of the Regulation. CZ: (Drafting):

	CZ: (Comments): It would be useful to have concrete examples of past or potential misuse of AI in the EU with negative impact on fundamental rights mentioned in the recitals so as to illustrate why the regulation is needed and why the sectoral specific legislation is not sufficient. All regulation should be evidence-based. BE: (Comments): The scope of the AIA is essential as to its applicability and enforcement, requiring clear, easily interpretable and applicable definitions. Belgium therefore suggests refining the scope of the AIA by providing further clarification where needed. FI: (Comments): It is important to clarify the scope with regards to public authorities and private entities acting on behalf of public entities. For constitutional reasons, Member States must be able to regulate use of AI systems in public authorities in situations that are not explicitly regulated in the proposed Regulation (in particular, authorities and activities not covered by Annex III). It should be reconsidered if the issue at hand should in part be regulated using a Directive instead (cf. the field of data protection, where both a Regulation and

	a Directive are used). It should be clarified in the scope what is the Regulation's relation to scientific research concerning AI systemsas well as AI systems developed or used for national security purposes As a transversal technology, the *very same AI application* can be used for different purposes in a variety of contexts, and the positive or negative consequences of the technology will depend heavily thereon. For example, image (e.g. face) recognition for the purpose of identifying ethnic minorities should be classified as high-risk, and possibly forbidden entirely. However, precisely the same technical application can also be used for socially acceptable purposes or in the service of the general interest. An example is a road vehicle, where the image recognition system can be used for distinguishing a pedestrian from a plastic bag when deciding whether to stop the vehicle. From a technical point of view, it utilises the very same components than the problematic high risk or red flag applications (e.g. recognizing images and retrieving information from a database. This applies for many, if not all, AI applications. *Given this multitude of uses for the same software and software components*, it is crucial that when formulating a regulatory framework, this is taken into account. It should be made explicit that neutral or beneficial uses of these systems, or their components, are clearly excluded from the high-risk category, even if they utilise *the same technical components*.

1. This Regulation applies to:	PT: (Comments): It came to our attention that AI researchers and software developers regularly upload AI models and other AI related materials to repositories, which have a critical and beneficial role in the software ecosystem. Therefore, given the wording of this article there is a risk that those who upload these materials to software repositories (e.g. open-source), or the operators of these repositories, could be viewed as a regulated entity without "placing on the market" or "putting into service" the system in the EU, which might have an impact on research and open-source software innovation on the EU. Consequently, we recommend that the terms "placing on the market" and "putting into service" should specifically exclude use of AI systems for internal research and development purposes. SK: (Comments): **SK:** As the proposal leaves extremely limited room for MSs to regulate other aspects of AI (because of full harmonisation approach), it is suitable to either expand the scope of the regulation to non-professional provision and use of AI systems or to explicitly state that the regulation does not pre-empt MSs´ competence to regulate such provision and (especially) use of AI systems beyond the scope of the regulation. The non-professional provision and especially use of AI systems, including by unknown actors, can be at least as highly risky as in professional cases. It is also hard to prove whether the use is

	professional or not. To the extent that the proposal does not intend to regulate R&D, this should be stated clearly in this article. However, as regards R&D, the iterative (constantly developing) nature of many AI systems needs to be taken into account.
(a) providers placing on the market or putting into service AI systems in the Union, irrespective of whether those providers are established within the Union or in a third country;	
(b) users of AI systems located within the Union;	PL: (Drafting):

	users of AI systems located by seat or by branch within the Union;
(c) providers and users of AI systems that are located in a third country, where the output produced by the system is used in the Union;	PL: (Drafting): providers and users of AI systems that are located by seat or by branch in a third country **DELETED**

	DK: (Comments): We support the objective of creating a level playing field. However, it is still unclear how article 2.1.c can be enforced in practice.
	DK: (Drafting): (d) manufacturers, importers, distributors or any other third-party placing on the market, making available on the market or putting into service AI systems in the Union; DK: (Comments): As a technical remark, we are questioning why article 2.1 does not apply to manufacturers, importers, distributors and any other third party as laid out in article 24, 26, 27 and 28.
2. For high-risk AI systems that are safety components of	PL: (Comments):

products or systems, or which are themselves products or systems, falling within the scope of the following acts, only Article 84 of this Regulation shall apply:	The effects of Art. 2 clause 2. - does it mean that all artificial intelligence systems related to rail transport, air transport, equipment and agricultural equipment, etc., will fall outside the scope of this regulation until the outcome of the review under 84? This issue requires a clear decision. MT: (Comments): Malta stresses that any technology should be explored even if the classification is high risk or outright bans, however, ONLY if the proposed solution is developed in a controlled environment such as Regulatory SANDBOX followed by proper documentation why such solution needs to be explored and what is to be learnt. Proposals can be assessed by a panel of experts which may allow or suggest improvements to the concept or deny such development. Developing restrictive solutions will help to improve/update regulations as the concept is proven and tested. Malta notes that with respect to Public Health, especially in the categorisation of natural persons, there might be specific population health interventions to protect Public Health which would require the use of Artificial Intelligence techniques to implement said interventions in a short period of time. There needs to be provisions that need to allow for such population-level interventions. DK: (Comments):

	In order to classify as a high-risk system, third-party conformity assessment in the specific legislation is required. We would like to see this criterion reflected. FI: (Drafting):
(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	PL: (Drafting):

developed or used exclusively for military purposes.	This Regulation shall not apply to AI systems developed or used exclusively for military purposes till AI system impacts civil affects and is auditable of transparency . PL: (Comments): Dual-effect military testing and dual-use applications should also be considered. **DELETED** SK: (Comments): **SK:** The issue of division of competences between the EU and its MSs as well as sufficiency of legal bases needs to be examined. See above general comments to the entire proposal. CZ: (Drafting):

	This Regulation shall not apply to AI systems developed or used exclusively ~~for military purposes~~ or predominantly for safeguarding of national security or defence. CZ: (Comments): The current wording of the exemption contained in Art. 2 (3) is too restrictive. It applies only to AI systems developed or used "exclusively" for "military" purposes. In addition, recital 12 contains very limited explanation of this exemption, which focuses on the exclusive remit of the Common Foreign and Security Policy regulated under Title V of the Treaty on the European Union (TEU). Firstly, "exclusive" use of AI system for "military" purposes may be difficult to establish in many situations (e.g. AI system designed for air and space military defence could be used against natural space object on collision course). Secondly, AI systems are a special class of "products" which are characterized mainly by "processing of data" (rather than by physical features or purpose of usage). Therefore, the exemptions should reflect this dual nature of AI systems in order to delineate more clearly the competencies of the EU and the Member States. The EU law related to (personal) data processing establishes, for good reasons, the scope of relevant rules more precisely. For example, the GDPR (Art. 2(2) of the Regulation 2016/679/EU) does not apply in the course of an activity which falls outside the scope of Union law, which includes matters of national

	security and defence. In addition, Art. 23(1)(a)(b) of GDPR allows significant divergence from GDPR where necessary for safeguarding of national security or defence. More profoundly, the Council general approach on draft e-Privacy regulation addresses the issue of obligatory participation by the private sector entities on the lawful tasks of security and defence authorities by stipulating (Art. 2(2)(a) of document ST 5840/21) that "(t)his Regulation does not apply to activities, which fall outside the scope of Union law, and in any event measures and processing operations concerning national security and defence, regardless of who is carrying out those operations". Given that AI systems need to process data to achieve the intended ends, it is obvious that the exemptions related to both components need to be more aligned. The current wording would mean that the Regulation applies to situations where national security authorities buy AI systems for national security purposes (as these systems are on the market and therefore have to fulfil the conditions of the Regulation). The only exemption related to national security relates to situations when security agencies develop the system in-house. This concept is not acceptable. If national security agency needs to buy an AI system to be used for national security purposes, such system should be exempted from the scope of this Regulation. MT: (Comments): Malta notes that this needs to be reconsidered. They should likewise be captured by this Regulation and in

	case of exemptions, these should only be allowed after a public consultation and the carrying out of the required impact assessments, including human rights impact assessments. LV: (Drafting): This Regulation shall not apply to AI systems developed or used exclusively for military and national security purposes. LV: (Comments): Article 4 point 2 of the EU Treaty (exclusive competence of Member States in the field of national security) EE: (Drafting): 3. This Regulation shall not apply to AI systems developed or used exclusively for military **or national security** purposes. EE: (Comments): It should be stated explicitly that national security is not in the scope of the regulation.

	Estonia supports the current exemption according to which this regulation does not apply to AI systems developed or used exclusively for military purposes. We would propose to keep this exemption. Furthermore, in our view, national security (a closely linked field to military matters) should also be exempted from the scope of application of the regulation due to its nature. This would include e.g. such AI that is used by intelligence agencies for the purposes of ensuring national security. Those exemptions should also apply to high risk solutions developed or used exclusively for military or national security purposes. According to art 4 (2) of the Treaty on European Union (TEU), national security remains the sole responsibility of each Member State. Taking this into account, we suggest adding a corresponding recital in due time. Depending on the final wording of the general exemption clause, there may be a need to amend specific articles. Therefore, we would like to reserve the right to come back to them if need be. We would also suggest that the relevant recital excluding military use from the scope, would also explain that this regulation does not address Lethal Autonomous Weapons Systems (LAWS), since those are governed by the relevant international law. Additionally, this article text or recitals should clarify that if an AI system initially developed exclusively for military purposes is at some point used for civilian purposes, the civilian use of such a system is not excluded from the scope of the Regulation. DK: (Drafting):

	3. ~~This Regulation shall not apply to AI systems developed or used exclusively for military purposes.~~ This Regulation shall not apply to AI when developed or used in relation to Member States' defence or national security, regardless of which entity is carrying out those activities and whether it is a public entity or a private entity. This Regulation shall be without prejudice to actions taken by Member States for the protection of information the disclosure of which is contrary to their essential interests of national security, public security or defence. DK: (Comments): We would like to see a clause which clearly and effectively excludes national security from the scope. Furthermore, it should be reflected that the regulation does not oblige member states or entities to supply information where such a supply of information would be contrary to national security or defence interests. Similar wording can be found in the scope of the NIS2. BE: (Drafting):

	This Regulation shall not apply to AI systems developed or used exclusively for military or national security purposes BE: (Comments): When AI systems are used or developed in order to protect the national security, they should also be excluded from the scope of the Regulation, taking into account the exemption of national security enshrined in Art. 4(2) TEU. ES: (Drafting): 3. This Regulation shall not apply to AI systems developed or used exclusively for military purposes or in the context of National Security. ES: (Comments): Article 4.2 of the EUT considers National Security as a national attribution of Member States. **DELETED**

	DELETED SE: (Drafting): 3. This Regulation ~~shall~~ does not apply to AI systems developed or used ~~exclusively~~ for the purpose of activities which fall outside the scope of Union law, and in any event activities

	concerning national security and defence, regardless of whether it is a state actor or non-state actor who is developing or using the system. SE: (Comments): It is clear from Article 4.2 TEU that national security and defence remain the sole responsibility of each Member State. However, from the ECJ's recent judgements in cases C-623/17 and joined cases C-511/18, C-512/18 and C-520/18 it is equally clear that, from the ECJ's perspective, the article alone may not be sufficient to fully exclude Members State measures for the protection of national security and defence from the material scope of a legislative act. Instead, a clause that clarifies what is excluded from a legislative act because of national security concerns may be necessary. The current exclusion clause in the proposal is insufficient as it does not (i) explicitly exempt national security from the scope of the act, (ii) clearly exclude relevant activities by entities that are otherwise in scope of the act, or (iii) reflect that most AI systems developed or used for the purpose of national security or defence are dual use systems. Very few systems are developed exclusively for the purpose of national security or defence. For these reasons, we propose that Article 2.3 is replaced with an exclusion clause modelled after the Council draft of Article 2 ePrivacy regulation of 10 February 2021.
	CZ:

	(Drafting): This Regulation shall not apply to research activites in relation to AI. CZ: (Comments): It should be clearly stated that research activities are not covered by this draft regulation and are not included in its scope. In relation to that, last sentence of recital 16 should be deleted so as to prevent any confusion or lack of legal clarity. More concretely, this sentence should be deleted from recital 16 as soon as the new para is added to Article 2 as proposed: "Research for legitimate purposes in relation to such AI systems should not be stifled by the prohibition, if such research does not amount to use of the AI system in human-machine relations that exposes natural persons to harm and such research is carried out in accordance with recognised ethical standards for scientific research." BE: (Drafting): This Regulation shall also not apply to research activites in relation to AI. BE: (Comments):

	Research activities are not in the scope of the regulation. This should be made explicit by introducing wording in the text and by the deleting last sentence of recital 16. SE: (Drafting): This regulation does not apply to research for legitimate purposes for any AI system if such research is carried out in accordance with recognised ethical standards for scientific research. SE: (Comments): In accordance with recite 16 research need to clearly be excluded. Ethical and other regulations already exist- otherwise AIA risk leading to less innovation and competitiveness and potential security risk for Europe. Important to allow for research even on/for system no one want to use Otherwise it is missing a regulation that clarifies the conditions under which AI systems can be used or developed in research. It needs to be clarified how research and development is limited in conducting activities that possibly could lead to projects with moderate to high risk. It also needs to be clarified how the proposal relates to the ethical review that takes place today within the research and innovation system. It is doubtful whether the proposal is compatible with Swedish law when a Swedish university is a developer of AI systems, for example. requirements for deletion of data in Article 54 (g).

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	PL: (Drafting): [link or note to proper other regulation is needed] PL: (Comments): In the event of divergent regulations, what will be the effect on AI systems used simultaneously by MS and some EU agencies? SK: (Comments): **SK**: This exemption opens up possibilities for deviation from the general rules contained in the proposal, such as article 2 (1) (c) . Impacts on protection of fundamental rights of EU citizens (including on article 16 TFEU) need to be analysed in depth. Such analysis was not contained in the impact assessment. CZ: (Comments): We suggest adding a reference to the Article 39 and explaining the position of Conformity assessment

judicial cooperation with the Union or with one or more Member States.	bodies of third countries in the text of the Article 2. The applicability of the AI regulation on the third countries has to be clear. MT: (Comments): Malta notes that this needs to be reconsidered. Public Authorities should likewise be captured by this Regulation and in case of exemptions, these should only be allowed after a public consultation and the carrying out of the required impact assessments, including human rights impact assessments. BE: (Comments): We suggest to add a reference to Article 39 and to explain its relation with the Article 2 (4). The applicability of the AI regulation on the third countries has to be clear. ES: (Drafting): 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 for cases having a clear

	internationa impact and provided that these actions enter in the competences of such authorities and international organisations, not constituing a substitution of functions with regards national authorities. ES: (Comments): This is an important way for circumvention. This should be limited to uses where a clear international limitation is agreed. We suggest a new formulation, being aware that limiting this disposition may be hard. SE: (Comments): Does this apply to the work that is within the realm of Interpol/Europol and associated organisations for the purpose of crime prevention? How can the boundaries about the systems and applications used in the collaboration and used by member countries be exempted?
	PL: (Drafting): This Regulation shall not apply to civil liability of harms in developing, deploying, operating, using and utilisng AI systems PL:

	(Comments): [*The EC planns to update the Product Liability Directive from 1986 to the digital age, and is looking at ways to address harms specifically caused by AI systems*].
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 of Directive 2000/31/EC of the European Parliament and of the Council[1] [*as to be replaced by the corresponding*	SK: (Comments): **SK:** This provision should also state that the regulation does not affect relevant selected provisions of Regulation (EU) 600/2014 (MiFIR) and Directive 2014/65/EU (MiFID). At the same time, closer inter-linkage between these acts and the proposal should be considered as it may be beneficial in areas such as definition of AI systems or other legal definitions, etc. Legal certainty may encourage further innovation and investments in financial markets.

[1] 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).

provisions of the Digital Services Act].	
	PL: (Drafting): This Regulation is without prejudice to the right of Member States to restrict the use of a specific type of AI systems for aspects not covered by this Regulation. LV: (Drafting): *6. This Regulation is without prejudice to the competences of Member States concerning national security in compliance with Union law.* LV: (Comments): Article 4 point 2 of the EU Treaty (exclusive competence of Member States in the field of national security) AT: (Comments):

	Addition suggested to clearly define the scope of application of the AIA and avoid misunderstandings and ambiguities regarding the relationship of the data protection framework with the AIA. There should be added the full reference to the respective legislative acts. ES: (Drafting): 6. This Regulation shall not affect activities related to the development and put into service of AI systems in the field of reserch and development that are not assesed to be inmediatley placed in the market. It shall not affect either to the publication of open source AI systems that not are intended to be offer a functional operation. ES: (Comments): Even if R&D was not included, more clarity will be welcome in this regard. Open source AI that is published in repositories but it is not intended to be put into place for operational purposes should not be covered.
Article 3 Definitions	PT: (Comments):

	General remark regarding definitions: the regulation should, where possible, facilitate cooperation both at the domestic level (between MS) but also at the international level. As such, all definitions used should, in so far as possible, be compatible with similar definitions used in other relevant instruments on AI. SK: (Comments): **SK:** For the sake of legal certainty, Slovakia believes that this article should also define - "AI systems that continue to learn", - "subliminal techniques" - „significant changes" (in design or intended purpose) - "public security" (to the extent this is intended to be regulated under the proposal) - "public assistance". FI: (Comments): In Finland, the public sector is already utilizing various rule- and non-ruled based "algorithmic" methods for various tasks. In practice, these methods are (typically) developed and deployed in complex and distributed supply chains between several public sector actors and private sector companies. Moreover,

	these technologies are not static, but dynamic collections of subcomponents. They, and their components are constantly updated in real time processes. As it stands, it may not fit well with the actual distribution of work between organizations when they develop, deploy or utilize these technologies, and pose practical challenges. FI considers that the specific nature of the public sector must be taken into account and the right to good governance must be safeguarded with regard to public authorities. It must also be ensured that no unnecessary burden will be put upon the public sector actors as public sector is already object to national regulations related to good governance, transparency and data management practices. The Government views that the proposed regulation on tasks in the field of public administration using high-risk artificial intelligence systems needs to be clarified and specified. The Government states that the effects of the proposed regulation on the digitalization of public administration must be examined carefully.
For the purpose of this Regulation, the following definitions apply:	PT: (Comments): We kindly recommend ensuring that the definitions are set in alphabetic order with the aim of facilitating its reading, analysis, and application

(1) 'artificial intelligence system' (AI system) means software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with;	PT: (Drafting): Ex.1: OECD definition of AI system – *a machine-based system that is capable of influencing the environment by producing an output (predictions, recommendations or decisions) for a given set of objectives. It uses machine and/or human-based data and inputs to (i) perceive real and/or virtual environments; (ii) abstract these perceptions into models through analysis in an automated manner (e.g., with machine learning), or manually; and (iii) use model inference to formulate options for outcomes. AI systems are designed to operate with varying levels of autonomy.* Ex2.: The definition proposed by the High-Level Expert Group on Artificial Intelligence: *Artificial intelligence (AI) refers to systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals. AI-based systems can be purely software-based, acting in the virtual world (e.g. voice assistants, image analysis software, search engines, speech and face recognition systems) or AI can be embedded in hardware devices (e.g. advanced robots, autonomous cars, drones or Internet of Things applications).* PT: (Comments):

	We suggest using the AI definition made by the High-Level Expert Group on Artificial Intelligence: (ex2) Despite the remarkable effort made by the Commission in this context, we consider that the construction of the concept of 'Artificial intelligence system', as laid down in Article 3(1), deserves some remarks. Starting by noting that the first objective of the proposal is precisely to "ensure that AI systems placed on the Union market and used are safe and comply with existing legislation on fundamental rights and Union values", the concrete definition of what is meant by "Artificial Intelligence" plays a central role as it is the basis for the specific definition of all normative solutions included in the Proposal. Based on this premise, the solution adopted in the Proposal - which is based on the concept of "Artificial Intelligence System" - should adequately reflect the concern, expressed in Recital 6, according to which the definition to be adopted "(…) should be clearly defined to ensure legal certainty, while providing the flexibility to accommodate future technological developments [and] (…) be based on the key functional characteristics of the software, in particular the ability, for a given set of human-defined objectives, to generate outputs such as content, predictions, recommendations, or decisions which influence the environment with which the system interacts, be it in a physical or digital dimension." Considering the architecture built on the basis of Article 3(1) and its dynamic interaction with Annex I, we are not convinced that these conditions have been effectively achieved. By referring to the "techniques and approaches listed in Annex I", the definition relies on the accuracy of the list inserted therein. The problem is, in our view, that both provisions considered, we would have an absurdly vague definition: if the specific purpose of Annex I was to complete the definition by specifying

	which techniques and approaches constitute techniques and approaches in the field of artificial intelligence, it completely misses the point by enabling the inclusion of practically all computational techniques and approaches (machine learning, inductive and deductive logic, and statistical approaches). Since the title of Annex I refers to "Artificial Intelligence Techniques and Approaches," it could be assumed that the definition of, for example, 'logic-based approaches' is limited to logic-based approaches to artificial intelligence. However, as we have indicated above, since 'artificial intelligence' is defined as any algorithm which uses the techniques listed in Annex I, this specification has become circular and is therefore not a specification at all. Given the paramount importance of this definition and the inherent need for it to be technically robust enough to confer a degree of legal certainty compatible with the legal principles and values to be guaranteed by the proposed framework, it will be essential, we believe, to rethink this definition. The possible solution will be to carry out a comparative study of the definitions already advanced in the various fora which best takes into account these requirements. PL: (Drafting): 'artificial intelligence system' (AI system) means ~~software~~ a set ~~that is~~ developed with one or more than one of the techniques and approaches listed in Annex I excluding statistical techniques and regressive logic if it displays intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy or unexplainability of processing – to achieve specific goals ~~.~~ and can, for a given

	set of human-defined objectives or goals defined by a self-contained algorithm, generate outputs such as content, predictions, recommendations, or decisions influencing the external environments they interact with; PL: (Comments): Important notice to Annex I - statistical techniques and regressive logic, which are elements of data science models, but not elements of artificial intelligence techniques, should be excluded from the definition. Crucial point is to do not narrow AI systems to software or to do not cover any software as AI systems. **DELETED**

	DELETED

	DELETED

	DELETED SK: (Comments): **SK:** This definition appears too wide even if the cumulative nature (combined reading) of the provision and Annex I is taken into account. It covers also automating software other than AI systems, such as software – which uses one or more techniques in Annex I – that can also generate outputs influencing the environments they interact with, for a given set of human-defined objectives. At the same time, the definition should also cover software which is not only *developed* with, but also *comprising* (at the time of their placing on the market, putting into service or use) of one or more of the techniques and approaches listed in Annex I. In such a way we make sure that such techniques were not used solely as supplementary techniques in the development phase and that the AI systems are capable of functioning in environments other than those pre-defined or derived in the development phase.

	Focus on "software function" rather than "software" as such can be considered in the definition of AI system. Slovakia would welcome an existing practical example of true AI system using solely techniques mentioned in Annex I c) as it is uncertain that such true AI systems exist, as suggested by the proposed definition. CZ: (Drafting): ~~'artificial intelligence system' (AI system) means software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with;~~ "Artificial intelligence (AI) systems are software (and possibly also hardware) systems designed by humans that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge, or processing the information, derived from this data and deciding the best action(s) to take to achieve the given goal. AI systems can either use symbolic rules or learn a numeric model, and they can also adapt their behaviour by analysing how the environment is affected by their previous actions. As a scientific discipline, AI includes several approaches and techniques, such as machine learning (of which deep learning and reinforcement learning are specific examples), machine reasoning (which

	includes planning, scheduling, knowledge representation and reasoning, search, and optimization), and robotics (which includes control, perception, sensors and actuators, as well as the integration of all other techniques into cyber-physical systems)." CZ: (Comments): CZ proposes to use the updated definition put together by High-Level Expert Group on Artificial Intelligence instead of the one proposed by the Commission. The definition of AI system should not cover "simple" information systems that work with defined and unchanging algorithms that are determined by humans, not by a machine based on its learning, or statistical models and statistical prediction methods, such as logical and linear regressions (see for example approaches included under letter (c) in Annex I), as these approaches do not pose similar risk associated with more complex autonomous systems based on machine learning which is usually considered as an example/type of AI. Definition of AI system should also acknowledge that AI system could be software-based, as well as hardware-based. Whole definition as an integral part of the regulation should be fully embedded in the normative part of the text, in order to provide for legal certainty and fulfil the legitimate expectations. Adding clarifications to the recitals so as to ensure legal clarity is recommended. **DELETED**

	DELETED MT: (Comments):

	Malta notes that before a definition is finalised, one should focus on the various types and uses of AI and their differentiation in use and scope AT: (Comments): The definition of AI technologies Art. 3 and Annex I, is too broad . The technologies listed in Annex I would include typical machine learning approaches as well as logic & knowledge-based approaches and statistical methods, and would thus classify almost any modern software code as an AI application. The systems according to this definition clearly lack the characteristics of "exhibiting intelligent behaviour by analysing their environment and - with a certain degree of autonomy - take actions to achieve certain goals", previously used by the Commission to define artificial intelligence systems ("Artificial Intelligence for Europe", "AI for Europe"). EE: (Comments): AI definition in Article 3 in conjunction with Annex I is too broad and currently includes every data analytics-based solution and even much that is considered just IT. This is the case even if other conditions are considered and implied. AI must be defined more narrowly and rather include only more complicating machine learning and deep learning use-cases.

	DK: (Drafting): (1) 'artificial intelligence system' (AI system) means software that is developed with one or more of the techniques and approaches listed in Annex I and that ~~can~~, for a given set of human-defined objectives, operates with a level of autonomy and generates outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with; DK: (Comments): It is essential that we aim at a clearer and narrower definition of AI. We are aware of the complexity of the task, especially in order find a definition which can accommodate technical developments, while being precise enough to provide the necessary legal certainty. At the moment, we do not see that this objective has been fully achieved. The properties of AI as currently defined is too broad, as it for example encompasses common statistical systems. Systems which have been around for decades and should not be considered as AI. This is especially due to the fact that the definition does not take into account that AI systems operate with a level of autonomy. This is a key characteristic which separates AI from other types of traditional systems, and which is both reflected in the definition of the OECD as well as the HLEG. This would furthermore help to specify that an AI system is an intelligent system which finds and decides on the suitable steps to achieve human-defined objectives. This is so far missing from the definition. An accompanying recital would furthermore need to specify that systems which implements the automation of rules-based actions with defined inputs and outputs based on objective and logic criteria – meaning codified rules - would not be seen as an AI system and thereby not be within the scope of this regulation. Thereby, we clarify that all software systems enabling automated processes or decisions

	(ADM) are not automatically AI. Furthermore, we are sceptical of defining AI in an annex that can be updated through delegated acts, as the definition of AI is a fundamental part of the proposal, and as changes to this definition could result in consequences which were not originally foreseen in the ordinary legislative process. Thereby, we are still assessing whether an approach where such a fundamental part can be updated through a delegated act is the right way forward. In this light, we would like the opinion of the Council Legal Service in terms of whether the definition of AI would constitute a non-essential element according to article 290 TFEU as well as if the usage of an annex will affect the assessment in this regard. As a preliminary view of the annex 1, we as a minimum need to limit the list of techniques and approaches listed in Annex 1, cf. comments concerning Annex 1. It is important that we prioritize our efforts to discuss the definition in further detail and and carefully explore all possible options in order to agree on the best way forward, as agreement on this essential aspect is needed before we can meaningful decide on the content of the remaining content of the proposal. BE: (Comments): Belgium believes that the definition of an AI system as provided in Article 3(1), in conjunction with the list of approaches and techniques in Annex I, may be too broad, since it could potentially include more traditional/conventional software systems or analytical processing, that should not fall under the scope of the Proposal. This increases legal uncertainty for users and manufacturers and is harmful for global competition. For example, in law enforcement, some techniques that are already in use are not generally considered strict AI applications, but might fall under the Proposal's broad definition of AI, e.g. certain 'intelligent' search engines regarding personal data or risk assessment techniques; moreover, this is also

	seen in the medical sector, where randomized control trials fall under 'statistical approaches' as stated in Annex I, but few would see this as AI; furthermore, also in the migration and asylum sector the broad definition can cause uncertainty, e.g. it is not clear if the definition applies to all possible uses by the Immigration Office or only in cases where the use of the technology has a direct impact on the content aspects of an application in one of the procedures included in Annex III. The examples provided by the Commission in its presentations give some additional insight in the intended scope of the definition, but the AIA itself should be sufficiently clear. Therefore, the definition of 'AI system' should be refined and the analysis of the assessment of which approaches and techniques should or should not be covered by Annex I, should be further deepened, as this definition depends on this list. ES: (Drafting): (1) 'artificial intelligence system' (AI system) means ~~software~~ a machine-based system, that can be built from start or may use other AI systems, that operates with varying degrees of autonomy, ~~that is developed with~~ uses one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs addressing ambiguity, such as content, predictions, recommendations, or decisions influencing the environments they interact with; ES: (Comments):

	Software: Even though we are aware that software is the vast majority of systems, we prefer to stick to a wider definition for the sake of future AI developments, even if they are not still mature (i.e.: neuromorphic). - Based in other AI systems or built from the start-> in order to properly address the allocation of responsibilities when a developer puts into service or market an AI system that is based in other AI system(s). - Degrees of autonomy: it is appropriate, since Ai systems may differ in the need of external actions to generate the mentioned outputs. - 'Uses' instead of 'is developed with': it is more accurate since the tools for developing AI may refer to other aspects such as frameworks, libraries, etc. - Addressing ambiguity: Since the outputs that AI systems generate can't always be fully predicted by the natural person(s) developing such system (in opposition to software AMD systems that are not AI), it is important to highlight this characteristic in the definition: it will help to avoid that other software that is not AI falls in the scope of the regulation. SE: (Drafting): SE:

	(Comments): The definition needs further modification to narrow the scope. SE is still analysing the consequences with every modification. SE notes that the OECD definition also includes that "AI systems are designed to operate with varying levels of autonomy". The current proposal is also not in line with the proposed version from the HLEG AI. The definition of AI-system in article 3.1 ***in correlation*** with art. 6.2 (high-risk systems) ***and the corresponding*** point 6 (and 7 (b-c)) of Annex III would generate too serious impact on law enforcement ability to develop and use AI- systems since it would include "simple" information systems that work with defined and unchanging algorithms that are determined by humans.
	CZ: (Comments): Regarding Article 24 Obligations of product manufacturers: As the term "manufacturer" as such is not included in the list of terms and definitions of Art. 3, for the sake of legal certainty, we suggest this term to be included in the list. Regarding Article 9 Risk management system: As the terms "appropriate" and "intended purpose" are not included in the list of terms and definitions of Art. 3, for the sake of legal certainty, we suggest these terms to be included in the list.

	Regarding Article 16 Obligations of providers of high-risk AI systems: As the terms "technical documentation"; "necessary corrective actions"; „(non)conformity" are not included in the list of terms and definitions of Art. 3, for the sake of legal certainty,we suggest this term to be included in the list. ES: (Drafting): (2) 'AI System lifecycle': means the various phases of analyzing, designing, developing, applying, deployment, implantation, training, testing, parametrization and subsequently monitoring an artificial intelligence system, including human oversight, where applicable. These phases shall also include activities regarding the preparation and processing of data, where necessary for training and testing. (3) 'General purpose AI systems' means the AI systems that are designed for solving miscellaneous problems, such as text or speech recognition or image detection, among others. Their intended purpose is meant to be defined upon its deployment. (4) 'AI regulatory Sandbox': framework established by a pubilc authority that allows innovative companies or institutions to conduct live experiments in a controlled environment under the supervision of such authority. (5) Biases: systematic errors, which can include those of a statistical, cognitive, societal, structural or institutional nature, that place privileged groups at a systematic advantage or unprivileged groups at a systematic disadvantage, either directly or indirectly. Biases could motivate decisions based on gender, race or other individual or group characteristics that may result in favoring one individual or group over the other. ES:

	(Comments): It is important to include a definition for AI lifecycle. We suggest a definition, but other definitions based on the OECD could also be acceptable..
(1) '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 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;	PT: (Drafting): (~~1~~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 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; PT: (Comments): This notion appears to consider that all AI systems are developed as a stand-alone product or service and then "placed on the market"/ "put into service". Whereas the AI ecosystem is very diverse and there are many ways AI systems are developed and deployed, and there is almost never a singular entity or person that develops an AI system. AI systems are the result of numerous entities building on top of others' efforts, for example it may start by using open-source repositories created by several contributors and the resulting model might then be shared under an open-source licence for others to build on.

	Therefore, we should ask ourselves "who among all the contributors "develops an AI system?" It is of paramount importance to consider the range of developers, researchers, and innovators that make up the open-source community, which has been crucial to advancing the state-of-the-art of AI development. We need a more nuanced taxonomy to identify the relevant participants in the AI ecosystem and allocate the appropriate responsibilities and obligations to each one rather than a definition of "provider" that risks treating all contributions big and small to the same burdensome regulatory standards irrespective of their nature and role. Please consider correcting this small typo. PL: (Drafting): whether for payment or free of charge, even if it is subject only of science or development without aim of placing it on market or putting it into service; **DELETED**

	DELETED DK: (Comments): ES:

	(Drafting): (6) '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 ~~with a view~~ **in order** to placing it on the market or putting it into service under its own name or trademark, whether for payment or free of charge; FR: (Drafting): (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 ~~**with a view**~~ to ~~**placing it**~~**be placed** on the market or **put**~~**ting it**~~ into service under its own name or trademark, whether for payment or free of charge; FR: (Comments): "*with a view to*" is a very extensive notion that will cause interpretation problems , and that, in certain cases, may be understood as applying to R&D or to open source developments. FI: (Comments): It could be considered to introduce a definition of 'a manufacturer'. Alternatively, it could be clarified what is the relation of 'a manufacturer' to 'a provider'.

	ES: (Comments): Re-number definitions.
(3) 'small-scale provider' means a provider that is a micro or small enterprise within the meaning of Commission Recommendation 2003/361/EC[2];	PL: (Comments): support DK: (Comments): We are still questioning why this does not reflect the Commission Recommendation 2003/361/EC in its entirety. This is also relevant in subsequent articles, for example article 55 which in our view should be extended to SMEs. SE: (Drafting): (3) 'small-scale provider' means a provider that is a micro or small or medium enterprise within the meaning of Commission Recommendation 2003/361/EC[3];

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

	SE: (Comments): It is our understanding that start-ups are covered within this definition. If not, we would like further adjustments to include start-ups. FI: (Comments): FI supports the idea that SME's should be more supported during digital transformation. FI supports the objective of the proposed regulation to support SMEs through the establishment of regulatory sandboxes and testing and experimentation facilities, but highlights that the scope of the regulation and the obligations of different operators should be clearly defined in the act. The equal treatment of different operators should be ensured.
	PL: (Comments): "start-up company" appears next to the entity referred to as "small scale-provider". It is therefore appropriate to include the term "start-up" in the definition of "small scale-provider" or as a minium made note.

(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;	PT: (Drafting): PL: (Drafting): a personal ~~non-professional~~ activity PL: (Comments): keeping 'non-professional' creates risk of coverage professional activate but in different scope of where individualised AI system is used. For example: lectures, advising or home service as a secondary work. **DELETED**

	DELETED SK: (Comments): **SK**: See above comments to article 2. Notwithstanding the issue of non-professional users, Slovakia also believes that a new and distinct category (definition) needs to be created for a wider category of *all* persons directly or indirectly affected by deployment and use of AI systems as the proposed definition of user does not cover these. The notion of "consumer" or "end-user", as currently used in EU law, may be too narrow for protection of these affected persons. See also comments to article 9 below. FR: (Comments): It might be appropriate for the Commission to clarify the envisaged cumulative application of the different definitions provided for in the AI Regulation and in the Medical Devices Regulation, in particular. Indeed, FR has underlined an additional remark concerning the discrepancies between the definitions of "*user*"

	and "*operator*" in both of the regulations on AI and MD, which can result in making impossible a "cumulative" application of the requirements of these two regulations for operators, as initially envisaged by the Commission. The definition of "*user*" in this proposal excludes the layman. However, the Medical Devices Regulation includes this difference between two definitions, but this deifference is not taken into account in this proposal. Thus in AI Regulation: "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 context of a personal non-professional activity. In DM Regulation: "*user*" is any health professional or lay person who uses a device. In DM Regulation, "*economic operator*" means a manufacturer, agent, importer, distributor or the person referred to in Article 22(1) and 22(3).
	PL: (Drafting): 'end-user' means natuarl person interacting with AI system in the course of professional activity and personal activity who are not provider or user. PL: (Comments): "end-user" should be excluded from the definition of a user for a separate definition of the so-called end

	user: not only the client, consumer, but e.g. a doctor, judge or firefighter who uses an artificial intelligence system, and who is not subject to its supervision only by the organization in which he is employed or operates on the basis of a system provided by the supplier or operator; these concepts should be separated and a different risk assessment grid created
(5) 'authorised representative' means any natural or legal person established in the Union who has received a written mandate from a provider of an AI system to, respectively, perform and carry out on its behalf the obligations and procedures established by this Regulation;	PL: (Drafting): 'authorised representative' means any natural or legal person domiciled or established in the Union who has received and approved a written mandate from a provider of an AI system who has a seat or branch outside of the UE to, respectively, perform and carry out on its behalf the obligations and procedures established by this Regulation for providers; **DELETED** .

(6) 'importer' means any natural or legal person 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;	PL: (Drafting): 'importer' means any natural or legal person domiciled 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	PL: (Comments): support BE:

the importer, that makes an AI system available on the Union market without affecting its properties;	(Comments): In the Dutch version of the text, there is a mistake in the translation. See: *"distributeur": een andere natuurlijke persoon of rechtspersoon in de toeleveringsketen dan de aanbieder of de importeur, die een AI-systeem in de Unie ~~in de handel brengt~~ op de markt aanbiedt zonder de eigenschappen hiervan te beïnvloeden.*
(8) 'operator' means the provider, the user, the authorised representative, the importer and the distributor;	PL: (Comments): should be excluded from the definition of operator an end-user such as a customer, consumer, judge, physician or public servant. It works if approved is a addition of the definition of end-user above (after point 4) FR: (Comments): This proposal includes the definition of users. It's not the case in Medical Devices Regulation, as there is a distinction between operators and users. IA Regulation: "*operator*" means supplier, user, authorized representative, importer and distributor.

	FI: (Comments): The obligations imposed on producers, importers, distributors and users of artificial intelligence systems and the roles and responsibilities of the various actors must be clear. In addition, it is necessary to assess the extent to which knowledge and information on the content of legislation can be required from different actors. Attention must also be paid to the different size of the operators and to the actual opportunities to fulfill the obligations imposed.
(9) 'placing on the market' means the first making available of an AI system on the Union market;	PL: (Drafting): 'placing on the market' means the first making available of an AI system on the Union market, excuding transparent and auditable tests, experimentation or science research under the sand boxes rules; PL: (Comments): that addition creates an for the EU to build solid and auditable agile open for innovation legal framework **DELETED**

	DELETED SK: (Comments): **SK:** It needs to be considered whether the notion properly reflects practical varieties of production and dissemination of software.
(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	PL: (Comments): support SK: (Comments): **SK:** It needs to be considered whether the notion properly reflects practical varieties of production and

activity, whether in return for payment or free of charge;	dissemination of software. **DELETED**
(11) 'putting into service' means the supply of an AI system for first use directly to the user or for own use on the Union market for its intended purpose;	PL: (Comments): support **DELETED** SK: (Comments): **SK**: It needs to be considered whether the notion properly reflects practical varieties of production and dissemination of software.

(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;	PL: (Comments): support SK: (Comments): **SK**: The notion of "intended purpose" does not necessarily suit all the complex, dynamic and evolving value chains in AI. In other words, it is not clear whether the provider of AI system is always able to specify the intended purpose with the required clarity, as there may be instances where this can be done only "downstream", i.e. by the user. Even if we use the concept of intended use for the purpose of setting clearly the obligations and liabilities, such construction may not reflect the complexities of value chains. Innovative approaches to (collective and individual) liabilities and responsibilities seem to be necessary, going beyond one single person being liable. Last but not least, the possibilities under article 29 (2) for MSs to impose additional obligations on users do not represent an adequate solution to this problem, as this increases the risk of internal market fragmentation and divergent approaches in MSs in this important matter. Finally, if open-source tech companies/libraries and "general purpose" software were intended to be

	excluded from the scope of the regulation (and from the notion of provider) due to the fact that the intended purpose cannot be defined in such situations, this should be clearly stated in the text of the regulation. **DELETED** EE: (Comments): Some of the new systems may not have 'intended purpose'. Please replace 'intended purpose' with 'foreseeable use' using the same logic as in the proposal for the GPSR to make it more future proof. Alternatively, please use 'intended purposes' instead of 'intended purpose' or make sure multiple purposes are covered. New systems (such as Microsoft's Generative Pre-trained Transformer 3 (GPT-3)) already have many potential purposes instead of one specific, and this should be taken into account when setting requirements.
(13) 'reasonably foreseeable misuse'	PL: (Drafting):

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;	in a way that is not in accordance with its intended purpose not possible to be improved in usage in the sandboxes, SK: (Comments): **SK:** See comments above regarding the notion of "intended purpose". **DELETED** EE: (Comments): Please connect the meaning of 'reasonably foreseeable misuse' with 'foreseeable use' instead of the 'intended purpose' for the reasons mentioned above. If the use is reasonably foreseeable, the product should not cause harm, whether or not the use was in accordance with the original purpose (please see our comment about (23)). ES: (Drafting):

	(13) 'reasonably foreseeable misuse' means the use of an AI system, different from general purpose AI systems or those released under open source schemes, 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; ES: (Comments): It is impossible to cover all reasonable misuse when it comes to general purpose models that will be used by a myriad of providers.
	ES: (Drafting): (14) 'subliminal technique': the use of images, messages or other emotion triggers that, conveying a messages, have the possiblitity to influence the minds of the person interacting with the AI system, withouth them being fully aware of such use. (15) 'Materially distort a person's behaviour': practices that appreciably impair the persons behaviour when interacting with a certaing AI system, causing that persons to take decissions or actions that would not have taken otherwise.
(14) 'safety component of a	PL:

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;	(Comments): support **DELETED**
(15) 'instructions for use' means the information provided by the provider to inform the user of in particular an AI system's intended	PT: (Comments): We propose to clarify the definition "instructions for use" given the fact that we believe that this definition creates legal uncertainty regarding its scope. The "instructions for use" appear to be only applicable to "high risk AI" systems when these are useful and desirable for all AI systems as they are for other types of

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;	software. PL: (Drafting): 'instructions for use' means the information provided by the provider to inform the user of in particular an AI system's intended purpose and its proper use, ~~inclusive of the specific geographical, behavioural or functional setting within which the high-risk AI system is intended to be used~~ and any precationaty measures to be taken; PL: (Comments): make it more simple and referred to not only high-risky AI systems **DELETED**

	DELETED
(16) 'recall of an AI system' means any measure aimed at achieving the return to the provider of an AI system made available to users;	PL: (Comments): support EE: (Comments): Technically, such choice of words may not be correct for the software and can make it harder to meet the requirement in practice. The same objective can be achieved more effectively by requiring the system to be deactivated immediately and remotely.
(17) 'withdrawal of an AI system' means any measure aimed at	PL: (Comments):

preventing the distribution, display and offer of an AI system;	support
(18) 'performance of an AI system' means the ability of an AI system to achieve its intended purpose;	PL: (Drafting): 'performance of an AI system' means the ability of an AI system to achieve its intended purpose adecuate of AI technics' PL: (Comments): the definition of "artificial intelligence system performance" as meaning the ability of an artificial intelligence system to function as intended seems of little use. Machine learning models, whether they are designed for classification or regression, always have a specific measure used to evaluate the model. Always such a measure is ultimately expressed as a certain percentage of effectiveness. Whether the model is "effective" and thus useful for a specific prediction is assessed individually and subjectively, often by comparing with the currently existing "traditional" solutions.

	DELETED
(19) '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	PL: (Comments): Support

monitoring;	
(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;	PL: (Comments): support
(21) 'conformity assessment body' means a body that performs third-party conformity assessment activities, including	PL:

testing, certification and inspection;	(Comments): support
(22) 'notified body' means a conformity assessment body designated in accordance with this Regulation and other relevant Union harmonisation legislation;	PL: (Comments): support
(23) 'substantial modification' means a change to the AI system following its placing on the market	PT: (Comments): We believe this term needs further clarification. PL:

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;	(Comments): support **DELETED** EE: (Comments): Please connect the meaning of 'reasonably foreseeable misuse' with 'foreseeable use' instead of the 'intended purpose' for the reasons mentioned in our comment related to definitions (12) and (13). If the use is reasonably foreseeable, the product should not cause harm, whether or not the use was in accordance with the original purpose, i.e. prior to modification. DK:

	(Drafting): (23) 'substantial modification' means a change to the AI system following its placing on the market or putting into service which is not foreseen by the provider and 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; DK: (Comments): The definition of substantial modification is essential in order to take into account the specificities of AI. However, it should clearly specify that a substantial modification is a modification which has not been foreseen by the provider. This aspect is already reflected in article 43, paragraph 4, but the definition should also contain this aspect in order to exclude modifications which have been pre-defined by the provider. Furthermore, an accompanying recital should stipulate the benchmarks for when a modification would qualify as being substantial. In our view, it would not entail a software update nor training on new data. This should also clarify – as set out in other existing legislation - that in order to avoid an unnecessary and disproportionate burden, the substantial modification should not require to repeat tests and produce new documentation in relation to aspects of the system that is not impacted by the modification. Thereby, a substantial modification should not place providers completely at the starting line in terms of conformity assessment, but should take into account already assessed elements, thereby limiting the procedure.

	ES: (Drafting): (23) 'substantial modification' means a change to the AI system or a change in its training process, 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 ~~assesed~~ designed, leading to a new high-risk AI system; ES: (Comments): For more clarity and not to be confused with 'conformity assessment'. SE: (Comments): There should be no room for ambiguity about what constitutes a substantial modification.
(24) 'CE marking of conformity' (CE marking) means a	PL: (Comments):

marking by which a provider indicates that an AI system is in conformity with the requirements set out in Title III, Chapter 2 of this Regulation and other applicable Union legislation harmonising the conditions for the marketing of products ('Union harmonisation legislation') providing for its affixing;	But under condition of mutual recognition. Red line.
(25) 'post-market monitoring' means all activities carried out	PL: (Comments):

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;	support **DELETED**
(26) 'market surveillance authority' means the national authority carrying out the activities and	PL: (Comments): support SK:

taking the measures pursuant to Regulation (EU) 2019/1020;	(Comments): **SK:** The definition should be adapted/expanded in such a way so that the MSs can choose other national authorities than those listed in Regulation (EU) 2019/1020 for supervision of stand-alone systems mentioned in Annex III. The market surveillance authorities under regulation (EU) 2019/1020 are not necessarily suitable for that purpose, as confirmed also by art. 63 (3) and (5).
(27) 'harmonised standard' means a European standard as defined in Article 2(1)(c) of Regulation (EU) No 1025/2012;	PL: (Comments): support
(28) 'common specifications' means a document, other than a standard, containing technical solutions	PL: (Comments): support **DELETED**

providing a means to, comply with certain requirements and obligations established under this Regulation;	**DELETED** EE: (Comments): EE would like to understand whether the „common specifications“ could include a health, safety and fundamental rights risk/impact assessment model.
(29) ‘training data’ means data used for training an AI system through fitting its learnable parameters, including the weights of a neural network;	PL: (Comments): support **DELETED** SE:

	(Comments): All data will become training data when the system is in use. An AI system will continously become better and better based on the data used. Now training data could be interpreted as data used initially to train the system.
(30) 'validation data' means data used for providing an evaluation of the trained AI system and for tuning its non-learnable parameters and its learning process, among other things, in order to prevent overfitting; whereas the validation dataset can be a separate dataset or part	PL: (Comments): supprt

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;	PL: (Comments): support
(32) 'input data' means data provided	PL:

to or directly acquired by an AI system on the basis of which the system produces an output;	(Comments): support
(33) 'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person,	PL: (Comments): point 33 "biometric data" - deletion of the definition and reference should be considered in the scope of this concept to biometric data contained in art. 4 point 14) of the General Data Protection Regulation, and organically comply with the derogation standard set out in recital 7. DK: (Comments): As a purely technical remark, this is the same definition as in the GDPR, and as we do not want to end up with conflicting definitions, there should just be a clear reference to the definition set out in the GDPR.

such as facial images or dactyloscopic data;	
	AT: (Comments): It is important to detach the definitions of 'emotion recognition system' and 'biometric categorisation system' from the definition of 'biometric data', which has been copied from the GDPR and requires that the data allow or confirm the unique identification of a natural person. Emotion recognition and biometric categorisation, however, do not (necessarily) rely on personal data that allow or confirm the unique identification of a particular individual. It is therefore recommended to introduce a separate definition of 'biometrics-based 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;	PL: (Comments): support AT: (Drafting): (34) 'emotion recognition system' means an AI system for the purpose of identifying or inferring emotions, thoughts or intentions of natural persons on the basis of their ~~biometric~~ biometrics-based data;

	EE: (Drafting): (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~~ **data relating to their physical, physiological or behavioural characteristics**;
(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, ethnic origin or sexual or political orientation, on the basis of their	PL: (Comments): support AT: (Drafting): (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, ethnic origin, health, mental ability, personality traits or sexual or political orientation, on the basis of their ~~biometric~~ biometrics-based data; EE:

biometric data;	(Drafting): (35) 'biometric categorisation system' means an AI system **that uses data relating to the physical, physiological or behavioral characteristics of a natural person** for the purpose of assigning natural persons to specific categories ~~such as sex, age, hair colour, eye colour, tattoos, ethnic origin or sexual or political orientation, on the basis of their biometric data~~ **which can be reasonably inferred from such 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 data with the biometric data	PT: (Comments): In our opinion, it is also unclear the scope of this definition. The use of this system can pose risks to fundamental rights but can also have positive social benefits, such as monitor health and safety. Consequently, we recommend clarifying certain aspects to enable positive uses of this system. Further, it is not understandable the meaning of identifying natural persons "at a distance", especially taking into account that high risk uses of remote biometric identification cover, not only "real-time" but also "post" identification, and so it raises the doubt as how can the identification be made "after the fact" in any other way other than "at a distance". It seems that the intention was to cover mass surveillance

contained in a reference database, and without prior knowledge of the user of the AI system whether the person will be present and can be identified ;	"where "many people are being screened simultaneously" but the language should be clarified to reflect that intent. Otherwise, commonplace AI systems that identify natural persons at a distance such as smartphones used to identify friends in photos are also regulated under this provision. Moreover, it is also not clear the intention behind the exclusion from the definition "where the "user of the AI system" has "prior knowledge ...whether the person will be present and can be identified." For example, consumers might use their smartphone's AI to find in their photos the faces of family and friends that they trained their device to recognise. In that example, it is unclear who the user of the AI system is. If the consumers are users, they arguably have "prior knowledge" whether the individuals in their contacts or their photo album can be identified by the device. But if the "user of the AI system" is the smartphone or software vendor that designed the AI system for the device, would they have prior knowledge? The language of this article should be clarified in order to not prevent common and beneficial uses of AI to which people would be willing to consent, if given the appropriate opportunity." PL: (Comments): support **DELETED**

	DELETED AT: (Drafting): (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 data with the biometric data contained in a reference database, and without the conscious cooperation of the persons to be identified ~~prior knowledge of the user of the AI system whether the person will be present and can be identified~~ ; DK:

	(Comments): We would like to clarify the meaning of "at distance" in order to reflect that biometric authentication/verification/closed set identification as well as a controlled environment would not classify as being remote biometric identification. SE: (Comments): "reference database" restricts the definition, excluding other possible alternatives
(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	PL: (Comments): support **DELETED** AT:

without a significant delay. This comprises not only instant identification, but also limited short delays in order to avoid circumvention.	(Drafting): (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 on a continuous or large-scale basis over a period of time and without limitation to a particular past incident; ~~without a significant delay. This comprises not only instant identification, but also limited short delays in order to avoid circumvention.~~ AT: (Comments): It is also important to modify the notion of ‘real-time’ in the context of remote biometric identification because the pivotal point is not so much the duration of delay between capturing of live templates and identification but rather whether identification occurs on a large scale over a period of time. Where this is not the case and identification is just limited to a particular past incident, such as a crime captured by a video camera, we may not need the same strict regulation as for real-time remote identification. SE: (Drafting): (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 without a significant delay. ~~This comprises not only instant identification, but also limited short delays in order to~~

	~~avoid circumvention.~~ SE: (Comments): Inappropriate wording.
(38) ‘‘post’ remote biometric identification system’ means a remote biometric identification system other than a ‘real-time’ remote biometric identification system;	PL: (Comments): support
(39) ‘publicly accessible space’	PL:

means any physical place accessible to the public, regardless of whether certain conditions for access may apply;	(Comments): It is worth to add also a definition of "virtuall accessible space" where harms also can be done. **DELETED** SK: (Comments): **SK:** Given the importance of virtual digital platforms for peoples´ (public) collective interactions, it is suitable to expand the definition of "publicly accessible space" also to "virtual" places, or create a separate definition of "virtual space" for that purpose. **DELETED**

	DELETED ES: (Drafting): (39) 'publicly accessible space' means any physical place accessible to the public, ~~regardless of whether certain conditions for access may apply~~ either if it is privately or publicly owned; ES: (Comments): Maybe a simpler explanation on the definition helps for a better understanding. For example, recitals seem clearer in this point.
(40) 'law enforcement authority' means:	SK: (Comments): **SK:** The "execution of criminal penalties" should not be covered in the definition of law enforcement authorities and a separate, possibly more nuanced regime for a provision and use of AI systems should be provided in the regulation for penitentiary facilities.

(a) any public authority competent for 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; or	PL: (Comments): support
(b) any other body or entity entrusted by Member State law to exercise public	PT: (Drafting): (b) any **national security and intelligence agency** or other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of the prevention, investigation, detection

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;	or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; PT: (Comments): In order to prevent loopholes undermining the prohibition on real-time remote biometric identification, the use of AI systems by national security and intelligence agencies should be specifically included in this provision. PL: (Comments): support
(41) 'law enforcement' means activities carried out	PL: (Comments):

by law enforcement authorities for 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;	support SK: (Comments): **SK:** See comments to subsection 40 above.
(42) 'national supervisory authority' means the authority to which a Member State	PL: (Comments): support

assigns the responsibility for the implementation and application of this Regulation, for coordinating the activities 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;	**DELETED** ES: (Drafting): (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 activities entrusted to that Member State, including those of the different National Authorities, for acting as the single contact point for the Commission, and for representing the Member State at the European Artificial Intelligence Board;

	ES: (Comments): It is important to make it clear what is expressed in the proposed wording: the constellation of involved authorities (national competent authorities, Data protection Agencies, Drug Agencies, etc.) can be broad in different Member States. The National Supervisory Authority must have a mandate for coordinating the activities of other authorities with regards the compliance of this Regulation. Otherwise there is a high risk of double regulation or confusion for companies, who won't know where exactly they should address their issues concerning this regulation (this would include for example, if it was the case, coordination with Data Protection Agencies).
(43) 'national competent authority' means the national supervisory authority, the notifying authority and the market surveillance authority;	PL: (Comments): support **DELETED**

	DELETED FI: (Comments): FI supports Commission's efforts to ensure the current internal market regulation's effective implementation and enforcement, and in principle, supports the application of Market Surveillance Regulation (EU) 2019/1020 to the control of AI systems to ensure consistency of market surveillance procedures, leaving Member States sufficient room for leeway for designating authorities and organizing market surveillance in practice.
(44) 'serious incident' means any incident that directly or indirectly leads, might have led or might lead to any of	EE: (Comments): Inclusion of "might have led or might lead" creates some uncertainty and further clarifications are needed, for example in the recitals. BE:

the following:	(Comments): Can serious damage also be "a serious damage to a person's identity and rights"? For example, in case of "a new (read: wrong) created identity" by the AI system after two identities of two different persons (for example of twins (same name, same date of birth, similarities in biometrics…) are mixed of combined. If this stays unnoticed for a certain time, it can have long term negative effects for the persons: lost data (and lost rights at level of for example social security rights), long term problems of identification, …. It can be important to introduce specific rules about combining 2 files of what seems to be 2 files of one and the same person, for example "never compile 2 files to 1 file" when there are 2 different unique identification numbers, even when all the other data like last name, date of birth, …. are the same. SE: (Comments): The definition of serious incident should be coordinated with the AMR and TCO regulations.
	PL: (Drafting): 'incident' means a malfunction of an artificial intelligence system' Alternative: 'incident' means any event that has a real negative impact on the security, resiliance and trustworthyness

	of the artificial intelligence system PL: (Comments): To consider adding in art. 3 incident definitions (eg "" incident "means a malfunction of an artificial intelligence system"). The definitions should be based on the concepts contained in Decision No 768/2008 / EC of the European Parliament and of the Council of 9 July 2008 to avoid the risk of divergent interpretation. Relatively, the definition of an "incident" should follow the definition of an incident from Art. 4 point 7) of Directive (EU) 2016/1148 of the European Parliament and of the Council of 16 July 2016 on measures for a high common level of security of network and information systems in the territory of the European Union. Analogic proposal could say: "means any event that has a real negative impact on the security of the artificial intelligence system".
(a) the death of a person or serious damage to a person's health, to property or the environment,	PL: (Drafting): the death of a person or serious damage to a person's health, dignity or privacy of end-user, to property or the environment,

	DELETED BE: (Comments): The word "person" seem to cover only natural persons. What about "serious incidents" seriously damaging the property of legal persons, or threatening its existence, e.g.?
(b) a serious and irreversible disruption of the management and operation of critical infrastructure.	CZ: (Comments): CZ suggests adding a definition of "critical infrastructure" in the list since it is needed to make sure that this area is sufficiently circumscribed, for example by making a reference to the annex of the future CER Directive. BE: (Comments): A definition of "critical infrastructure" is needed to make sure this area is sufficiently circumscribed, for

	example by making a reference to the annex of the future CER Directive.
	PT: (Drafting): ”Personal data” means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. PT: (Comments): We propose to include a definition of “personal data” in line with the Regulation (EU) 2017/679 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 (General Data Protection Regulation) given the fact that this concept is used several times in the proposed text and that is included in the text a definition of “biometric data”. **DELETED**

	DELETED FR: (Drafting): **Additional paragraph** **Where a high-risk AI system related to a product, to which the legal acts listed in Annex II, section A apply, and where the same term is also defined in the legal acts listed in Annex II, Section A, both definitions apply.** FR: (Comments): A number of definitions on identical terms included in Regulation 2017/745/EU on medical devices and in Regulation 2017/746/EU on in vitro diagnostic medical devices are different from those mentionned in the present proposal. All these definitions are not contradictory, but which definition applies is not clear for all the actors involved.
Article 4 Amendments to Annex I	**DELETED**

	DELETED CZ: (Drafting): ~~Article 4~~ ~~Amendments to Annex I~~ CZ: (Comments): See comment on Article 3 (1) on the definition of AI system. Whole definition should be part of the normative text and it should be updated by standard procedure by co-legislators. Delegating this power to the Commission would create a significant legal uncertainty and could undermine the competitiveness of EU companies. Unpredictability of the regulation without due legislative process is in direct opposition to the basic principles of the EU law. Simmilar approach was proposed by the Commission in the MiCA proposal and was not adopted by the Council. AT: (Comments):

	We are still sceptical wheather adjustments to the definition of AI that may become necessary after the entry into force of the Regulation can be made by means of a delegated act. Delegated acts may only relate to supplementing or amending "non-essential" provisions in EU basic acts (Art. 290(1) TFEU). As the definition of AI is an essential provision of the Regulation, adaptations should only be made through an ordinary legislative procedure in order to respect the principles of the rule of law and legal certainty and not be introduced or amended at a later stage through delegated acts. EE: (Comments): It should be further assessed whether the Commission should be able to adopt delegated acts to update the list in Annex I as this defines the scope of the regulation. According to the Article 290 (1) TFEU, a legislative act may delegate to the Commission the power to adopt non-legislative acts of general application to supplement or amend certain **non-essential elements of the legislative act**. Further analysis and an assessment by the Council Legal Service is needed as to whether the use of a delegated act to amend these provisions is legitimate to ensure compliance with TFEU Article 290. Consequently, we would prefer that list determining the scope of the regulation are established in the Regulation and not by delegated acts.

	In any case, to ensure compliance with TFEU Article 290, Article 4 should outline specific and limited criteria based on which the list of techniques and approaches listed in Annex I could be updated. FI: (Comments): FI notes that the purpose of the amendments is to ensure that the regulation is future-proof, however, notes that the scope of the Regulation should not be dependent on delegated acts, and the proposed powers should be narrowed down or removed.
The Commission is empowered to adopt delegated acts in accordance with Article 73 to amend the list of techniques and approaches listed in Annex I, in order to update that list to market and	PL: (Drafting): ~~The Commission is empowered to adopt delegated acts in accordance with Article 73 to amend the list of techniques and approaches listed in Annex I, 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~~. PL: (Comments): If the purpose of the act is to ensure uniform conditions for the implementation of legally binding EU acts,

technological developments on the basis of characteristics that are similar to the techniques and approaches listed therein.	the form of the implementing act is preferred, not the delegated act (see Reg. 182/2011). The proposed provision seems to be inconsistent with Art. 290 TFEU. The essential elements of EU normative acts cannot be regulated in the form of delegated acts (cf. Article 290 TFEU). It is noted that the proposal to use the form of a delegated act in the draft regulation results only from the fact that these issues were included in the regulation in the form of an annex (although elevated to a normative rank). The disclosure of new techniques or ways of using AI systems, as well as their qualification as high-risk systems, should be considered during the ordinary legislative process involving multilateral agreements and respect for the sovereignty of Member States, including their national constitutional orders. **DELETED** SK: (Comments): **SK:** See above general comments to the entire proposal.

	CZ: (Drafting): ~~The Commission is empowered to adopt delegated acts in accordance with Article 73 to amend the list of techniques and approaches listed in Annex I, 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~~ **DELETED** DK: (Comments): As stated in relation to our comments related to the definition of AI, we are still sceptical of amending the definition of AI through a delegated act and would like the opinion of the Council Legal Service in this regard. ES: (Drafting):

	The Commission is empowered to adopt ~~delegated~~ implementing acts in accordance with Article 73 to amend the list of techniques and approaches listed in Annex I, 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. ES: (Comments): Does article 290.1 of TFEU allow the use of a delegated act to ammend annex I, taking into account that the definition (composed of article 3.1 and annex I at the same time) is an essential element of the AIA? On the other hand, it is seen that implementing acts have been used in other laws for big purposes (i.e: art. 57.2 of Electronic Communications Code). We see that for so important changes it would be necessary to take into account MS votes. We are not sure of the viability of an implementing act for this purpose, but it would be worth to explore this or other options. SE: (Drafting): The Commission is under the following conditions empowered to adopt delegated acts in accordance with Article 73 to amend the list of techniques and approaches listed in Annex I if - it has been three or more years since a delegated act in accordance with this article was adopted - and that a qualified majority of the member states formally has asked for a delegated act,

	in order to ~~update that~~ adjust the list to market and technological developments on the basis of characteristics that are similar to the techniques and approaches listed therein.
TITLE II	
PROHIBITED ARTIFICIAL INTELLIGENCE PRACTICES	
Article 5	PL: (Comments): The terms used are so vague that they prevent the effective application of these provisions by both entrepreneurs and public authorities. Additionally, those who may be affected by these practices do not know what practices may not be applicable to them. Therefore, it is necessary to use more precise terms, and even to define some of them (e.g. subliminal techniques). Nevertheless, the recitals of the regulation should include examples of situations where Art. 5 is applicable.

	It should be considered appropriate to take into account in this provision, physical **or mental harm to** the person concerned. In this way, the cognitive nature of the human-machine relationship is emphasized and **the need to protect both human autonomy and his psychi-physical integrity is emphasized.** Article 5 should also take into account other types of sensitivities than those mentioned in it, which would be consistent with the position of the Commission presented, for example, in the Guidelines for the implementation / application of Directive 2005/29, and take into account the violation of economic interests. It is necessary to determine whether Member States may introduce other prohibitions per se or whether this is only possible by amending the regulation (similar to in the case of Directive 2005/29 / EC). In addition, it should be considered whether the issue of the threshold of the "subliminal technique" varies from person to person. If such a threshold is different for different people, it seems important to define the parameters of forbidden subliminal techniques. Otherwise, we doom ourselves to far-reaching regulatory uncertainty SK: (Comments): **SK:** The proposal should explicitly secure issuance of more detailed guidance for interpretation of the prohibitions which may also take into account evolving experiences and practices.

	CZ: (Comments): CZ welcomes general objective and purpose of this Article and supports the aim to protect EU citizens and their rights. However, it will be crucial to clarify especially the exceptions for the purpose of law enforcement, but also other exceptions for the sake of protection of public interests and it should be carefully examined. This relates notably to exceptions which might be needed for the purpose of protection of health and safety and similar. CZ would also welcome any concrete examples which the EC could list in order to clarify which concrete activities are covered by this Article and which are out of scope. The Commission should also prove that the mentioned misuse of AI system is not already covered by the EU legal framework currently in force, especially, in the area of protection of fundamental rights. Otherwise, it could create new and unnecessary barriers for entry to the market and high administrative costs. MT: (Comments): Malta notes that whilst a balance needs to be struck between the lawful use of AI and respect for fundamental rights, we need to ensure that restrictions posed are proportionate and fair.By categorising certain types of AI as 'high risk', for example, AI systems intended to be used for crime analytics to search complex related and unrelated large data, could lead to disproportionate burdens as their use is

	subject to authorisation by a supervisory or regulatory authority. In this sense, law enforcement authorities will be faced with situations where valuable time saved by using AI that processes complex sets of data (which is in any case consequently subject to human oversight) will be consumed instead on extensively justifying its use. DK: (Comments): In general, we are supportive of identifying and having prohibited practices in the exceptional case where a specific use of AI may result in serious, irreparable harm to individuals or society or where the use is inconsistent with applicable law or fundamental rights, and where this cannot be mitigated or addressed in other ways. However, article 5 seems to contain very broad categories of practices. In our view, we need to follow the proportionate, risk-based approach, meaning that we need to define and further delimit these categories in order to only target those practices which can lead to unacceptable risk and which are not adresseed by other means, for example existing legislation. In general, we find that this article deserves further discussion and improvement.
1. The following artificial intelligence practices shall be	PL: (Comments):

prohibited:	. DK: (Comments): As a technical remark, in recital 16, it is stated that research for legitimate purposes should not be stifled by the prohibition, "if such research does not amount to use of the AI system in human-machine relations that exposes natural persons to harm and such research is carried out in accordance with recognized ethical standards for scientific research." We would need to clarify that both embedded as well as non-embedded systems would be covered by this. Furthermore, we find that such exclusion of research activities should not only cover article 5, but should apply in all cases of AI. SE: (Comments): The exemptions should be more precise, to make it clearer what falls outside the prohibited area.
(a) the placing on the market, putting into service or use of an AI system that	PL: (Comments): The provision of art. 5 pts 1 letter a) contains a number of open, ambiguous premises ("weakness of a

deploys subliminal techniques beyond a person's consciousness in order to materially distort a person's behaviour in a manner that causes or is likely to cause that person or another person physical or psychological harm;	specific group", "significant distortion of behavior", "psychological harm"). Their blurring should be removed. The more so as the application of such ambiguous criteria falls under the hypothesis of the provision and is burdened with a significant financial penalty. SK: (Comments): **SK:** The qualifying cumulative condition of "causing or likely causing physical or psychological harm" should be deleted as this does not appear necessary and at the same time is hard to prove. CZ: (Comments): Art. 5 (1) letter (a) foresees that any placing on the market, putting into service or use of an AI system deploying subliminal techniques likely to cause that person or another person physical or psychological harm shall be prohibited. Naturally, any system which targets primarily a person's subconsciousness is questionable and dangerous. Due to these reasons, subliminal advertising methods are already prohibited under the Unfair Commercial Practices Directive and Article 9 (1) (b) of new Audiovisual Media Services Directive 2018/1808/EU (AVMSD) which says that "audiovisual commercial communications shall not use subliminal techniques...". Difference between wording in Article 5 AIA and those two Directives should be explicitly explained in AIA, together with the interplay between those legislative acts. It is also worth considering whether similar sentence from AVMSD would not be more suitable for the purposes of

	Article 5 AIA than what is proposed at the moment. In our view, the description in Article 5 which now reads "that causes or is likely to cause a psychological harm" may cause huge problems while applying in practice. Everyone has different levels of what can cause this person psychological harm and thus, it would be difficult to analyse it in practice. **DELETED** AT: (Drafting): […] in order to materially distort a person's behaviour in a manner that causes or is likely to cause that

	person or another person ~~physical or psychological~~ material and unjustified harm; AT: (Comments): **Art 5 para 1 (a) and (b):** It is recommended to broaden the scope of the three existing *per se*-prohibitions – manipulation by subliminal techniques, exploitation of vulnerabilities and social scoring – in several ways. In particular, it is recommended to replace 'physical or psychological harm' by 'material and unjustified harm', both with the aim of including economic harm and of avoiding overreaching effects. EE: (Drafting): (a) the placing on the market, putting into service or use of an AI system that deploys subliminal techniques beyond a person's consciousness in order to materially distort a person's behaviour **and which intentionally or unintentionally** ~~in a manner that~~ causes or is likely to cause that person or another person physical or psychological harm; EE: (Comments): Causing harm or likelihood of harm should remain a condition in determining whether the pertinent AI systems should be prohibited, but it should not be required that the intention of the provider is to cause harm or likely cause harm to the user or another person, rather only that the intention is to materially

	distort the behaviour of a person. Recital 16 should be amended accordingly. Further consideration should be given to the use of the phrase 'distort' – is that meant to refer to a negative change in person's behaviour? If not, a more neutral wording (e.g. 'affect') should be considered instead. If yes, the notion of negative distortion of person's behaviour should be elaborated further in the article text or the recitals. DK: (Comments): As a technical remark, we find that subliminal techniques should be defined, as it is an essential concept in order to understand this article. BE: (Comments): This Article describes the prohibition of an AI system that deploys subliminal techniques; however, 'subliminal technique' as such is not defined in the Proposal, neither is the cause-and-effect relationship between the applied technique and the harm nor is 'physical or psychological harm'. In this regard, further definition of said terminology is required. ES: (Drafting):

	(a) the placing on the market, putting into service or use of an AI system that deploys subliminal techniques beyond a person's consciousness in order to materially distort a person's behaviour in a manner that causes or is **reasonably** likely to cause that person or another person physical or psychological harm; ES: (Comments): Likely to 'reasonably likely' substitution-> the term is quite open otherwise. We understand how difficult is to be concrete in these cases, but this may be somehow narrower. SE: (Drafting): (a) the placing on the market, putting into service or use of an AI system that deploys subliminal techniques beyond a person's consciousness in order to materially distort a person's behaviour in a manner that causes or is likely to cause that person or another person physical, material or psychological harm; SE: (Comments): Material harm are meant to also include financial harm.

	Subliminal techniques should be more clearly defined, possibly in the recitals.
(b) the placing on the market, putting into service or use of an AI system that exploits any of the vulnerabilities of a specific group of persons due to their age, physical or mental disability, in order to materially distort the behaviour of a person pertaining to that group in a manner that causes or is likely to cause that	PL: (Comments): In the case of Item 1 b), it is worth paying attention to the possible consequences of overprotection, which may lead to discrimination, e.g. due to age and reliance, e.g. failure to propose certain products by the recommendation system based on the artificial intelligence system, which may consequently lead to exclusion of such persons on the basis of age, which should be a prohibited practice. It should also be noted that the artificial intelligence system does not need to know the characteristics of the people who use it, as indicated in this point. Therefore, a question arises whether such confidential information as, for example, disabilities should be known to the artificial intelligence system in order to protect such a group of people, or whether a person using AI should be able to define features that, according to him, should be subject to special protection, because automatic and mechanical protection on the basis of the indicated features may be in conflict with other laws. SK:

person or another person physical or psychological harm;	(Comments): **SK:** The qualifying cumulative condition of "causing or likely causing physical or psychological harm" should be deleted as this does not appear necessary and at the same time is hard to prove. CZ: (Comments): The same as for the letter (a) applies to letter (b) of Article 5 (1). Any examples of practical implementation of these two letters would be welcomed, notably with regard to already existing Union law which covers prohibition of use of sector specific techniques which may lead to physical or psychological harm, such as the Article 9 (1) of the AVMSD. These examples should be mentioned in the recitals. AT: (Drafting): (b) the placing on the market, putting into service or use of an AI system that exploits any of the vulnerabilities of i) a specific group of persons due to their age, ~~physical or mental~~ intellectual disability or social or economic situation; or ii) an individual whose vulnerabilities are characteristic of that individual's known or predicted

	personality or social or economic situation ~~in order to materially distort the behaviour of a person pertaining to that group~~ in a manner that causes or is likely to cause that person or another person ~~physical or psychological~~ material and unjustified harm; AT: (Comments): "Physical or mental" should be deleted in order to cover all kinds of disabilities and thus comply with Article 1 para 2 of the Convention on the rights of persons with disabilities. It is likewise recommended to extend the prohibition of exploitation of vulnerabilities from group-specific vulnerabilities to individual vulnerabilities, e.g. very individual personality traits discovered with the help of data analytics. According to Studies also mandated by the Commission it seems obvious, that everybody can become vulnerable in specific situations. EE: (Drafting): (b) the placing on the market, putting into service or use of an AI system that exploits any of the vulnerabilities of a specific group of persons due to their age, physical or mental disability, in order to materially distort the behaviour of a person pertaining to that group **and which intentionally or**

	unintentionally ~~in a manner that~~ causes or is likely to cause that person or another person physical or psychological harm; EE: (Comments): See (a). DK: (Comments): ES: (Drafting): (b) the placing on the market, putting into service or use of an AI system that exploits any of the vulnerabilities of a specific group of persons due to their age, physical or mental disability, in order to materially distort the behaviour of a person pertaining to that group in a manner that causes or is reasonably likely to cause that person or another person physical or psychological harm; SE: (Drafting):

	(b) the placing on the market, putting into service or use of an AI system that exploits any of the vulnerabilities of a specific group of persons due to their age, physical or mental disability, in order to intentionally and materially distort the behaviour of a person pertaining to that group in a manner that causes or is likely to cause that person or another person physical, material or psychological harm; SE: (Comments): Add the term "intentionally" to limit to AI-systems or services that has an intention to do physical or psychological harm. This reduces the risk that AI-regulation also includes Social media, for instance.
	AT: (Comments): **Art 5 para 1 (ba) and (bb):** in terms of AI practices missing in the list of prohibited practices, it is recommended to add total surveillance and violation of mental privacy and integrity
(c) the placing on the market, putting	PL: (Comments):

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:	support **DELETED** SK: (Comments): **SK:** Slovakia does not see a legitimate and justified purpose why the proposed prohibition should not apply also to private operators. Moreover and in any case, the proposal does not seem to be consistent as it enables public authorities to obtain outputs of AI systems – which they themselves would not be able to achieve – from private operators. Adequate safeguards should be included in this respect. AT:

	(Drafting): (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 […] AT: (Comments): **Art 5 para 1 (c):** the restriction to public authorities in the prohibition of social scoring is too narrow and should be extended to social scoring conducted by private actors, e.g. by a provider of a gatekeeper platform service. EE: (Comments): We are still analyzing this provision and we might later have proposals for amendments here. BE: (Comments): Regarding 'social scoring', further clarification about the practices that fall under the prohibition on general citizen scoring would be welcomed, as the language that is currently used in the AIA and the examples provided by the Commission in its presentations, are not always sufficiently clear. FI:

	(Comments): The concept of social scoring is unclear and requires further clarification.
(i) detrimental or unfavourable treatment of certain natural persons or whole groups thereof in social contexts which are unrelated to the contexts in which the data was originally generated or collected;	CZ: (Comments): This article should be more precise, vague formulation could cover a broad range of AI applications that aims not to harm but rightfully distinguish customers. AT: (Drafting): ~~(i) detrimental or unfavourable treatment of certain natural persons or whole groups thereof in social contexts which are unrelated to the contexts in which the data was originally generated or collected;~~ AT: (Comments): It is suggested that the two sub-paragraphs in lit c) be deleted and that only the criteria of disadvantage and discrimination be stipulated as conditions. ES:

	(Drafting): (i) detrimental or unfavourable treatment of certain natural persons or ~~whole~~ groups thereof in social contexts which are unrelated to the contexts in which the data was originally generated or collected; ES: (Comments): 2. 'whole' has been deleted. When talking about groups we understand that this may include the whole group.
(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;	CZ: (Comments): This article should be more precise, vague formulation could cover a broad range of AI applications that aims not to harm but rightfully distinguish customers. AT: (Drafting): ~~(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;~~

	ES: (Drafting): (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 for the purpose of law enforcement, unless and in as far as such use is strictly necessary for one of the following objectives:	PL: (Comments): support **DELETED** SK: (Comments):

	SK: Biometric categorisation systems and emotion recognition systems should be included in the provision because state-of the-art of these technologies does not appear to guarantee adequate reliability for now and, at the same time, are very sensitive and intrusive. Additionally, given the nature of technology and doubts about current tools of effective enforcement of legal rules in cyberspace, it is important to consider possible moratorium, a temporary complete ban on the use of "real time" biometric identification systems in publicly accessible spaces for the purpose of law enforcement. Slovakia does not see a legitimate and justified reason why the prohibition/restricted use should not apply also to private operators. Moreover and in any case, the proposal does not seem to be consistent as it enables public authorities to obtain outputs of AI systems – which they themselves would not be able to achieve – from private operators. Adequate safeguards should be included in this respect. CZ: (Comments): Recital 12 of the LED (2016/680) includes within the scope of the LED also activities of the law-enforcement authorities without prior knowledge if an incident is a criminal offence or not. The Commission explained that the proposal relates to "pure" law enforcement activities. This should be further explained, for example by stipulating in Recital 19 that only situations where the law enforcement

	purpose is clear at the time of application of AI are covered by the prohibition in Article 5(1)(d). AT: (Drafting): (d) the use of ~~'real-time'~~ remote biometric identification systems in publicly accessible spaces ~~for the purpose of law enforcement,~~ *[to be moved to a new Art. 5a]* AT: (Comments): It is unclear why post remote biometric identification is less harmful then real-time remote biometric identification. Recital 8 does not provide an explanation for the differentiation. It only states that real-time remote identification is more intrusive. From a data protection standpoint the processing of biometric data by means of analysing collected and retained surveillance material is similarly intrusive. It is unclear why remote biometric identification in public spaces should only be prohibited if it is done for the purpose of law enforcement. Surely remote biometric identification in public spaces for private/commercial purposes is eaqually intrusive and should generally be prohibited. Only the exemptions of the prohibition should refer to specific cases for the purpose of law enforcement.

	EE: (Comments): General comments: - We prefer a separate legal act for law enforcement with regards to AI. The related recital (33) should be amended as follows: "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. **Furthermore, the very use of remote biometric identification systems entails a serious interference in the right to respect for private and family life and the right to protection of personal data of all persons, among other fundamental rights.** Therefore, 'real-time' and 'remote post' biometric identification systems should be classified as high-risk. In view of the risks that they pose, both types of remote biometric identification systems should be subject to specific requirements on logging capabilities and human oversight." DK: (Comments): It is essential that the Danish opt-out on justice and Home Affairs is clearly respected in the regulation. Therefore, recital 26 should be extended to also cover article 5, paragraph 4. BE:

	(Comments): Belgium confirms that the use of real-time biometric identification by law enforcement in public spaces is a sensitive matter; however, taking into account the joint-opinion of the EDPB and the EDPS on the AIA of 18 June 20212, we believe that a more general ban on any use of AI for a 'real-time' automated recognition of human features in publicly accessible places should be incorporated in the AIA. In that sense, it should be closely examined if the actual choice to prohibit such a type of identification by law enforcement and provide for a system of exceptions is a workable and effective manner. In any case, we believe that other specific alternatives regarding possible exceptions should be analysed, e.g. providing a list with sufficient and concretely defined exceptions under realistic conditions, in particular for law enforcement objectives. ES: (Comments): Some discussions have risen in this regard: it seems that technological neutrality may not be fully respected here. There are other RBI systems in real time for law enforcement in public spaces that don't use AI and may have similar potential risks. It would be useful to discuss the justification of this choice. **DELETED**

	DELETED SE: (Comments): The writing implies stricter regulation on the use of 'real-time' remote biometric identification systems for LEA than for others, e.g., private users. This may result in an imbalance between the capabilities between private enterprises and LEA. LEA should have at least the same possibilities as private users, and preferably an increased mandate to use AI to identify, prohibit, and investigate crime. FI: (Comments): Please clarify the relationship to the Law Enforcement Directive 10 Art.
(i) the targeted search for specific potential victims of crime, including missing children;	CZ: (Drafting): (i) the targeted search for specific potential victims of crime, ~~including missing children;~~ search for witness of criminal offence or absconding convicted offender; CZ:

	(Comments): The Commission explained at the technical workshops that only missing children who are potential victims of crime are covered by this exception. The wording is however misleading. If only missing children as potential victims of crime are covered, it would be clearer to delete the text "including missing children" (as in such case all missing persons who are potential victims of crime are covered by this provision). Moreover, to enable more effective law enforcement, the circle of persons in relation to whom AI tools could be used should be extended to include at least also witnesses of criminal offences or offenders in enforcement proceedings (in case of absconding after conviction). CZ does not intend to extend the current legal framework for the law enforcement identification of persons. However, we believe that where legal basis for the identification of persons already exists, the future use of emerging technologies should not be limited right from the beginning. EE: (Drafting): the targeted search for specific potential victims of crime, including missing children **or vulnerable persons**; EE:

	(Comments): It should be possible to use RBI also in search for missing children when no credible info is available (yet) of potential crime. It should also be possible to use RBI in search for example, persons with mental problems. ES: (Drafting): (i) the targeted search for specific potential victims of crime, including missing children or other vulnerable groups, such as gender-based violence victims, people with disabilities or elderly people; ES: (Comments): The use of 'other vulnerable groups' should be also included here, as it was done in previous paragraphs.
(ii) the prevention of a specific, substantial and imminent threat to the life or physical safety	CZ: (Drafting): (ii) the prevention of a specific, substantial ~~and imminent~~ threat to the life or health or physical safety of natural persons or of a terrorist attack;

of natural persons or of a terrorist attack;	CZ: (Comments): The requirement that a threat be "imminent" makes deployment of the real-time RBI system impractical for true prevention purposes. Once a threat is imminent, prevention is seldom achieved by remote identification systems. The protections of "health" might be included under physical safety. However, we propose that this is stated clearly in the text. ES: (Comments): -As a general comment: even though the objective to be covered is obvious, the wording may generate confussion: the inminence of a terrorist attack may be measured within days and in other situations, within months, creating uncertainty to law enforcement authorities. -Would not a terrorist attack be included in the concept of threat to the life? FR: (Comments): Ongoing work by FR experts

	SE: (Drafting): (ii) the prevention of a ~~specific, substantial and imminent~~ threat to the life or physical safety or health of natural persons or of a ~~terrorist~~ antagonistic attack; SE: (Comments): Pending final text of art. 2 Specific attack is a very limited situation, the technology must be able e to be used to discover threat- not just after the fact. Terrorist attacks is a matter of definition often made after the event.
(iii) the detection, localisation, identification or prosecution of a perpetrator or suspect of a criminal offence referred to in Article 2(2) of Council	CZ: (Drafting): (iii) the detection, localisation, identification or prosecution of a perpetrator or suspect of a criminal offence ~~referred to in Article 2(2) of Council Framework Decision 2002/584/JHA3 and~~ punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least three years, as determined by the law of that Member State. CZ:

Framework Decision 2002/584/JHA[4] and punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least three years, as determined by the law of that Member State.	(Comments): We do not find the reference to the list of criminal offences established in the Framework Decision on EAW appropriate. This list was drafted under different circumstances (as an agreement/compromise related to cross-border cooperation of MSs in criminal matters) and is not suitable to decisions regarding deployment of certain systems in national context. There are certainly very important serious crimes that are not on the EAW list, for example intentional damage to water dam or to electricity distribution which endangers people and property on large scale. In the Czech legal context, this behavior amounts to the criminal offence of "intentionally causing public danger", which is similar to terrorist attack but lacks terrorist intent. When raised at the workshop, the Commission explained that the list in Art. 2(2) EAW was used as there was already an agreement. In fact, several different such lists now exist in EU law. More importantly, the determination of serious offences will mostly apply within territory of relevant Member State, so it should be based on gravity of the offence. EE:

[4] 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).

	(Drafting): (iii) the detection, localisation, identification or prosecution of a perpetrator or suspect of a criminal offence ~~referred to in Article 2(2) of Council Framework Decision 2002/584/JHA[5] and~~ punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least three years, as determined by the law of that Member State. EE: (Comments): The list in the Council Framework Decision (2002/584/JHA) relates to the objectives of EU cooperation and not necessarily to the seriousness of the crime. For example, counterfeiting of means of payment is rather meaningless in this list, while e.g. crimes against the state are not included. ES: (Drafting): Review criminal offences for justifying the use of RBI. It might be necessary to include a more precise list, where serious crimes are not left while some others don't seem serious enough to activate RBI use. ES:

[5] 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).

	(Comments): Article 2.2 of the Framework Decission 2002/584/JHA, includes some reasonable crimes to activate RBI systems. Other crimes under that article, such as 'computer-related crimes', 'fraud' or 'facilitation of unauthorised entry and residence' don't seem serious enough to activate RBI. At the same some serious crimes are not covered by article 2.2 of the Framework Decission, namely: - Sexual abuse - Abuse in the family environment - child abduction SE: (Drafting): (iii) the detection, localisation, identification or prosecution of a perpetrator or suspect or the prevention or disruption of a criminal offence referred to in Article 2(2) of Council Framework Decision 2002/584/JHA[6] and punishable in the Member State concerned by a custodial sentence or a detention

[6] 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).

	order for a maximum period of at least three years, as determined by the law of that Member State. SE: (Comments): Article 2(2) of the Council Framework Decision 2002/584/JHA, the EAW, deals with serious crimes. Unless new technology such as remote biometric identification in real time can be used in order to prevent or disrupt such crime there will be a lacunae between the prevention of imminent risks and addressing a completed crime. Sweden therefore finds it justified to develop the purposes for which remote biometric identification in real time can be used also in order to prevent the EAW-crimes referred to and to disrupt them.
	CZ: (Drafting): (iv) the prevention of an intentional criminal offence punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least three years, as determined by the law of that Member State, within security-sensitive public spaces. CZ: (Comments): The Commission explained at the technical workshops that a closed secure zone at the airport would not

	be covered by the prohibitions of RT RBI systems, while those parts of the airports which are publicly accessible would be covered by the prohibitions. CZ believes that use of AI systems in security-sensitive public spaces, such as parts of the airports should be exempted from the limitations. These are strategic places visited by a very large number of people, where it is necessary to ensure maximum security of those who are present in such a place as well as to prevent serious crimes. Security sensitive public spaces could be defined in recital along the judgment in cases C-511/18 and C-512/18 as "places with a high incidence of serious crime, places that are particularly vulnerable to the commission of serious criminal offences, such as places or infrastructure which regularly receive a very high volume of visitors, or strategic locations, such as airports, stations or tollbooth areas". AT: (Comments): **rt 5 para 1a and 1b**: in any case, it is recommended to clarify that Article 5 needs to be seen in the context of a host of prohibitions following from other law, which apply irrespective of whether AI is involved or not (see above paragraph 1a), and to allow for flexibility by empowering the Commission to update the list of prohibited AI practices by way of delegated acts. ES: (Drafting): (iv) Management of complex events presenting clear risks in terms of public order, such as major sporting

	competititons, summits or other. ES: (Comments): Even if national security is a competence of member states it would be helpful to be clear in this point. SE: (Drafting): iiii) the detection, localisation, identification or prosecution of a perpetrator or suspect of an infringement related to entry or exit of goods in to or out of the Member state, constituting a criminal offence punishable with imprisonment for a maximum period of at least two years in the member state concerned, when the publicly accessible space is an area in proximity to a customs control area. SE: (Comments): An additional exemption for border areas where some surveillance could be expected, for crimes related to entry and exit of goods.
2. The use of 'real-time' remote biometric	PL: (Comments):

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:	support AT: (Drafting): *[Paragraphs 2 to 4 to be moved to new Article 5a]*
(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	**DELETED**

of the system;	
(b) the consequences of the use of the system for the rights and freedoms of all persons concerned, in particular the seriousness, probability and scale of those consequences.	**DELETED**
In addition, the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose	PL: (Comments): Under analitical consideration CZ:

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.	(Drafting): 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~~. CZ: (Comments): Regarding the compliance with necessary and proportionate safeguards for the use of real-time biometric identification systems for the purpose of law enforcement, CZ is of the opinion that is it not necessary to take into account temporal, geographic and personal limitations pursuant Article 5 (2). It would be sufficient only to assess necessity and proportionality of the use of such system in each individual case. We do not consider it necessary to justify in detail the use of these systems from a temporal, geographical and personal point of view, inter alia because it will not always be possible to clearly identify such restrictions. Alternatively, the text could read "(…) if possible as regards the temporal, geographic and personal limitations". ES:

	(Drafting): 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 **justified** personal limitations. ES: (Comments): 'justified personal limitations is added' – some personal limitations are always justified (i.e: stop the system once the person has been detected). Somo others, on the other hand, may lead to discrimnation (why is it applied to some groups and not others?) FR: (Comments): Ongoing work by FR experts
3. As regards paragraphs 1, point (d) and 2, each individual	PL: (Comments): Under analytical consideration

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, issued upon a reasoned request and in accordance with the detailed rules of	SK: (Comments): SK: "Duly justified situation" should be defined for the sake of legal certainty and prevention of internal market fragmentation by giving concrete examples of such situations. CZ: (Drafting): 3. As regards paragraphs 1, point (d) iv) 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, 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. CZ: (Comments): The general requirement of prior judicial authorisation (except situations of urgency) is excessive. CZ suggests requiring prior authorisation for the suggested point iv) which relates to security – sensitive

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.	spaces (see above). We do not find it proportionate to require prior independent authorization for example for the purpose of finding an offender by law enforcement. We are however ready to discuss this aspect if there is an evolution concerning points i), ii) and iii). In the spirit of compromise, we could accept prior authorization by "administrative authority" that would verify that all conditions are fulfilled. MT: (Drafting): 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, and if such authorisation is rejected, its use shall be stopped with immediate effect. MT: (Comments): Malta notes that whilst it is understandable that Remote Biometric Identification Systems are categorised as high risk by virtue of their biometric processing without explicit consent from the data subjects, the fact that prior authorisation from a judicial authority is required for "each individual use" of the AI even in cases of "preventing specific, substantial and imminent threat" to the life or physical safety of natural persons or of a terrorist attack, defeats the purpose of rapidly deploying AI to save lives and protect

	national security. Confusingly there is an exception whereby in a "duly justified situation of urgency" the use of real time remote RBI systems could be commenced without an authorisation and the authorisation could be requested only during or after the use. Therefore, Malta proposes to delete the word "individual" and to provide clarification on what could "duly justified situation of urgency" consist of. EE: (Drafting): As regards paragraphs 1, point (d) and 2, each individual ~~use~~ **case** 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, 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. EE: (Comments): The wording "each individual use" might create the need to ask for an authorisation in a single procedure each time a person is identified at a different location and/or in a different camera image, which would create a heavy administrative burden.

	Realistically, in most cases 'real-time' use of RBI is a situation of urgency and the exemption from prior authorisation is necessary. Is "duly justified" additional requirement that needs to be proved and if so, in which stage of the process? ES: (Drafting): 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 of the Member State in which the use is to take place, issued upon a reasoned request and in accordance with the detailed rules of national law referred to in paragraph 4. The procedure for the authorization granting should ensure that, where appropriate, its issuance is effective within xxx working days. 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 during or after the use, with the shortest possible delay. ES: (Comments): The authorization should be issued by a judicial authority. It is not reasonable to compare an administrative authorization with a judicial one.

	This issuance should be done in a short timeframe. Any urgency situation requiring the system to be put in place without authorization should need to ask for it as soon as possible. SE: (Drafting): 3. (a) As regards paragraphs 1, point (d) i-iii 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, 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. SE: (Comments): It seems redundant to use both each and individual. It is therefore proposed to delete "individual". The requirement that national law shall be detailed does not necessarily bring anything substantial to the Regulation. Ultimately, national law must in any case be in compliance with the requirements of the Charter when it comes to limiting fundamental rights.

	SE: (Drafting): (b). As regards paragraphs 1, point (d) iiii and 2, each use for the purpose of law enforcement of a 'real time' remote biometric identification system in publicly accessible spaces shall be subject to a documented assessment of legitimate interests of the law enforcement verses the interests of personal rights and freedoms, ensuring the proportionality of its use, in accordance to an internal documented procedure. SE: (Comments): A prior authorisation granted by a judicial authority or by an independent administrative authority is an unnecessarily resource consuming procedure. A catalogue of crimes, in this case in a defined area, combined with an internal order under the supervision of a supervisory authority should be sufficient. The internal order would be subject to a prior consultation under the GDPR.
The competent judicial or administrative authority shall only grant the authorisation	PL: (Comments): Under analitical consideration ES:

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 request, the competent judicial or administrative authority shall take into account the	(Drafting): For the purpose of requesting the authorization, the Law enforcement auhotirty shall deliver a report inlcuding the specific purpose for which the system will be used, an explanaotory note on the justification of its use, conditions and safeguards for its put into service and the technical documentation of the system, respecting the content described in annex IV. 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 request, the competent judicial or administrative authority shall take into account the elements referred to in paragraph 2.

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	PL: (Comments): Under analytical consideration SE: (Drafting): 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 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 and iiii*)* thereof, the competent authorities may be authorised to use those systems for the purpose of law enforcement. SE:

shall lay down in its national law the necessary detailed rules for the request, issuance and exercise of, as well as supervision 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	(Comments): The requirement that national law shall be detailed does not necessarily bring anything substantial to the Regulation. Ultimately, national law must in any case be in compliance with the requirements of the Charter when it comes to limiting fundamental rights.

use those systems for the purpose of law enforcement.	
	AT: (Drafting): AT: (Comments): With regard to real-time remote biometric identification an entirely new regulatory approach is suggested. As the provisions on real-time remote biometric identification do not resemble the *per se*-prohibitions in Article 5, but rather stipulate conditions for the use of these techniques, they should be moved to a separate Title IIa on 'Restricted AI practices'. As to the structure, the close interplay with Article 9 GDPR would become much clearer if the new provision were structured in a similar way and if explicit reference to the several justifications in Article 9 GDPR were made (see above paragraph 1). There should be a clarification that the new provisions do not in any way derogate basic principles of other laws, notably of the GDPR, such as that data must only be stored as far as strictly necessary to achieve the relevant law

	enforcement purpose (see above paragraph 5). Given that real-time remote identification achieved with the help of other than biometric techniques (e.g. with the help of mobile phone signals) may be almost as problematic it could be an option to remove the restriction to biometric identification and include also other techniques of mass identification.

	As emotion recognition systems and biometric categorisation systems pose a significant threat to fundamental rights, and as they are currently not covered by Article 9 GDPR (but only by Article 6 GDPR), it is recommended to establish for these techniques a regulatory regime similar to that of Article 9 GDPR. This regime could then also include biometric identification that does not qualify as real-time remote biometric identification. If such a provision is introduced it might be advisable to integrate the provision on transparency obligations which is currently to be found in Article 52(2) AIA Proposal (see paragraph 3 above). There should also be a clarification that further requirements or restrictions following from other Titles of the Act or from other law remain unaffected (see paragraph 4 above).

	We propose a special rule on decision making based on biometric techniques. This rule would be without prejudice to Article 22 GDPR, but as the latter applies only to fully automated decisions without meaningful human intervention there is a conspicuous gap which should be filled. The proposed Article 5c combines elements of Article 22 GDPR and Article 14 (5) AIA Proposal but modifies the latter as it is problematic in several respects.

TITLE III	CZ: (Drafting): ~~TITLE III~~ CZ: (Comments): The Commission has not provided any real-life example of the so called high-risk AI system that caused harm in the EU in the past. Or that such AI system has not been covered / regulated by the existing EU legal framework. Unless the Commission proves beyond any doubt that the principle of the evidence-based policy is kept, we suggest deleting the whole part on High-risk AI systems as it is unjustified.
HIGH-RISK AI SYSTEMS	CZ: (Drafting): ~~HIGH-RISK AI SYSTEMS~~

Chapter 1	CZ: (Drafting): ~~Chapter 1~~
CLASSIFICATION OF AI SYSTEMS AS HIGH-RISK	CZ: (Drafting): ~~CLASSIFICATION OF AI SYSTEMS AS HIGH-RISK~~
Article 6 Classification rules for high-risk AI systems	PL: (Comments): The very general formulation of the principle of classifying artificial intelligence systems on the basis of Annex 3 in conjunction with Art. 6 of the project. The generic description included in the annex means that even the simplest recruitment programs or supporting the work of lawyers may be classified as high-risk artificial intelligence systems without any apparent reason. This is particularly important for the application of "artificial intelligence systems" in medicine. It is questionable whether the indicated

	programs can be considered as "high risk artificial intelligence systems". Therefore, it is necessary to clarify Annex 3 in a way that avoids the creation of the legal regulation referred to in point 3.1., Ie similar to the "Red Flag Act." CZ: (Drafting): 3. Moreover, information systems working with defined and unchanging algorithms which are determined by humans, not by a machine based on its learning, or statistical models and statistical prediction methods, such as logical and linear regressions or Bayesian estimation, are not considered high-risk systems. CZ: (Comments): It is crucial to explain in detail what exactly is meant by the 2 conditions contained in letters (a) and (b) of Article 6 (1) and define it in a clearer way directly in the text. The Article is so broadly defined that basically as a general rule, any AI system will be considered as high risk. It is important for the Czech Republic that the proposed regulation makes it clear that simple information systems are not considered high-risk, even if they fall under one of the areas covered in Annex III. Therefore, we suggest adding the highlighted part in the 2nd column. At the same time, we suggest removing the statistical methods from the scope of the proposal.

	The European Commission should provide the Member States with clarifications and more details on how the delicate balance will be secured between the respective competences of the Member States and subject matters of AI Systems (education, health…). The Commission should specify what approach and methodology will be chosen for the AI systems which fall under the shared and supportive Union competences. DK: (Comments): It is appropriate to apply stricter requirements for the development and use of AI which may entail high risk for individuals and society, but we must clearly limit the category to applications that may cause such high risk. In our view, further work is needed on setting the right benchmark for what is to be considered high-risk AI – also when it comes to setting a clear methodology for evaluating future use cases. Only AI systems which poses significant risk for serious harm or violation of rights where the result would be difficult to reverse should be considered high-risk. BE: (Comments): Belgium considers the classification rules for high-risk AI systems, as set out in Chapter 1 of Title III of the Proposal, in conjunction with Annex III, to be overall vague and in particular challenging to apply in practice. It remains to a large extent unclear which concrete use cases, tools or practices are in scope,

	especially for in-house development and small scale use. Further clarification on these classification rules and how to apply them correctly to particular cases, e.g. in the security services sector, is therefore welcomed. SE: (Comments): It is important that the regulation concerning high-risk AI Systems is proportionate to the purpose of the regulation. New requirements must not conflict with existing requirements in other regulations. New rules should not overlap with existing rules, as this risks complicating the application and reducing the effectiveness of the rules. It must also be taken into consideration that the application of the new regulation cannot lead to every activity using a modern IT-based component or support practically is to be regarded as high-risk.
1. Irrespective of whether an AI system is placed on the market or put into service independently from the products	SK: (Comments): **SK:** It is unclear what is meant by the formulation „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)". The provision should be reformulated as it seems that the original intention was not to create a new unknown category of

referred to in points (a) and (b), that AI system shall be considered high-risk where both of the following conditions are fulfilled:	AI systems but rather a closed list of hisk-risk systems listed Annex II and III. Note no. 229 on page 50 of the Impact Assessment (SWD(2021) 84 final, Part 1/2) seems to imply that the current wording was meant to cover safety components placed on the market independently from the products under a) and b), but the wording in article 6 is different as it refers to AI systems in general. In addition, article 6 applies a somewhat mechanistic and possibly even oversimplifying classification of (high) risks. Firstly, as Annex II can be updated only via standard legislative procedure, the list of products referred to in article 6 (1) may not catch on time the spread of IoT run on AI systems. For instance, wearables, implantables, embeddables, ingestibles or voice and other personal assistants may already today present a high risk to fundamental rights and health, yet are not covered by the current product harmonisation legislation under NLF and Old Approach. Secondly, it is not clear why the risks are being reduced to safety components of products under article 6 (1), as the risks and dangers to fundamental rights may go beyond those risks of products identified in article 3 (14), such as risks to privacy and dignity. Thirdly, the Impact Assessment lacks a detailed analysis proving an absence of possible duplications and overlaps with existing sectorial legislation (such as medical devices). Fourthly, for the whole article 6, we need to ensure that *all* high-risk systems – both the stand-alone systems under article 6 (2) and the products under article 6 (1) - are matched with an equal level of requirements, obligations and comparable costs for operators, including obligations related to the type of assessment (internal vs. third party; this has naturally also impacts on equal protection of fundamental rights of affected persons). Fifthly, the classification of risks is focused only on risks related to individual products and stand-alone systems, while systemic risks not addressed by other EU legislation are not considered at

	all (e.g. mutual interactions between AI systems; AI systems deployed on digital platforms but not specifically addressed by the Digital Services Act – see below comments to Annex III; AI systems deployed on financial markets and not addressed by sectorial legislation; impacts on public services and real economy on macro-scale). It follows that new types of flexible lists of products and risks need to be created, possibly via delegating powers to an independent EU authority, while respecting the *Meroni* and *Romano* line of case-law of CJEU.
(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;	SE: (Drafting): (a) the AI system is intended to be used as a safety or a security component of a product, or is itself a product, covered by the Union harmonisation legislation listed in Annex II; SE: (Comments): Safety component indicates operational reliability. Add the term security to include AI-based security solutions.

(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.	SE: (Comments): Is the condition that a third-party conformity assessment has to be done?
2. In addition to	PL:

the high-risk AI systems referred to in paragraph 1, AI systems referred to in Annex III shall also be considered high-risk.	(Comments): Art. 6 sec. 2 of the draft together with point 4) (a) of Annex III: It is not clear why in Annex III, the application "informing about vacancies ". The question is whether informing about vacancies, which are generally publicly available, i.e. about job vacancies in a given organization, constitutes an element of the high risk of the organization. It needs to be clarified whether all the systems described in Annex III are "high risk" systems ("automatic"), especially as stated in recital 32. On the basis of this recital, it can be argued that the system set out in Annex III should be assessed each time (the recital indicates the regulation, but it seems to be Annex III). With such an interpretation, not every system (application) indicated in Annex III would have to be automatically considered as a high risk system. Perhaps adopting such an interpretation would be reasonable and desirable (the issue would require a broader analysis), but it should be considered contrary to the literal wording of Art. 6 sec. 2 of the project. CZ: (Drafting): 2. In addition to the high-risk AI systems referred to in paragraph 1, AI systems referred to in ~~Annex III~~ New article shall also be considered high-risk. CZ: (Comments):

	The far-reaching definition combined with Annex III might lead to a situation when, for example, almost all law enforcement systems are considered high risk. Under the current wording also a "simple" system, which on the basis of input data and fixed algorithms conducts tasks clearly defined by humans without the possibility for self-judgement or self-modification, could be included in those categories. The development or use of such systems in practice does not create a risk comparable to machine learning and skills improvement. Therefore, the definition should be adapted to exclude such systems and AI system contained in Annex III should be categorized as high-risk only in justified cases where the level of risk is really high. EE: (Comments): We prefer a separate act on AI in the field of law enforcement similarly to the GDPR. The AI Act regulates the use of AI in the field of criminal and judicial procedures and sets great limitations on fight against crime. However, Articles 82 and 83 of the TFEU are not considered in the legal basis. BE: (Comments): See comment on Article 6. FR:

	(Drafting): 2. In addition to the high-risk AI systems referred to in paragraph 1, AI systems**, posing a risk of harm to the health and safety, or a risk of adverse impact on fundamental rights,** referred to in Annex III shall also be considered high-risk. FR: (Comments): Only AI systems that may present a risk of harm to the health and safety, or a risk of adverse impact on fundamental rights should be considered as high-risk. Furthermore, the same criteria should be applied to draw and amend the list of Annex III. SE: (Comments): 6.2 and corresponding point 6(g) of Annex III: With reference to the comments already stated on art. 3.1, the definition of "AI-system" in combination with the rules stated in p.6(g) of Annex III would put unnecessary restraints on the development and use of certain small scale AI-system used in law enforcement. Practically all R&D within the area of law enforcement is conducted for the purposes of those accounted for in p.6(g), as well as most "basic operation procedures". Thus, the regulation would have too serious impact on LEA:s abilities. FI:

	(Comments): The list in Annex III of high risk AI systems referred to in Article 6 (2) should be clarified. Especially point 5 Access to and enjoyment of essential private services and public services and benefits is very vague. As it reads now, it could be interpreted as to include mandatory insurance run by private insurance companies, which can sometimes in certain member states be classified as being part of social security (eg. motor insurance, workers´ compensation). It is probably not the intention to include such mandatory insurance as high risk AI systems. We ask that this would be clarified in the wording of the annex or at least in a recital.
	CZ: (Comments): CZ suggests incorporating the list in Annex III directly into the normative text, for example through creating a new article.
Article 7 Amendments to Annex III	**DELETED**

	DELETED CZ: (Drafting): ~~Article 7~~ ~~Amendments to Annex III~~ CZ: (Comments): Since CZ suggests moving the list in Annex III into the text, there would be no need for the original Article 7. As a minimal requirement, more competencies should be given to the European Artificial Intelligence Board as proposed by article 56 to be directly involved in the amendment process, as well as other well defined criteria.

	EE: (Comments): Comments made under Article 4 regarding the legitimacy of delegated acts that define the scope of the regulation apply here as well. We would prefer that list determining the scope of the regulation are established in the Regulation. In any case, for the purposes of ensuring compliance with TFEU Article 290, the Commission's discretion to adopt delegated acts for amending Annex III must be very clearly defined. Art 7 should further introduce a specific impact assessment procedure prior to amending Annex III and guarantee the involvement of stakeholders. Further consideration should be given to the matter of creating a procedure for updating the areas that can be considered as high-risk in Annex III. BE: (Comments): Belgium believes that the Commission's power to adopt delegated acts to update the list of high-risk AI systems in Annex III, in the light of Article 7, goes too far and hence, further clarification as to other

	possibilities to amend this Annex is needed. In any case, additional clarifications are required and should be duly specified in the AIA, in particular, as to the relevant criteria, consultation procedures and implementation process when making use of this power. It is also very important that a broad set of industry stakeholders is involved in the process, ensuring the consultation of representatives of the civil society, industry, academia and the public sector. We therefore give priority to a more inclusive approach in this matter, in order to provide legal certainty and ensure trust. SE: (Comments): The process for updating the list is too vague and lacks sufficient transparency. Adding new topics to the list has the potential to significantly influence individual enterprises as entire markets. There is obviously a trade-off to be made here between long term stable conditions and agile regulation. However, even when advocating for agile regulation, which is recommendable, one must adhere to transparency and democratic values. One example of a vaguely formulated point concerns “essential private services“ which would give potential room for finding AI systems in entire services sectors as being of high risk. FI: (Comments): FI notes that the purpose of the amendments is to ensure that the regulation is future-proof, however, notes

	that the scope of the Regulation should not be dependent on delegated acts, and the proposed powers should be narrowed down or removed.
1. The Commission is empowered to adopt delegated acts in accordance with Article 73 to update the list in Annex III by adding high-risk AI systems where both of the following conditions are fulfilled:	PT: (Drafting): 1. The Commission is empowered to adopt delegated acts in accordance with Article 73 to update the list in Annex III by adding high-risk AI systems where ~~both of the following conditions are fulfilled:~~ PT: (Comments): As it now stands, the regulation only allows the inclusion of new high-risk AI systems if they fall under any of the eight listed areas and are deemed to pose at least as great a risk (to health and safety or adverse impact on fundamental rights) as systems already in Annex III. In our opinion, while the eight domains listed seem broad enough, there is a real possibility that they are unable to exhaust the range of domains within which AI systems may have significant impacts on the individual's lives in the future. AI systems' use in various other domains could raise significant additional risks that are not sufficiently encompassed in these eight risk areas (one example: AI-based personal digital assistants which could be used to give individuals important financial, legal, or medical advice with significant consequences for health and

	safety, and do not appear to be covered by the current risk categories). There is also the natural and rapid evolution of these systems, a reality which in itself makes the extent of its impacts very difficult to anticipate. PL: (Drafting): ~~The Commission is empowered to adopt delegated acts in accordance with Article 73 to update the list in Annex III by adding high-risk AI systems where both of the following conditions are fulfilled~~ PL: (Comments): If the purpose of the act is to ensure uniform conditions for the implementation of legally binding EU acts, the form of the implementing act is preferred, not the delegated act (see Reg. 182/2011). The proposed provision seems to be inconsistent with Art. 290 TFEU. The essential elements of EU normative acts cannot be regulated in the form of delegated acts (cf. Article 290 TFEU). It is noted that the proposal to use the form of a delegated act in the draft regulation results only from the fact that these issues were included in the regulation in the form of an annex (although elevated to a normative rank). The disclosure of new techniques or ways of using AI systems, as well as their qualification as high-risk systems, should be considered during the ordinary legislative process involving multilateral agreements and respect for the sovereignty of Member States, including their national

	constitutional orders. **DELETED** CZ: (Drafting): 1. The Commission is empowered to adopt delegated acts in accordance with Article 73 to update the list in Annex III by adding or removing high-risk AI systems where both of the following conditions are fulfilled:

	CZ: (Comments): Since CZ suggests moving the list in Annex III into the text, there would be no need for the original Article 7. As a minimum requirement for this paragraph, we suggest adding an option to also remove certain high-risk systems, should it be needed. If, as the GSC suggested, this is not possible to do by the delegated acts, the Commission should come up with a solution and describe the process or refer to it in the text. DK: (Comments): We are supportive of establishing a process for updating the high-risk category in order to take into account future technological and market developments. However, any potential, future adjustment of the category must always take place on the basis of a concrete risk assessment as well as clear and predictable criteria. At the moment, we still find that the criteria laid out in the regulation could be further improved as well as specified further in the rectials. Also, we are questioning the choice of instrument in terms of a delegated act, as the potential mandate for these amendments seems quite broad with the current formulations and could thereby result in greater changes to the scope. In this light, we would like the opinion of the Council Legal Service in terms of whether the annex III and the addition of high-risk systems would constitute a non-essential element according to article 290 TFEU. In this connection, we also see a need for greater involvement of the member states, including the direct

	involvement of the European Board for AI in the risk assessment Furthermore, a process for updating the category should also allow for both adjustments and deletions. Otherwise, the list of systems will only become longer, as we go along – and technological and market developments could merit both additions as well as adjustments and deletions. BE: (Comments): Article 7 introduces a double conditionality to amend Annex III on high-risk application systems. It does not seem possible to add areas other than those already indicated (as it would probably be considered as a substantial change to the text). This means that an exhaustive list of areas shall be defined with no possibility of revision. Belgium retains a study reservation on this matter. ES: (Drafting): 1. The Commission is empowered to adopt ~~delegated~~ **implementing** acts in accordance with Article 73 to update the list in Annex III by adding high-risk AI systems ~~where both of the following conditions are fulfilled:~~ that 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. ES:

	(Comments): - Implementing acts: same reason as in article 4. - We are sure that it is a good idea to initially stick to the 8 areas of annex III (so the regulation does not regulate too little or too much. However, we don't see it is valid reason when it comes to updating annex III. It is perfectly possible to foresee the detection of a HRAIS out of the 8 areas indicated in annex III. We consider that it is more appropriate to base the update on a risk assessment only. FR: (Drafting): The Commission is empowered to adopt ~~delegated~~ **implementing** acts **every XX years,** in accordance with Article ~~73~~ **XXXX** to update the list in Annex III by adding high-risk AI systems where both of the following conditions are fulfilled: FR: (Comments): It is not a question of amending an essential element of the legislative act, but rather of its application. Only the Council should therefore intervene, among the co-legislators. Moreover, it is convenient to provide for a fixed periodicity of revision of the list, in order to keep control over this revision. If the necessity to be able to modify this annex rapidly, considering the very important technological

	progress in this sector, it is nevertheless problematic that the Member States are not associated in the decision process, which will have very important consequences on the work of their services. It would be preferable and essential to allow the Commission to modify Annex III by means of implementing acts, thus allowing prior consultation of the Member States. SE: (Drafting): 1. The Commission is empowered to adopt delegated acts in accordance with Article 73 to ~~update~~ amend the list in Annex III by adding or deleting high-risk AI systems, or systems that no longer should be considered high risk, where both of the following conditions are fulfilled: SE: (Comments): Technical and societal development may lead to that some systems no longer should be considered high risk. The regulatory choice of empowering the Commission to adopt delegated act to update the list in Annex III, should be replaced by the choice of implementing acts. This since the additional rules or change in definitions are intended merely to implement or to give effect to the rules already contained in the basic act.

(a) the AI systems are intended to be used in any of the areas listed in points 1 to 8 of Annex III;	PT: (Drafting): ~~(a) the AI systems are intended to be used in any of the areas listed in points 1 to 8 of Annex III;~~ ES: (Drafting): ~~(a) the AI systems are intended to be used in any of the areas listed in points 1 to 8 of Annex III;~~ SE: (Drafting): (a) it has been three or more years since a delegated act in accordance with this article was adopted and that a qualified majority of the member states formally has asked for a delegated act to amend Annex III ~~(a)~~(b) the AI systems are intended to be used in any of the areas listed in points 1 to 8 of Annex III; SE: (Comments):

	Proposed point (a) will be point (b) and so on.
(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	PT: (Drafting): ~~(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 PL: (Comments): The term of fundamental rights should be significantly clarified by clarifying the text of the provision or adding a recital that would tighten the directions of interpretation (in accordance with international, regional and national (constitution) binding instruments or/and non-binding international, regional or national recommendations see: work of UN, Council of Europe, UNESCO or the EC's Trustworthy AI Guidelines or Charter of Fundamental Rights. AT:

referred to in Annex III.	(Drafting): (b) the AI systems pose a risk of harm to the health and safety, or a risk of adverse impact on fundamental rights including economic risks and risks to society at large AT: (Comments): It should be clarified that the notion of 'fundamental rights risks' may include economic risks and risks for society at large. 'Fundamental rights' are often understood as specifically meaning individual rights listed in the Charter, which might give rise to the misunderstanding that risks such as fraud or the undermining of democratic elections are not covered. From a consumer perspective, the inclusion of economic risks and societal risks is definitely of key importance DK: (Comments): The benchmark of "equivalent to or greater to" is still unclear to us, especially as the use cases listed in annex 3 are very diverse. BE: (Drafting): ~~(b)~~ (a) 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. ES: (Drafting): ~~(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.~~ SE: (Drafting): ~~(b)~~(c) 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.
2. When assessing for the	PL:

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:	(Comments): Referring to Art. 6 comment above: on the other hand, taking into account the content of Art. 7 sec. 2 of the draft, it can be argued that the legislator, when creating Annex 3, already took into account the criteria from recital 32 (i.e. we do not reassess). That needs to be clarified. SK: (Comments): **SK:** It should be clearly stated that the criteria are not cumulative (as Slovakia understands was the original intention). CZ: (Drafting): 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 all the following criteria: CZ: (Comments): Since CZ suggests moving the list in Annex III into the text, there would be no need for the original

	Article 7. As a minimal requirement, we suggest emphasizing that all the criteria are taken into account before the amendment is made. AT: (Drafting): […] an AI system poses a risk of harm to the health and safety , or a risk of adverse impact on fundamental rights including economic risks and risks to society at large AT: (Comments): It should be clarified that the notion of 'fundamental rights risks' may include economic risks and risks for society at large. 'Fundamental rights' are often understood as specifically meaning individual rights listed in the Charter, which might give rise to the misunderstanding that risks such as fraud or the undermining of democratic elections are not covered. From a consumer perspective, the inclusion of economic risks and societal risks is definitely of key importance EE: (Comments): More transparency and clarity is needed to understand how different criteria are evaluated and what they

	are based on.
(a) the intended purpose of the AI system;	**DELETED**
(b) the extent to which an AI system has been used or is likely to be used;	FI: (Comments): We would kindly ask for some clarification on this, especially on how the extent is determined (eg. according to the amount of people that are affected).
	DELETED

	DELETED
(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	PL: (Comments): Artificial intelligence systems pose a risk of harm to health and safety or a risk of adversely affecting fundamental rights which, in terms of severity and probability of occurrence, is equivalent to the risk of harm or adverse impact posed by high-risk AI systems already listed in Annex III, or bigger. " It is possible to risk a thesis that any use of "artificial intelligence systems" in medicine may (theoretically) pose a "risk of harm to health", which would lead to the conclusion that all "artificial intelligence systems; In medicine, it would constitute "high-risk artificial intelligence systems", which would have all the consequences set out in the draft Regulation for "high-risk artificial intelligence systems". It should be considered whether such an approach will "stifle" the development of medical technologies. AT: (Drafting):

demonstrated by reports or documented allegations submitted to national competent authorities;	[…] harm to the health and safety, or a risk of adverse impact on fundamental rights including economic risks and risks to society at large interacting with the AI system […] AT: (Comments): Reasoning see above.
(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;	**DELETED**
(e) the extent to which potentially harmed or adversely impacted persons are	**DELETED**

dependent on 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;	**DELETED** FI: (Comments): The definition of the potential harm requires clarification. Is it considered harm, for example, if artificial intelligence would conclude that, as a result of increased in come or a certain amount of benefit, the amount of a certain social benefit received by a person should be reduced? Due to the foresaid example it is essential that the outcome is considered as a whole, in order to ensure equal outcome for individuals. However, when considering the matter from the perspective of a single information system or application, the impact can be considered to be harmful as the level of the benefit would be decreased.
(f) the extent to which potentially harmed or adversely impacted persons are	ES: (Drafting): (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, **physical or**

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;	**psychological position**, economic or social circumstances, or age; ES: (Comments): In order to include people with disabilities
(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	**DELETED**

reversible;	Therefore, we propose to redraft the proposed wording as per the text in the second column BE: (Comments): Cf. our remark on the definition of "serious incident" (art. 3, (44)); quid legal persons (e.g. outcome produced with an AI system impacting the existence or viability of a legal person)? FI: (Comments): Consider mentioning impacts on the private life or reputation of persons. Public disclosure of facts of a person's private or family life is not easily reversible.
(h) the extent to which existing Union legislation provides for:	

(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.	
Chapter 2	
REQUIREMENTS FOR HIGH-RISK AI SYSTEMS	DK: (Comments): As a general remark in terms of the requirements, it is positive to see an approach based on the New

	Legislative Framework, meaning a principle-based approach which leaves certain room for maneuver for the specific technical solution as well as usage of standards in relation to compliance. However, we find that there is room for further operationalization of the requirement. This is a prerequisite for facilitating an effective compliance procedure as well as enforcement. We have highlighted in some of the requirements, where operationalization is especially important, but we find that this is necessary in all of the requirements. Furthermore, preparation of practical guidance as well as standards which needs to be available before the application of the regulation are also essential elements. This should be specifically reflected in the regulation. For example, article 58 concerning the task of the AI Board could be further specified in terms of needed guidance. In that respect, it is also essential to develop practical guidance tools in order to increase legal certainty. One practical tool would be a horizontal assessment tool, especially targeted SMEs, which would enable providers and users quickly to clarify whether they would be subject to the requirements of high-risk AI. SE: (Comments): Article 8-15 need to be reviewed and re-made. Instead of disproportionately imposing requirements on the structure of work within companies, what is illegal (not desirable) should be regulated. The legislation should not lay down new administrative requirements, but specify what is not desirable,

	that is, what is illegal. Creating a large compliance structure for good technology support is unfortunate, complicated and unwarrantedly burdensome. The use of AI does not withdraw an employer of responsibility under applicable national nor international laws and regulations. Should there be insufficient regulation in certain areas, these should be complemented rather than implementing regulation targeted one specific technology. If there are to be administrative requirements, these need to be different depending on the type of company and the industry, for example, SMEs do not have the same conditions as multinational enterprises. (today, the proposal only means that SMEs should receive targeted information and lower fees).
Article 8 Compliance with the requirements	PL: (Comments): Under analitcal consideration
	PL: (Comments):

	It is questionable whether a risk analysis as such is only required in a "high risk" situation. Risk analysis should be an obligatory element of any artificial intelligence and it (risk analysis) should show whether we are dealing with high risk or not. Focusing only on "high risk" means that entities that will create, use artificial intelligence will have "room for maneuver" to prove that a given artificial intelligence is not high-risk, and thus it may sometimes infringe the rights of people, who will use it. Thus, Art. 8 and 9 should refer to "risk" as such and to "high risk".
1. High-risk AI systems shall comply with the requirements established in this Chapter.	BE: (Comments): Belgium believes that the requirements for high-risk AI systems are sometimes slightly vague and may need to be better defined (cf. comment on Article 6), as generally they are perceived as being too strict, especially taking into consideration the broad spectrum of AI systems that would be considered high risk. In addition, several of these requirements are still topics of active research and concrete approaches for achieving these requirements might not be available on time depending on the specific AI technique.
2. The intended purpose of the high-risk AI system and the risk management	SK: (Comments): **SK:** An explicit reference to technological “state-of-the-art” should be included among the elements to be

system referred to in Article 9 shall be taken into account when ensuring compliance with those requirements.	taken into account for all requirements under Chapter II Title III. Recital 49 is not sufficient and too narrow. For comments on the notion of "intended purpose" see above. EE: (Comments): The tendency of the regulation to take into account (under current wording) one specific purpose of an AI system is problematic. See, for example, Article 8 (2) and Article 9 (2) (b). New systems (such as Microsoft's Generative Pre-trained Transformer 3 (GPT-3)) already have many potential purposes instead of one specific, and this should be taken into account when setting requirements. Please see our comment in the definitions section.
	ES: (Drafting): 3. For the purpose of providing with guidance on the implementation of the following requirements, the Commission shall draw up in collaboration with member States, taking into consideration article 58, guidelines on the practical implementation and protocols to be established concerning those requirements. ES: (Comments): It is very important for us to have a clear mandate on developing guidelines and other tools, that are most

	useful to SMEs or Start-ups. They will need to hire expensive consultant services otherwise, leading to the inviability of useful and innovative projects. FR: (Drafting): (New) **3. When some of the requirements laid out in articles 8 to 15 may enter into conflict, the development of AI systems can adopt a balancing approach between them. The balance should be explicit** FR: (Comments): We should adopt a holistic approach to risk mitigation. Some of the 7 key requirements identified by the HLEG on AI are often at odds, leading to unavoidable trade offs; for instance accuracy vs robustness, privacy (data minimization) vs fairness, or accuracy vs fairness etc. However, the balance made has to be assumed and could be part of explainibility in Article 13.1.
Article 9 Risk management system	PT: (Comments): As a general comment, we believe that the risks this article intends to address with the recitals, that explicitly state the importance of addressing risks to health, safety, and fundamental rights, should be

	more harmonized. Furthermore, we consider to be of paramount importance to be very clear on the types of risks we are attempting to address and define clear procedures to help guide providers, developers, etc through the risk assessment process. Additionally, it is important to stress out the need to define the concept "lifecycle", which is used in this article, as well as in several others. The undefinition of this concept will create legal uncertainty and confusion. Moreover, and as referred above AI products/systems are generally created by several contributors and usually using open-source technologies and as so it is necessary to define how the risks in these cases will be managed, e.g. will the person who used the open-source materials be responsible/liable for the materials used? Or will be the person who created the open-source material? Finally, considering the principles of the New Legislative Framework it seems that AI system providers will carry most obligations and requirements established in the proposed Regulation. Nevertheless, it is important to keep in mind that many obligations and requirements can only be managed, in practice, by the user (who controls the AI system and its use). Even if a provider complies with all its obligations and requirements it cannot foresee all potential uses of the system PL: (Comments):

	Under analitical consideration **DELETED** SK: (Comments): **SK:** The risk management system should incorporate systemic risks (see comments above related to article 6) and also risks for *all* affected persons beyond those specified in article 9 (8) or article 5 (1) (b) (see comments above related to definition of "user" – article 3 4)). CZ: (Comments): As technology develops constantly and swiftly, "the most appropriate risk management measures" as stipulated by Art. 9 (5) and the testing procedures as stipulated in para (6) do develop and change in time. It is necessary to specify who will determine what is "the most appropriate measure" and how so as to

	make clear how it will be enforced. The definitions do include, i.e. the term "intended purpose" and "conformity assessment" but it is unclear what exactly can be regarded as "appropriate" and similar terms. MT: (Comments): Malta understands that here the intention is for such risk management systems to also be applicable to CIs when using AI and they shall fall within the context of Article 74 of the CRD. Malta notes that it is essential that in such cases, credit institutions understand the underlying risks of this technology and thus mange them appropriately, whilst keeping in mind the investment in technology that institutions may need to do, and financial constraints given that this would prove costly. SE: (Drafting): Article 9 Risk management ~~system~~ SE: (Comments): Delete "system", not to imply an IT solution.

1. A risk management system shall be established, implemented, documented and maintained in relation to high-risk AI systems.	PL: (Comments): 4Article 9 of the draft Regulation raises doubts in the context of GDPR risk management. The relationship between risk management within the meaning of the analyzed provisions and the provisions of the GDPR should be clarified. ES: (Drafting): 1. A risk management system shall be established, implemented, documented and maintained in relation to high-risk AI systems and the foreseeable risk to the health and safety of fundamental rigths of persons associated to them. ES: (Comments): A High Risk AI system could be associated with several risks. It is appropriate to specify what kind of risks should be addressed, even if this is specified in the recitals. SE: (Comments): The practical definition of a “risk management system” is not clear and should therefore be more precise:

	does a risk management system imply the need for separate IT-system for the monitoring of each individual AI-system, or does it imply the establishment of an administrative scheme for compliance monitoring? The first alternative would significantly add to the administrative burden of LEA. It might be difficult to set up an efficient post-market monitoring system prior to implementing a system. There is a risk of the system not being effective since effects of using the system are not always apparent before it is put to use.
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	**DELETED**

comprise the following steps:	**DELETED** DK: (Comments): It is unclear what is meant by a lifecycle which should be defined in the regulation. Furthermore, the requirement to perform regular systematic updating needs to be specified. ES: (Drafting): 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 will address risks associated with health and safety or fundamental rights and it shall comprise the following steps:
(a) identification and analysis of the known and foreseeable risks associated with each high-risk AI system;	EE: (Drafting): (a) identification and ~~analysis~~**assessment** of the known and foreseeable risks **to health, safety and fundamental rights** associated with each high-risk AI system; EE:

	(Comments): It should be more clearly defined either in the recitals or in the annex, which kind of risks must be assessed. The proposed amendments outline the risks more clearly and follow the wording of recital 1. Reference to identification and assessment better reflects the two-step process of (i) determining which rights and freedoms are potentially negatively impacted, if at all, and (ii) assessing how and to what degree. This allows for appropriate risk management measures to be implemented. The corresponding recital should be amended accordingly. BE: (Comments): Will the risks associated with each high-risk AI system be transparent for users and the public? Will the risk analysis report be available for the user before buying and using the AI system? ES: (Drafting): (a) identification and analysis of the known and foreseeable risks associated with each high-risk AI system, with a view of the different probability and severity of harms concerning safety, health, rights and freedom of persons or group of persons associated to each risk;

(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;	EE: (Drafting): **identification** ~~estimation~~ and **assessment** ~~evaluation~~ of the risks **to health, safety and fundamental rights** that may emerge when the high-risk AI system is used in accordance with its intended purpose and under conditions of reasonably foreseeable misuse; EE: (Comments): See (a).
	PT: (Drafting): (c) **evaluation of broader societal harms, beyond risks to health and safety or fundamental rights;** PT: (Comments):

	While most risks from AI technology can be thought of as the potential for harms to an individual's health and safety or of adverse impact on their fundamental rights, AI may also cause significant harm, on a societal level (for example, a digital personal assistant could be used to promote certain products, services, or even ideologies well above others, with the potential to contribute to substantial and potentially harmful shifts in our markets, democracies, and information ecosystems). However, the impacts on individual health, safety, or fundamental rights may be difficult to determine. Adding an extra step to this risk management system requiring evaluation of broader societal harms from AI systems would ensure that these risks are duly assessed by the providers of AI systems.
(c) evaluation of other possibly arising risks based on the analysis of data gathered from the post-market monitoring system referred to in Article 61;	EE: (Drafting): **identification and assessment** ~~evaluation~~ of other possibly arising risks **to health, safety and fundamental rights** based on the analysis of data gathered from the post-market monitoring system referred to in Article 61; EE: (Comments): See (a). ES:

	(Drafting): (c) Periodic identification and evaluation of other possibly arising risks based on the analysis of data gathered from the post-market monitoring system referred to in Article 61 ; ES: (Comments): An analysis on this data could lead to identification of new risks. This activity should be done regularly.
(d) adoption of suitable risk management measures in accordance with the provisions of the following paragraphs.	
3. The risk management measures referred to in paragraph 2, point (d)	DK: (Comments): It is still unclear to us how generally acknowledge state of the art should be interpreted as well as how this affects the different requirements. Therefore, we would ask for further specification of this concept.

shall give due consideration to the effects and possible interactions resulting from the combined application of the requirements set out in this Chapter 2. They shall take into account the generally acknowledged state of the art, including as reflected in relevant harmonised standards or common specifications.	Furthermore, it would be useful with further clarification on how the provider is required to consider the effects and possible interactions from the combined application of the requirements. SE: (Comments): This article is rather vague and would fit better as a recital.
4. The risk management measures	PT: (Comments):

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.	It is established that mitigation should be used until the "overall residual risk of the high-risk AI system is judged acceptable", once again, is not clear what it means "acceptable". Therefore, we consider it is necessary to develop best practices and standards to define these concepts in the proposed regulation.

In identifying the most appropriate risk management measures, the following shall be ensured:	
(a) elimination or reduction of risks as far as possible through adequate design and development;	PL: (Drafting): elimination or reduction of risks as far as possible through adequate design and development of AI system; DK: (Comments): It is unclear what is meant by adequate design and development which could be further clarified in a recital. ES:

	(Drafting): (a) elimination or reduction of identfied and evaluated risks as far as possible through adequate design and development; ES: (Comments): In order to set coherence with previous dispositions.
(b) where appropriate, implementation of adequate mitigation and control measures in relation to risks that cannot be eliminated;	EE: (Drafting): where appropriate, implementation of adequate mitigation and control measures**, including human oversight,** 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 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	EE: (Drafting): In eliminating or reducing risks **to health, safety and fundamental rights** related to the 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.

to be used.	
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.	PT: (Comments): This number covers "testing procedures" but it is not clear which type of testing they are referring to. The lack of specification will create misunderstandings, legal uncertainty, and confusion. There are several types of test procedures, such as, unit tests, integration tests, performance tests, operational tests, etc. These tests are of paramount importance and its use will help to mitigate the risks. Hence, we suggest adding an article to regulate the test phase of AI solutions in order to mitigate the risks of AI. Additionally, we also propose to mention technics such as Explainable Artificial Intelligence (XAI), referred in the EC Communication regarding Artificial Intelligence for Europe. The use of these technics should be encouraged given the fact that these can help debugging and auditing activities. A new article is proposed further in this document
6. Testing	PT:

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.	(Comments): It is not explained what it means to be "suitable" and due to the fact, there are no best practices or standards, as there are for instance for data protection, the use of these terms will create legal uncertainty and as so we recommend to develop standards and best practices to define these concepts. This number covers "testing procedures" but it is not clear which type of testing they are referring to. The lack of specification will create misunderstandings, legal uncertainty, and confusion. There are several types of test procedures, such as, unit tests, integration tests, performance tests, operational tests, etc. These tests are of paramount importance and its use will help to mitigate the risks. Hence, we suggest adding an article to regulate the test phase of AI solutions in order to mitigate the risks of AI. Additionally, we also propose to mention technics such as Explainable Artificial Intelligence (XAI), referred in the EC Communication regarding Artificial Intelligence for Europe. The use of these technics should be encouraged given the fact that these can help debugging and auditing activities. A new article is proposed further in this document EE: (Drafting): 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~~.

	EE: (Comments): Please remove the part as indicated. It is not saying anything from legal perspective (the regulation itself indicates what is necessary and to what extent). It can create confusion during application and potentially conflict with the GPSR's safety net.
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.	PT: (Comments): This number covers "testing procedures" but it is not clear which type of testing they are referring to. The lack of specification will create misunderstandings, legal uncertainty, and confusion. There are several types of test procedures, such as, unit tests, integration tests, performance tests, operational tests, etc. These tests are of paramount importance and its use will help to mitigate the risks. Hence, we suggest adding an article to regulate the test phase of AI solutions in order to mitigate the risks of AI. Additionally, we also propose to mention technics such as Explainable Artificial Intelligence (XAI), referred in the EC Communication regarding Artificial Intelligence for Europe. The use of these technics should be encouraged given the fact that these can help debugging and auditing activities.

Testing shall be made against preliminarily defined metrics and probabilistic thresholds that are appropriate to the intended purpose of the high-risk AI system.	A new article is proposed further in this document ES: (Drafting): 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 or after a substantial modification of the AI system has been performed, provided the new AI system constitutes a High-risk AI system. Testing shall be made against preliminarily defined metrics and probabilistic thresholds that are appropriate to the intended purpose of the high-risk AI system.
8. When implementing the risk management system described in paragraphs 1 to 7, specific consideration shall be given to whether the high-risk AI system is likely to	EE: (Drafting): 8. When **establishing and** implementing the risk management system described in paragraphs 1 to 7, specific consideration shall be given to whether the high-risk AI system is likely to be accessed by or have an impact on children. EE: (Comments): It is important to take the rights of the child into consideration from the very beginning when assessing the

be accessed by or have an impact on children.	impact on fundamental rights.
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.	PL: (Comments): The concept of "child" (within the risk management system - Art. 9 (9)) should be clarified. First, indicating a specific age limit would solve the problem of discrepancies at the level of national laws. Second, the impact assessment on the child as part of the risk management system should be based o specific age limits due to significant cognitive and emotional differences in children aged 7, 10 or 13. It is not possible to adopt effective criteria for all age groups. It would also be a good direction to indicate what kind of impact on children is particularly undesirable in terms of the objectives of the regulation. CZ: (Comments): We suggest the deletion of the Annex III 5 (b) and incorporation of the Annex III to the main legislative text. If this Article aims also to other applications than those listed in Annex III 5 b), it should be specified. Also similar exemption should be considered for a broader range of financial institutions regulated and overseen by relevant authorities.

	Additional requirements for credit institutions regarding AI risk assessment and compliance specific requirements in the draft AI regulation could be, especially in light of their other obligations, overly burdensome for these institutions. This should be discussed and evaluated on the appropriate platform. Given that the EC proposal amending the CRD is due to be discussed at ECOFIN on 9 November, it would be preferable to remove references to the CRD from the draft AI Regulation and discuss the proposed obligations in the context of the CRD legislative process. IT: (Comments): *It would be welcome if the Commission provided more clarification about the scope of the regulation with reference to the credit and financial sector.*
	PT: (Drafting): 10. Appropriate meaningful explanations shall apply for the development of high-risk AI systems in order to increase the user benefit, the social acceptance, the assisting with audits for compliance with regulations, and system debugging, and the support of field testing reerred in to Article XX (new proposed article futher in this document)

	PT: (Comments): We propose to mention technics such as Explainable Artificial Intelligence (XAI), referred in the EC Communication regarding Artificial Intelligence for Europe . The use of these technics should be encouraged given the fact that these can help the debugging and auditing activities previous to the deployment and need for human oversight.
Article 10 Data and data governance	PT: (Comments): General remark: In our opinion, the repeated use of the term "appropriate" in several provisions of this Article may result in excessive imprecisions and legal uncertainty: in paragraphs 2 and 6 (***appropriate*** *data governance*), in paragraph 3 (***appropriate*** *statistical properties*) and in paragraph 5 (***appropriate*** *safeguards for the fundamental rights and freedoms of natural persons*). For example, it is very difficult to know particularly what constitutes an "adequate" statistical property: does this require the data to be a representative sample of the entire population, or only of the potential *ad hoc* groups that may be subjected to the AI system's analysis? This decision is thus left to the respective provider, who will thus make the realisation as he sees fit. PL: (Comments):

	Under analitical consideration CZ: (Comments): We need to have absolute legal and practical clarity between this Article and other EU legislation which also deals with significant legal provisions on data processing, such as the ePrivacy regulation, Cybersecurity Act and others. We propose some reference to the relevant legislation in the text. MT: (Comments): Pursuant to Article 10, Malta notes that it covers the use of data sets of which applies exclusively to high-risk AI and does not include activities where AI is still experimentation phase, this can pose an upstream harm in the AI chain. DK: (Comments): It is essential to set tangible data requirements for the development and use of high-risk AI. AI is only as useful, as the data which it is trained upon. Data quality is essential, especially due to the complexity of an AI system as well as its scalability.

	However, at the same time, the article - as currently phrased - is rather ambiguous, thereby, leaving it difficult for providers, especially the SMEs, to know when they are in compliance with the article's requirements.
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.	
2. Training, validation and testing	**DELETED**

data sets shall be subject to appropriate data governance and management practices. Those practices shall concern in particular,	**DELETED** ES: (Drafting): 2. Training, validation and testing data sets shall be subject to appropriate data governance and management practices in the context of the intended purpose of the high-risk AI system. Those practices shall concern in particular,
(a) the relevant	

design choices;	
(b) data collection;	**DELETED**
(c) relevant data preparation processing operations, such as annotation, labelling, cleaning, enrichment and aggregation;	**DELETED**

(d) the formulation of relevant assumptions, notably with respect to the information that the data are supposed to measure and represent;	
(e) a prior assessment of the availability, quantity and suitability of the data sets that are needed;	PL: (Drafting): a prior assessment of the availability, quantity, security, and suitability of the data sets that are needed PL: (Comments):

	We note that in high-risk systems it is necessary to take into account security criteria (GDPR, cybersecurity, identity management, business countinuity etc.). In connection with the above, we suggest that after the expression "quality criterion" add "and safety"
(f) examination in view of possible biases;	PL: (Comments): The terms "bias" and "discriminatory effect" should be clarified. A possible solution would be a "positive exclusion", ie an indication of eg when "bias" is acceptable.
(g) the identification of any possible data gaps or shortcomings, and how those gaps and shortcomings can be addressed.	**DELETED**

	DELETED ES: (Drafting): (g) the identification of any possible data gaps or shortcomings, sensitive variables or proxy variables in the dataset and how those gaps, sensitive features and shortcomings can be addressed. ES: (Comments): Several features must be addressed when preparing quality data.
	ES: (Drafting): The practices listed in this paragraph will be adapted to the fasiblity of their adoption in high-risk AI systems that continue to learn or in the context of federated learning systems, by using updated state of the art or best industry practices. ES: (Comments):

	Some of the activities listed in this paragraph are not feasible in the context of systems that continue to learn or use Federated Learning. An adaptation of the measures should be foreseen, ideally with technical standards.
3. Training, validation and testing data sets shall be relevant, representative, free of errors and complete. They shall have the appropriate statistical properties, including, where applicable, as regards the persons or groups of persons on which the high-risk AI system is intended to be used. These characteristics of the	PT: (Drafting): Training, validation and testing data sets shall ~~be relevant, representative, free of errors and complete. They shall~~ have the appropriate statistical properties, including, where applicable, as regards the persons or groups of persons on which the high-risk AI system is intended to be used, as well as, the appropriate statistical properties to be included as the requirements refferred to in Article 13(2) and to help the interpretation of the system behaviour in the utilization phase tasks reffered to in Article 14. PT: (Comments): The entire data collection and data management process may include access to old data that did not pass quality criteria such as those required in this proposed article, which does not mean that they have no value at all. So, concepts such as data relevance, representativeness, freedom of errors and completeness should be better defined or avoided at all. On the other hand, the concept "statistical properties" should be defined. The first part of this provision ("Training, validation and testing data sets shall be relevant, representative,

data sets may be met at the level of individual data sets or a combination thereof.	free of errors and complete") seems to introduce an obligation that is potentially unrealistic or at least very difficult to fulfil. Perhaps the specific wording should be softened. **DELETED**

	DELETED SK: (Comments): **SK**: The requirements are unrealistic and need to be adjusted. CZ: (Drafting): 3. Training, validation and testing data sets shall be relevant, representative ~~, free of errors~~and reliable~~ and complete~~. CZ: (Comments): As regards the words “free of errors”, the Commission explained at the workshops that this requirement did not have to be ensured 100% and that this provision had to be read together with Art. 8 and thus be taken into account together with the purpose of the system and the risk management system. CZ suggests talking about reliable data sets. Perfect data which are complete and free of errors do not exist. For the sake of legal clarity, we suggest the reference to such data is removed. Furthermore, the Commission’s explanation should be incorporated into the relevant recital. It is not clear from the current wording that ”no errors“ should be read as ”no relevant errors”.

	AT: (Drafting): 3. Training, validation and testing data sets shall be up-to-date, relevant, representative, diverse, inclusive, free of errors and complete. AT: (Comments): We suggest including aspects of the most current image of society, especially with regard to ethnic groups, minorities, gender, religion, ideology, disability, age and sexual age and sexual identity (based on Art. 14 ECHR) that in the development of test data sets or the conformity assessment. EE: (Drafting): 3. Training, validation and testing data sets shall be relevant, representative, ~~free of errors and complete,~~ **considering the state of the art and appropriate to the intended purpose of the AI system**. They shall have the appropriate statistical properties, including, where applicable, as regards the persons or groups of persons on which the high-risk AI system is intended to be used. These characteristics of the data sets may be met at the level of individual data sets or a combination thereof. EE:

	(Comments): It is generally impossible to have perfect data sets with no errors, therefore the wording of this requirement should be revised. Thus, it should be clearly established, that the intended purpose of the AI system must be taken into account when establishing requirements for training, validation and testing data. DK: (Drafting): 1. Training, validation and testing data sets shall ensure a level of relevance, representativeness and accuracy that is appropriate to the intended purpose of the system, taking into account, as far as possible, available state-of-the art. ~~shall be relevant, representative, free of errors and complete~~. They shall have the appropriate statistical properties, including, where applicable, as regards the persons or groups of persons on which the high-risk AI system is intended to be used. These characteristics of the data sets may be met at the level of individual data sets or a combination thereof. DK: (Comments): The Commission has specified that the objective is not to achieve data sets which for example are free of errors – which in our view would be impossible to attain – but that this should be seen in connection with the state of art. In this light, the article needs to be clarified. Furthermore, the quality and appropriateness of the data sets should be measured against the intended

	purpose of the system. BE: (Drafting): Training, validation and testing data sets shall be relevant, representative~~, free of errors~~ and reliable ~~and complete.~~ BE: (Comments): Belgium supports to use "reliable data" sets instead of "free of errors and complete" to make the requirement practically implementable (in relation to the state of the art). ES: (Drafting): 3. Appropriate measures will be taken to ensure that training, validation and testing data sets shall be sufficiently relevant, representative, fairly free of errors and fairly complete, consistent with best practices in the state of the art. They shall have or be prepared to have the appropriate statistical properties, including, where applicable, as regards the persons or groups of persons on which the high-risk AI system is intended to be used and the domain to which they will be applied. These characteristics of the data sets may be met at the level of individual data sets or a combination thereof. When techniques such as differential privacy are used to prevent the unintentional disclosure of sensitive data are used, this will not

	be considered to be sistematically against to what is established in this article. ES: (Comments): It is impossible to find a 100% free of errors or completedata set. Data should be carefully treated not only because of geographical, behavioural or functional criteria. It should also take into account the domain to which it will be applied. **DELETED** SE:

	(Drafting): 3. Training, validation and testing data sets shall be sufficiently relevant, representative~~,~~ and free of errors and complete with regards to the intended purpose of the system. They shall have the appropriate statistical properties, including, where applicable, as regards the persons or groups of persons on which the high-risk AI system is intended to be used. These characteristics of the data sets may be met at the level of individual data sets or a combination thereof. SE: (Comments): Change is in accordance with recital 44 in the proposal and the following addition aims to ground the term "sufficient" and in the context of the intended purpose of the system. The aim is to soften the requirements as the initial formulation is too strict. The use of “inaccurate” or “dirty” data sets can be necessary for the development of some AI-systems, e.g. for detecting hate-speech online. FI: (Drafting): Training, validation and testing data sets shall be sufficiently relevant, representative, free of errors and complete. FI:

	(Comments): The requirement for the quality of data may be difficult to meet in practice. The requirement should be met only to the extent possible and where feasible. See the amendment in this paragraph.
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.	PT: (Drafting): Training, validation and testing data sets shall take into account, whenever possible, to the extent required by (…) **DELETED**

	ES: (Drafting): 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. Any constraint applied on these data sets will be specific to the domains to which the algorithms will be applied.
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	**DELETED** EE: (Comments): The corresponding recital (44) should refer to Article 9(2)(g) of Regulation (EU) 2016/679 as the basis for such exemption. ES:

process special categories of personal data referred to in Article 9(1) of Regulation (EU) 2016/679, Article 10 of Directive (EU) 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	(Comments): Evaluate whether any exemption to article 5.1.e of GDPR should be added, taking into account that maybe for a correct monitoring of bias, keeping a baseline of data during a extended period for the purpose of comparing could be useful (static datasets). We understand that the mentioned practices shoulds not violate GDPR (since bias monitoring could be a reason to consider a necessary action to keep that data), but it would be good to assess it.

measures, such as pseudonymisation, or encryption where anonymisation may significantly affect the purpose pursued.	
6. 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	**DELETED** DK:

systems comply with paragraph 2.	(Comments): As a technical remark, we are still unsure what this article is meant to cover and why this only partly covers article 10.
	FR: (Drafting): (New) **7. In order to comply with the requirements laid out in this article, the minimization principle shall be interpreted with consideration for the full life cycle of the system.** FR: (Comments): The minimization principle laid out in GDPR and its interpretation by EDPB shall take into account the necessity to retain some training evaluation and testing data, during the whole life cycle of the system.
Article 11 Technical documentation	PL: (Comments): Under analitical consideration CZ: (Comments):

	To Articles 11–14: CZ wishes to reiterate its comments from previous WP on these Articles. CZ suggests some specific guidelines clarifying all the open questions on who will control and enforce all the obligations and the entire process put in place in these Articles. Also maybe even some easy diagrams might help to understand the concrete steps which are needed and should be taken for a respective high risk AI system before it's put on the market.
	PL: (Comments): In the field of "high risk" artificial intelligence systems, technical documentation is an indispensable element of any production process of such a system. All the more, it should be an obligatory element in the production of an artificial intelligence system. Thanks to the technical documentation, it is possible to trace not only the purpose of creating an artificial intelligence system, but also its individual components, potential borrowing from other solutions (potential infringement of intellectual property rights, unfair practices, criminal aspects, intentionality, etc.). Regardless of the technique used for the production of an artificial intelligence system and its level of risk, the technical documentation should be compulsorily kept for each type of such system. It is worth emphasizing that the regulation should reconcile two values: on the one hand, consumer protection, and on the other hand, support innovation in the field of AI. The obligations of all artificial intelligence systems should be moderate in order not to suppress them in the

	EU area, the first victim of which will be EU consumers.
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.	
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	**DELETED**

provide national 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.	**DELETED**
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	CZ: (Drafting): 3. The Commission is empowered to adopt ~~delegated~~ implementing acts in accordance with Article 73 to amend Annex IV where necessary to ensure 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.

necessary to ensure 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.	CZ: (Comments): Annex IV related to technical documentation should be amended by implementing acts. DK: (Drafting): The Commission is empowered to adopt implementing acts ~~delegated acts~~ in accordance with Article 73 to amend Annex IV where necessary to ensure 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. DK: (Comments): We find that annex IV should be amended through an implementing act, as the technical documentation relates directly to the implementation and compliance of the high-risk requirements. Requirements which will not change in the process, therefore, implementing act is in our view the right instrument.
Article 12 Record-keeping	PL:

	(Comments): Under analitical consideration MT: (Comments): Malta welcomes the traceability and transparency elements introduced in the regulation, particularly under Articles 12 & 13. FI: (Comments): For how long must the records be kept?
1. High-risk AI systems shall be designed and developed with capabilities enabling the automatic recording of events	PL: (Drafting): High-risk AI systems shall be designed and developed with capabilities enabling the automatic recording of events (not limited to 'logs') while the high-risk AI systems is operating. Those logging capabilities shall conform to recognised standards or common specifications. **DELETED**

('logs') while the high-risk AI systems is operating. Those logging capabilities shall conform to recognised standards or common specifications.	**DELETED** DK: (Comments): It is still unclear to us what the logs should consist of in order for the provider to comply with this

	requirement. A list of minimum elements should be set out in the article. Furthermore, we are questioning why conformity with recognised standards or common specifications are explicitly mentioned in this article and not in other articles describing requirements for high-risk AI. Firstly, these are essential for operationalising most of the high-risk requirements. Secondly, by specifying that logging capabilities shall conform with these, recognised standards or common specifications would no longer be voluntary.
2. The logging capabilities shall ensure a level of traceability of the AI system's functioning throughout its lifecycle that is appropriate to the intended purpose of the system.	**DELETED** SE: (Drafting): 2. The logging capabilities shall ensure a level of traceability of the AI system's functioning

	throughout its lifecycle that is appropriate to the intended purpose of the system but no longer than ten years. SE: (Comments): Should be sufficient with ten years, which is the standard timeframe for record keeping.
3. In particular, logging capabilities shall enable the monitoring of the operation of the high-risk AI system with respect to the occurrence of situations that may result in the AI system presenting a risk within the meaning of	SK: (Comments): **SK:** Persons with lawful access to logs need to be specified.

Article 65(1) or lead to a substantial modification, and facilitate the post-market monitoring referred to in Article 61.	
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).	
Article 13 Transparency and provision of information to users	PT: (Comments): [please see comment to Article 29/2] PL: (Comments): support MT: (Comments): Malta welcomes the traceability and transparency elements introduced in the regulation, particularly under Articles 12 & 13.
1. High-risk AI systems shall be designed and	PT: (Comments):

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.	We would like to draw the attention to the fact that, of expressions such as "sufficiently transparent" or "appropriate type of degree of transparency" seems likely to allow those who make them available, a high degree of discretion in (self)evaluating the level of transparency of their own systems. PL: (Comments): This provision again focuses solely on "High-risk" AI systems. Transparency and disclosure of information to users in the case of using artificial intelligence should take place at every contact with an artificial intelligence system - not only in the field of high-risk systems. The consumer should know what risks and consequences are involved in order to be able to make a rational decision before buying, using or any other activity that may have legal consequences for him. The provision of Article 11 - in the light of recital 47 - is aimed at, inter alia, mitigating anti-consumer black-box effects. Due to the relative threats resulting from the use of high-risk artificial intelligence systems, its use in relation to this category is appropriate. However, it should not be used universally as it would be asymmetric for "less risky" systems **DELETED**

	DELETED EE: (Drafting): 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 in order to allow for the effective protection of rights where an AI system may cause harm to health, safety or fundamental rights.** EE: (Comments): Transparency requirements are vital in order to be able to effectively identify and remedy harm to health, safety or fundamental rights. The text should clarify that the transparency requirement must enable effective protection of health, safety and fundamental rights, for example, to ensure that if the decision

	undertaken by the user of AI system affects third persons, the user is able to provide sufficient explainability or transparency to the individuals, in order to safeguard the rights and freedoms of such individuals. Transparency is also important to ensure the right to an effective remedy. The corresponding recital should be amended accordingly. **DELETED**
2. High-risk AI	PT:

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 comprehensible to users.	(Drafting): High-risk AI systems shall be accompanied by instructions for field testing and use in an (…) PT: (Comments): Specific tasks of system test in operational conditions should be included as mandatory as pre-requirement for the use of the high-risk AI systems. PL: (Comments): instead of the phrase "in an appropriate digital or other format" suggest shift "on a “durable medium" (see e.g. Directive 2007/64 /) DK: (Comments): It could be useful with further clarification on the information required to be presented to the user. A template could also prove helpful in this regard. FI: (Comments):

	The concepts of ”conciseness, completeness and correctness” need clarification.
	ES: (Drafting): 3. The High risk AI system will inform its users about the rules, instructions and mechanisms on which such systems base their outputs or decisions.
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:	SE: (Comments): In law enforcement there is often a need to keep certain abilities secret, even internally. For example, if you have the ability to get into a specific hardware, that information needs to be protected from leaking. For example, in the case of EncroChat and Sky ECC, it was very important not to reveal what was actually known, similar conditions exist in many situations.
(i) its intended purpose;	
(ii) the level of accuracy, robustness and cybersecurity referred to in Article 15 against which the high-risk AI system has been tested and validated and which	PT: (Drafting): (ii) the level of accuracy, robustness and cybersecurity referred to in Article 15 against which the high-risk AI 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, including the appropriate statistical properties as referred to in Article 10(3) of the data sets used to train the system, to support operational testing before use, comparing these provided statistical properties with

can be expected, and any known and foreseeable circumstances that may have an impact on that expected level of accuracy, robustness and cybersecurity;	similar statistical properties of data input foreseeable to be found in the operational environment where the system shoud be deployed; PT: (Comments): We consider a good practice to perform an assessment of the operational environment where the system will be used. Comparing the statisticals properties of the data sets used to train the system with a data sample of the population where the system should be deployed, allows the user to assume a more protective behaviour in the future use of the system, in particular if the two sets of statisticals properties differ substantially.
	PT: (Drafting): **(iii) the specific parameters used in testing the system;** **(iv) the real conditions of normal use "in the field";** PT: (Comments): Considering the list of information specified in the list in Article 13(3), it appears that results generated in the testing phase - for instance, in terms of performance and accuracy - will be sufficient to satisfy the

	requirements which the rule is intended to cover. However, as experience has shown, these results can be substantially different when the system is tested in a real environment. We would therefore suggest adding to the list a requirement to make available information about the real conditions of normal use of the system and about the parameters used in testing it. Also, the possible ways in which those subjected to the system may be adversely impacted by it could be of some added value.
(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;	FR: (Drafting): (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~~; FR: (Comments): It is too difficult to predict cases of possible misuse

(iv) its performance as regards the persons or groups of persons on which the system is intended to be used;	PT: (Drafting): (iv) its performance as regards the persons or groups of persons on which the system is intended to be used **and indication on the possible ways in which they may be adversely impacted by it.**
(v) when appropriate, specifications for the input data, or any other relevant information in terms of the training, validation and testing data sets used, taking into account the intended purpose of the AI system.	

	PT: (Drafting): (vi) esplanatory data recorded during the development of the system to support the field test as referred to in Article XX (new proposed article futher in this document) PT: (Comments): We propose to mention technics such as Explainable Artificial Intelligence (XAI), referred in the EC Communication regarding Artificial Intelligence for Europe. The use of these technics should be encouraged given the fact that these can help the debugging and auditing activities previous to the deployment and need for human oversight.
(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	FI: (Comments): FI views that the requirement concerning human oversight over artificial intelligence systems needs to be clarified and specified.

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 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.	
	PT: (Drafting): <new article> Subject: Field Testing 1. Users of high-risk AI systems should, whenever possible, be encouraged to use the data provided by the supplier, as referred to in Article 13, to develop a field test of the system using their own historical data including: a) the execution of statistical tests on their own historical data to verify that the statistical properties are compatible with those provided by the supplier in accordance with the provisions of Article 10; b) the placing of the high risk AI system running in a controlled environment (sandbox) using their own classified historical data to verify that the performance of the high risk AI system is compatible with the metrics referred to in Article 13 and Article 15. 2. Users of high-risk AI systems should, whenever possible, be encouraged to run a battery of tests on the explanations provided by the system in order to:

	a) test the meaning of the explanations and their level of significance for different test groups; b) compare the explanations obtained with those provided by the provider in accordance with Article 13. PT: (Comments): We suggest adding an article to regulate or just suggest the test phase of AI solutions in order to mitigate already identified risks of high-risk AI systems and/or adicionally new risks that should be discovered in the new environement where the system is to be deployed. Comparing the statisticals properties of training data with the statisticals properties of future data inputs should be considered a good pratice. Additionally, we also propose to mention technics such as Explainable Artificial Intelligence (XAI), referred in the EC Communication regarding Artificial Intelligence for Europe. The use of these technics should be encouraged given the fact that these can help the debugging and auditing activities previous to the deployment and need for human oversight.
Article 14 Human oversight	PT: (Comments): W recommend defining the concept of “effective human oversight” and the specific results this article intends to seek. In our view, “human oversight” differs depending on the deployment scenario and the nature of the related risks. Consequently, we recommend that the proposed Regulation requires deployers

	to implement sufficient, qualified human oversight as is appropriate to the deployment scenario at issue. It is also important to bear in mind that for the "human oversight" to be meaningful and successful it is necessary to ensure that the humans performing the oversight are trained and equipped appropriately in accordance with the instructions of use and other information provided by the supplier. Additionally, the oversight should be tied to the intended use of the AI system and accountability mechanisms should be created to assess the effectiveness of the human overseer. [Please see comment to article 29/3] PL: (Comments): The obligation as defined in Art. 14 should be implemented, for the protection of (customers) consumers, in relation to all artificial intelligence systems, not only "high-risk artificial intelligence systems MT: (Comments): Malta notes that human oversight is also a welcome addition. Malta suggests that Article 14 should be revisited to introduce more balanced terms with regards to human oversight, in particular here, supervising and demonstrating adherence to concepts of authority as well as competence can be somewhat disproportionate on operations.

	DK: (Comments): When categorized as high-risk AI, we are generally positive towards having a requirement of appropriate and proportionate involvement of human oversight in the specific AI application, meaning that ability to intervene, reverse the output etc. However, as currently outlined, it is unclear how this requirement should work in practice or how providers and users can comply with this requirement. For example, it will be difficult for providers to design measures which enables the individual to whom human oversight is assigned to fully understand the capacities and limitations. Such aspect would also be interlinked with the competences of that specific individual.
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 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 measures:	
(a) 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) 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.	
	PT: (Drafting): **(c) identified by the user, defining non-technical organisational measures to ensure robust human supervision, consisting of at least training for decision-makers, registration requirements, and clear *ex-post* review processes.** PT:

	(Comments): In our opinion, it is still not sufficiently clear whether the human supervision measures in Article 14 apply to the user or to someone independent from the user, or even whether "user" refers to the organisation using the AI system as a whole or to a specific individual who is responsible for a particular decision. In fact, we believe that supervision is necessary for all actions related to the development, implementation and use of AI systems, to ensure that fundamental rights are protected in the best possible way at every stage. This will include, of course, human supervision of the process, but also regular and independent human supervision of the very people who participate in it and who are ultimately responsible for making the final decision, informed by the outputs produced by the system. It is not enough, therefore, to know whether supervisors are properly aware of the possibility of bias, but it must also be possible to demonstrate, transparently and effectively, that the actual decisions were not taken on the basis of excessive confidence in the outputs produced by the system. We, therefore, believe it is advisable to add a third category to Article 14(3) that adequately recognises the need for users to put in place organisational measures to ensure robust human supervision, consisting of at least: training for decision-makers, registration requirements, and clear ex-post review processes.
4. The measures referred to in paragraph 3 shall enable the individuals	SK: (Comments): **SK:** Qualification of persons responsible for human oversight should be specified.

to whom human oversight is assigned to do the following, as appropriate to the circumstances:	
(a) fully 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	**DELETED** ES: (Drafting): (a) have sufficient training with regards the AI system and oversight methods and ~~fully~~ adequately understand the capacities and limitations of the high-risk AI system, including the impacts that may arise in each use case, 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;

addressed as soon as possible;	ES: (Comments): Fully understand a system could be impossible. Having training on the Ai system must be specified. SE: (Drafting): (a) ~~fully~~ 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; FI: (Comments): "full understanding" needs clarification as well as the relationship with the "intended purpose".
(b) remain aware of the possible tendency of automatically relying	FI: (Comments): What is actually meant by "natural persons"? If it refers also to consumers (as a contrast to the "users", which refers to professional use only), the requirement might not serve the purpose of making the use of

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;	AI systems safe. This is because the consumers do not pose such thorough understanding of the systems that is needed for effective oversight and the safe interference of the functioning of the system. The safe deployment and use of AI systems requires that the systems are capable of handling e.g. system failures in a safe manner on their own ("fail-safe)
(c) be able to correctly interpret the high-risk AI system's output, taking into account 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.	
	ES: (Drafting): (f) being able to assess the efficiency of the oversight processes, so they can optimized under the light of the experience of having practiced such human oversight on the given AI system.
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	PT: (Drafting): ~~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 verified and confirmed by at least two natural persons.~~ OR 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 verified and confirmed by at least two natural persons, **based on a separate/independent assessment by each of them.** PT:

been verified and confirmed by at least two natural persons.	(Comments): In our opinion, reliance on human supervision as a sufficient safeguard should only be considered when it is possible to prove that the use of intrusive systems is necessary and proportionate in a democratic society, preventing it from functioning to legitimize the use of technologies that should not be used in light of their potential to violate fundamental rights. We would therefore reiterate that human supervision cannot act as a panacea for the (very serious) problems that the use of certain systems can give rise to, and consequently cannot be used to validate and – by that way, legitimize – that system or its use in a given context. In order to ensure any useful effect to this provision, the verification carried out by at least "two natural persons" **should be based on a separate assessment by each of them.** For example, by requiring that one is 'in the field' to identify, or 'spot', the individual in question from a different perspective, rather than reducing this requirement to a verification made by two people side-by-side looking at the same screen. CZ: (Comments): During the workshops a questions was raised, whether the 4 eyes principle did not violate judicial independence. The Commission answered that this was not applicable to courts but rather to initial assessment of the outputs of a RBI system. It would be appropriate to explain this in the relevant recital. ES: (Drafting):

	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 verified and confirmed by **one** natural person with sufficient qualification concerning AI / regulation (to be further developed) and concerning risks associated to Remote Biometric Identification Systems. ES: (Comments): The frequency of use of biometric identifiers, especially in border management, should not be lost of sight. The obligation of double verification could greatly complicate its operation and could force to have an unreasonable availability of human resources with adequate training in EEMMs. It should not be lost sight of the fact that the whole system of police decisions is subject, always and in any case, to judicial control (with the possibility of appeal). FR: (Drafting): 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 verified and confirmed by at least ~~two~~ **one** natural persons.

	FR: (Comments): Burdensome, we could limit this to one natural person. In principle, human verification and confirmation seems acceptable. However, despite COM's explanation on the "four eyes" rule, this will require some kind of procedural formalization in order to be adequately registered in the records. Therefore, it would be relevant to leave some latitude to MS in the practical application of this principle. We believe that in terms of allocation of human resources and of practical application of that obligation, verification by two persons is excessive.
Article 15 Accuracy, robustness and cybersecurity	PL: (Comments): support SK: (Comments): **SK:** A closer inter-linkage between EU cybersecurity certification may be considered, beyond what is already proposed (art. 42 (2), 47, 54, 61, 62, 65-67). Cybersecurity dimension of AI systems is crucial and may require a special analysis or opinion by ENISA or other similar authority.

	CZ: (Comments): It would be benefitial if the Commission develops in more detail on how this provision will interact with EU cybersecurity regulation, notably with the Act on Cybersecurity, the currently negotiated NIS2 directive and the CER directive (resilience of critical entities). As the Article itself refers to accuracy, robustness and cybersecurity and resilience, what does it mean for the concrete providers of a high risk AI system? Will it suffice for them to comply simply with Article 15 as a general precondition for a basic safety and cyber security of AI products and services, or will this Article de facto oblige the AI providers to comply with the key cybersecurity legislation? It would be useful to have this specified explicitly in the AIA. EE: (Comments): For the sake of the regulation being future proof, recital 50 needs to be supplemented or Article 15 interpreted in such a way as to avoid system instability due to problems other than the possibility of biased output due to feedback loops. Often the problem is not that the outputs are used as inputs, but that the outputs have an indirect effect on future inputs, including potential changes in human behaviour aimed at abusing limitations of the artificial intelligence system. FI:

	(Comments): The concrete requirements for an accurate level of cybersecurity should be clarified.
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.	PT: (Comments): According to the proposed Regulation the "high-risk AI systems shall be designed and developed in such a way that the 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." However, it is not defined what it means "an appropriate level of accuracy, robustness and cybersecurity", is 90% accuracy appropriate or 70%? And does the appropriate level changes depend on the context? If it is a critical infrastructure or a system used in a factory? We strongly recommend the development of best practices and standards do define these and other concepts.

2. The levels of accuracy and the relevant 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	PT: (Comments): We recommend reviewing the first paragraph of this article, taking into account the definition of "intended purpose" set in article 3, number 12 of the proposed Regulation. Please note that it is not possible to ensure that AI systems are 100% resilient to errors, faults, or inconsistencies. The uncertainty is part of the AI system. We also suggest adding the importance of quantifying this uncertainty, given its high impact on other topics addressed in this proposal, such as the risk of AI systems.

interaction with natural persons or other systems.	**DELETED** ES: (Drafting): 3. Appropriate technical and organisational measures will be taken to ensure that 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, consistent with the state of the art, in particular due to their interaction with natural persons or other systems, taking into consideration the seriousness of errors of the algorithm. Additionally where applicable, the system will include methods to minimize the probability of successive similar errors.

The robustness of high-risk AI systems may be achieved through technical redundancy solutions, which may include backup or fail-safe plans.	PT: (Drafting): The robustness of high-risk AI systems may be achieved through technical redundancy solutions, which may include backup or fail-safe plans, **such as the inclusion of mechanisms that prohibit some unexpected system behaviours, including preventing the system from operating, if inputs or outputs fall outside a predefined "safe" range.** PT: (Comments): To help shape the standardisation process appropriately, further clarification and indicative examples could be added in article 15.
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	DK: (Comments): This seems to establish a separate category of AI, instead we find that this could be a characterisctic in terms of defining AI. The HLEG also states in their updated definition that "AI systems can also be designed to learn to adapt their behaviour by analysing how the environment is affected by their previous actions." Further, this characteristic could also be relevant for other requirements besides article 15.

possibly biased outputs due to outputs used as an input for future operations ('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.	
Chapter 3	
OBLIGATIONS OF PROVIDERS AND USERS OF HIGH-RISK AI SYSTEMS AND OTHER PARTIES	DK: (Comments): We are supportive of differentiating obligations depending on the specific placement in the value chain. However, when it comes to the obligations of the provider and the user, the interface between the two is not always clear. Furthermore, we are still assessing whether we need a more nuanced distribution of roles – and thereby a more nuanced distribution of obligations - in order to reflect the AI ecosystem, where there are different routes of developing an AI system, for example by building on top of existing systems, using open-source code development etc. SE:

	(Comments): Article 16-29 need to be reviewed and re-made. Instead of disproportionately imposing requirements on the structure of work within companies, what is illegal (not desirable) should be regulated. The legislation should not lay down new administrative requirements, but specify what is not desirable, that is, what is illegal. Creating a large compliance structure for good technology support is unfortunate, complicated and unwarrantedly burdensome. The use of AI does not withdraw an employer of responsibility under applicable national nor international laws and regulations. Should there be insufficient regulation in certain areas, these should be complemented rather than implementing regulation targeted one specific technology. If there are to be administrative requirements, these need to be different depending on the type of company and the industry, for example, SMEs do not have the same conditions as multinational enterprises. As it stands now, SMEs should receive targeted information and lower fees.
Article 16 Obligations of providers of high-risk AI systems	PL: (Comments): The correct distribution of responsibilities between the various participants of the artificial intelligence value chain raises doubts (who/when). Also with relation of user/or end-user.

	SK: (Comments): **SK:** Obligations need to be distributed among operators in such a way so that they realistically reflect the complex value chains in AI and do not stifle innovation. For more details see above comments to article 3 (4). Moreover, Slovakia notes that the proposal does not contain any enforceable material and procedural rights of affected persons which would possibly correspond to the obligations of operators. Specific rights and effective tools of protection need to be considered, also in light of the awaited "digital principles and rights" to be declared in common EU inter-instituional declaration. A timely and effective protection of fundamental rights in AI-driven cyberspace may be difficult for many reasons, a limited effectiveness of horizontal effect of fundamental rights towards private parties and slowness of off-line proceedings being two of those. It appears impractical, ineffective and costly to burden operators with an additional obligation of *ex ante* fundamental rights/health impact assessment. A special environment for policy prototyping (such as special testbeds, representative testing groups, TEFs etc.) could be created to inform necessary amendments resulting from a continous assessment of sensitive use cases encroaching upon fundamental rights and health. Such activity, including necessary amendments of lists of use cases could be delegated to an independent EU authority, while respecting the *Meroni* line of case-law of CJEU.

Providers of high-risk AI systems shall:	
(a) ensure that their high-risk AI systems are compliant with the requirements set out in Chapter 2 of this Title;	DK: (Comments): Some of these requirements such as human oversight are addressed towards the user. This should be reflected in order not to make the provider responsible for all requirements.
(b) have a quality management system in place which complies with Article 17;	ES: (Drafting): (b) have a ~~quality~~ management system in place which complies with Article 17; ES: (Comments): See explanation in art. 17

(c) draw-up the technical documentation of the high-risk AI system;	**DELETED**
(d) when under their control, keep the logs automatically generated by their high-risk AI systems;	DK: (Comments): We find it necessary to define what is meant by under their control.
(e) ensure that the high-risk AI system undergoes the relevant conformity assessment procedure, prior to its placing on the market or putting into service;	BE: (Comments): For the major part of high-risk AI systems, the conformity assessment seems to be a self-assessment (see art. 43). In the field of the administration of Justice, e.g., one can wonder whether this system of self-assessment ex ante by the provider of the high-risk AI system in question

	- will be sufficient, concerning the potentially large impact of this kind of use? - will be efficient, concerning the apparent undercapacity for control and enforcement ex post, at least in a first stage? (see explanatory memorandum, 5.2.3, last paragraph, that states that "expertise for auditing is only now being accumulated") - will be feasible and not overly burdensome, e.g. for Startups and SME's? FR: (Comments): Ongoing work by FR experts.
(f) comply with the registration obligations referred to in Article 51;	
(g) take the necessary corrective actions, if the high-	CZ: (Comments):

risk AI system is not in conformity with the requirements set out in Chapter 2 of this Title;	Regarding Art. 16 (g) to take "*the necessary corrective actions*": What is meant by this term? Who will determine what is necessary in a respective case and how will the "*knowledge about nonconformity*" be treated? We suggest incorporation of these terms into Article 3.
	DK: (Drafting): h) 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 possible, on its packaging or its accompanying documentation, as applicable; DK: (Comments): As a technical remark, importers are obligated to provide this information, cf. article 26(3) which should be also be relevant in the case of a provider. Otherwise this information would not be accesible, unless an importer can be identified.
(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-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;	SE: (Comments): Still unclear how CE-marking requirement are to correspond to for example the CSA and cyber security certification. Should be clarified.
(j) upon request	**DELETED**

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.	**DELETED** CZ: (Comments): Regarding Art. 16 (j) on demonstration of the conformity of the high-risk AI system: What will the national authority require in practise? A list of all criteria as foreseen by Chapter 2 or also a real time demonstration of some/all of them? It would be beneficial to have this clearly defined in the regulation.
	PL: (Drafting): k) have a document confirming the fulfillment of the obligation to conclude a contract Insurance
Article 17 Quality management	PL:

system	(Comments): Under analitical consideration ES: (Drafting): Article 17 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	**DELETED**

manner in the form of written policies, procedures and instructions, and shall include at least the following aspects:	**DELETED** ES: (Drafting): 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: ES: (Comments): Many AI companies already have management systems that could be adapted to ensure compliance with this Regulation. In contrast with quality management sytems, very used in manufacturing, management systems that are in place could be reused for the purposes of this Regulation, bringing less costs to companies. This is particularly important for SMEs. FI: (Comments):

	FI considers it important to ensure proportionality and accuracy also with regard to data management and data quality requirements for artificial intelligence systems
(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;	
(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	DK: (Comments): It should be clarified what the benchmark is for being compliant with the requirement on examination, test and validation procedures before, during and after the development of the high-risk AI system.

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 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 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	CZ:

aspects referred to in paragraph 1 shall be proportionate to the size of the provider's organisation.	(Comments): The expression "shall be proportionate to the size of provider" is too vague. Who and how will decide the adequacy? CZ supports proportionality but clearly set, preferably with clear exemption e.g. for small enterprises. EE: (Comments): Although the purpose of the requirement to take into account the size of the provider's organisation is understandable and right, it is not clear to what extent can a company be released from specific obligations. Thus, these provisions do not provide the necessary legal clarity and legal certainty and may lead to unequal treatment. Additional clarifications should be considered. SE: (Comments): Proportionate to "size" in what sense? There's a lack of reference point for the interpretation of "proportionate". This could in practice generate discriminatory effects on organisations with a high number of employees but without no/ small revenue on one hand, and organisations with a small number of employees but with high revenues on the other hand.

3. For providers that are credit institutions regulated by Directive 2013/36/ EU, the obligation to put a quality management system in place 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	CZ: (Comments): We suggest the deletion of the Annex III 5 (b) and incorporation of the Annex III to the main legislative text. If this Article aims also to other applications than those listed in Annex III 5 b), it should be specified. Also similar exemption should be considered for a broader range of financial institutions regulated and overseen by relevant authorities. Additional requirements for credit institutions regarding AI risk assessment and compliance specific requirements in the draft AI regulation could be, especially in light of their other obligations, overly burdensome for these institutions. This should be discussed and evaluated on the appropriate platform. Given that the EC proposal amending the CRD is due to be discussed at ECOFIN on 9 November, it would be preferable to remove references to the CRD from the draft AI Regulation and discuss the proposed obligations in the context of the CRD legislative process. **DELETED** ES:

40 of this Regulation shall be taken into account.	(Drafting): 3. For providers that are credit institutions regulated by Directive 2013/36/ EU, the obligation to put a ~~quality~~ management system in place 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. ES: (Comments): 'quality' removed.
Article 18 Obligation to draw up technical documentation	PL: (Comments): Under analitical consideration
1. Providers of high-risk AI systems	**DELETED**

shall draw up the technical documentation referred to in Article 11 in accordance with Annex IV.	**DELETED**
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	CZ: (Comments): We suggest the deletion of the Annex III 5 (b) and incorporation of the Annex III to the main legislative text. If this Article aims also to other applications than those listed in Annex III 5 b), it should be specified. Also similar exemption should be considered for a broader range of financial institutions regulated and overseen by relevant authorities. Additional requirements for credit institutions regarding AI risk assessment and compliance specific requirements in the draft AI regulation could be, especially in light of their other obligations, overly burdensome for these institutions. This should be discussed and evaluated on the appropriate platform. Given that the EC proposal amending the CRD is due to be discussed at ECOFIN on 9 November, it would be preferable to remove references to the CRD from the draft AI Regulation and discuss the

to Article 74 of that Directive.	proposed obligations in the context of the CRD legislative process.
Article 19 Conformity assessment	PL: (Comments): Under analitical consideration SK: (Comments): **SK:** See remarks on the entire proposal above. MT: (Comments): Malta notes that AI creates interdependancies with other countries outside the EU. The fact that the regulation does not recognize this is problematic, given the starting point of the EU AI market and the edge countries like China, Japan, India and USA and the interdependence needs that might be required. Limiting the EU regulation and measures to a regional as opposed to a global approach exacerbates its negative impact on trade, interoperability, innovation as well as global market presence.

1. Providers of high-risk AI systems shall 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	FR: (Comments): Ongoing work by FR experts. SE: (Comments): The obligation for the providers of high-risk AI systems to draw an EU-declaration and affix the CE marking of conformity in accordance with art. 48 would have a serious impact on LEA given the definition of an AI-system in combination with p.6(g) of Annex III as previously stated.

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	CZ: (Comments): We suggest the deletion of the Annex III 5 (b) and incorporation of the Annex III to the main legislative text. If this Article aims also to other applications than those listed in Annex III 5 b), it should be specified. Also similar exemption should be considered for a broader range of financial institutions regulated and overseen by relevant authorities. Additional requirements for credit institutions regarding AI risk assessment and compliance specific

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.	requirements in the draft AI regulation could be, especially in light of their other obligations, overly burdensome for these institutions. This should be discussed and evaluated on the appropriate platform. Given that the EC proposal amending the CRD is due to be discussed at ECOFIN on 9 November, it would be preferable to remove references to the CRD from the draft AI Regulation and discuss the proposed obligations in the context of the CRD legislative process. IT: (Comments): *It would be welcome if the Commission provided more clarification about the scope of the regulation with reference to the credit and financial sector.*
Article 20 Automatically generated logs	PL: (Drafting): Automatically generated logs or events PL: (Comments): From resiliance of AI's point of view the logs seem to be not enough

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 for a period that is appropriate in the light of the intended purpose of high-risk AI system and	SK: (Comments): **SK:** Log**s** retention period should be specified.

applicable legal obligations under Union or national law.	
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.	CZ: (Comments): We suggest the deletion of the Annex III 5 (b) and incorporation of the Annex III to the main legislative text. If this Article aims also to other applications than those listed in Annex III 5 b), it should be specified. Also similar exemption should be considered for a broader range of financial institutions regulated and overseen by relevant authorities. Additional requirements for credit institutions regarding AI risk assessment and compliance specific requirements in the draft AI regulation could be, especially in light of their other obligations, overly burdensome for these institutions. This should be discussed and evaluated on the appropriate platform. Given that the EC proposal amending the CRD is due to be discussed at ECOFIN on 9 November, it would be preferable to remove references to the CRD from the draft AI Regulation and discuss the proposed obligations in the context of the CRD legislative process. **DELETED**

	DELETED
Article 21 Corrective actions	PL: (Comments): Under analitical consideration CZ: (Comments): Article 21 makes space for very broad application on a case-by-case basis, as mentioned before, especially the part "have reason to consider that a high risk system (…) is not in conformity of the regulation" can significantly change in time. How it will be safeguarded that distributors will not be overwhelmed by such information obligation? Will for this purpose suffice a typical "bug notification" thus i.e. automatic software updates generated by the provider? It would be helpful if this is specified in the text.

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 take the necessary corrective actions to bring that system into conformity, to withdraw it or to recall it, as appropriate. They shall inform the	DK: (Comments): As a technical remark, we find it useful to extend this obligation, so that users would also be informed about such considerations of risks. SE: (Drafting): 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 the causes in open collaboration with the reporting user party and take the necessary corrective actions in order 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.

distributors of the high-risk AI system in question and, where applicable, the authorised representative and importers accordingly.	
Article 22 Duty of information	PL: (Comments): support CZ: (Comments): There is a risk that the national authorities, especially in middle sized and small Member States, might be overwhelmed with such information obligation. What will happen to the high-risk system after such notification?

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	**DELETED** FI: (Comments): Consider adding a duty for the national competent authorities to inform the natural persons affected.

and of any corrective actions taken.	
Article 23 Cooperation with competent authorities	PL: (Comments): support
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	**DELETED** DK: (Comments): In order not to subject a provider to 27 different request, it could be relevant to have some form of coordination and sharing of best practice between member states and enforcement guidance from the

high-risk AI system with the requirements set out in Chapter 2 of this Title, in 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	Commission in due time before the regulation is applicable. Furthermore, it would be relevant to stipulate format as well as level of abstraction when it comes to the information and documentation, as this could be necessary in order to validate the documentation. ES: (Drafting): Providers of high-risk AI systems shall, upon request by a national competent authority, in accordance with the detailed provisions set out in article 64 of this Regulation, 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 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.

user or otherwise by law.	
Article 24 Obligations of product manufacturers	PL: (Comments): Under analitical consideration CZ: (Comments): As the term “manufacturer” as such is not included in the list of terms and definitions of Art. 3, for the sake of legal certainty, we suggest adding this term in the list. BE: (Drafting): Article 24 Obligations of ~~product~~ manufacturers of the final product BE: (Comments):

	Cf. recital 55 where this wording is used as well (since there is no definition of 'manufacturer').
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	**DELETED** DK: (Comments): As a technical remark, this seems to refer more broadly to the products contained in the legal acts in annex II. However, it should specify that it is a product which is required to undergo third-party assessment.

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	PL: (Comments): support SE: (Comments): It is importat to ensure that rules regarding autorized representatives and others rules which concerns AI systems from providers outside of the EU do not impacts external trade to a larger externt than stricly

	necessary and are in line with EU:s commitments in trade agreements.
1. Prior to making their systems available on 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.	FR: (Drafting): 1. Prior to making their systems available on 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. FR: (Comments): The appointment of an authorised representative has to be foreseen where the provider is established outside the EU
2. The authorised representative shall perform the tasks	

specified in the mandate received from the provider. The mandate shall empower the authorised representative to carry out the following tasks:	
	FR: (Drafting): **Additional paragraph** **3. 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 together under the responsibility of an authorised representative, the authorised representative of the product shall fulfil the obligations imposed by the present Regulation on the authorised representative, together with the obligations imposed in the specific legal act listed in Annex II, Section A.** FR:

	(Comments): The obligations of authorised representative under Regulation 2017/745/EU on medical devices and under Regulation 2017/746/EU on in vitro diagnostic medical devices are different from those mentionned in the present proposal. All these obligations are not contradictory but the legal obligations of each economic operator have to be clearly stated.
(a) 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 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 system to the extent such logs are under the control of the provider by virtue	**DELETED**

of a contractual arrangement with the user or otherwise by law;	
(c) cooperate with competent national authorities, upon a reasoned request, on any action the latter takes in relation to the high-risk AI system.	PL: (Comments): The letters a and b describe the forms of cooperation between the representative and the national authorities. So, de facto they are covered by letter c. Therefore, this provision should be reworded
Article 26 Obligations of importers	PT: (Comments): The article foresee that importers and distributors should not place on the market or make the system available, and the difficulty is in determining whether an importer or distributor has established capabilities to recognize non-compliance for an AI system.

	PL: (Comments): Under analitical consideration CZ: (Comments): For the purpose of legal clarity, we suggest that it is clearly defined what an "appropriate conformity assessment" means and who will be responsible to decide that. The AI regulation does include the definition of conformity assessment in its Art. 3 and also further stipulates other conditions for it in Art. 19. However, Article 26 further adds to these requirements by need to comply with other obligations. We propose to adjust the wording of this and related Articles so that it is absolutely clear to the addressees of this regulation what is required and what exactly they need to fulfill. We strongly recommend creating some guidance or some example diagram, which will, step by step, explain to respective parties what concrete steps and when they should make in specific situations.
1. Before placing a high-risk AI system on the market,	**DELETED**

importers of such system shall ensure that:	**DELETED**
(a) the appropriate conformity assessment procedure 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 conformity marking and is accompanied by the required documentation and instructions of use.	
	DK: (Drafting): d) the provider has indicated 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 possible, on its packaging or its accompanying documentation, as applicable in accordance with Article 16(h). DK: (Comments): A remark which is in line with previous addition in article 16.
2. Where an importer considers or has reason to consider	

that a high-risk AI system is not in conformity with this Regulation, 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 possible, on its packaging or its accompanying documentation, as applicable.	FI: (Comments): The further processes should also ensure that the registration of high-risk AI systems in the EU database is appropriate and secure.
4. Importers shall ensure that, while a high-risk AI system is	**DELETED**

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.	**DELETED**
5. Importers shall provide national competent authorities, upon a reasoned request, with all necessary information and documentation to demonstrate the conformity of a high-risk AI system with	DK: (Comments): It is difficult to see why logs should be in the possession of the importer. These are not included in the technical documentation. FI: (Comments): The compliance with the obligations should not increase the threshold or result in delays for innovative development and market implementation. Moreover, it is considered important that the proposed

the requirements set out in Chapter 2 of this Title in a language which can be easily understood by that national competent authority, 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	regulation enables scientific research on artificial intelligence as well as business activities. The effects of the proposed regulation on companies' research, development and innovation activities need further clarification.

action national competent authority takes in relation to that system.	
	FR: (Drafting): **Additional paragraph** **6. 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 under the responsibility of an authorised representative, the authorised representative of the product shall fulfil the obligations imposed by the present Regulation on the authorised representative, together with the obligations imposed on the authorised representative in the specific legal act listed in Annex II, Section A.** FR: (Comments): The obligations of importers under Regulation 2017/745/EU on medical devices and under Regulation 2017/746/EU on in vitro diagnostic medical devices are different from those mentionned in the present proposal. All these obligations are not contradictory but the legal obligations of each economic operator have to be clearly stated.

Article 27 Obligations of distributors	PT: (Comments): The article foresee that importers and distributors should not place on the market or make the system available, and the difficulty is in determining whether an importer or distributor has established capabilities to recognize non-compliance for an AI system. PL: (Comments): Under analitical consideration
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 instruction of use, and that the provider and the importer of the system, as applicable, have complied with the obligations set out 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 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	PT: (Comments): This standard establishes characteristics and competences that should be of the exclusive responsibility of those who develop AI systems, considering that this obligation will be, once again, difficult to observe.

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 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	**DELETED** CZ: (Drafting): 4. A distributor that ~~considers or has reason to consider~~ finds out 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 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~~ without undue delay 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. CZ: (Comments): CZ understands that this provision shall provide for some sort of "internal autocorrection" and this is why it operates with terms such as "(...) XY considers or has reason to consider that a high risk AI system does

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.	not comply (....).” On the other hand, this provision seems rather vague and may lead to different levels of implementation and it is highly arbitrary, thus for some distributors this might be vague and lead to confusion. The same applies to the term “immediately”, what does this mean and how shall the distributor inform such an authority? Via email, phone, prescribed notification? Via an online application? Would the term “without undue delay” be more suitable with this regard as it is common in legal terms?
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 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 on any action taken by that authority.	
	FR: (Drafting):

	Additional paragraph **6. 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 under the responsibility of a distributor, the distributor of the product shall fulfil the obligations imposed by the present Regulation on the distributor, together with the obligations imposed on the distributor in the specific legal act listed in Annex II, Section A.** FR: (Comments): The obligations of distributors under Regulation 2017/745/EU on medical devices and under Regulation 2017/746/EU on in vitro diagnostic medical devices are different from those mentionned in the present proposal. All these obligations are not contradictory but the legal obligations of each economic operator have to be clearly stated
Article 28 Obligations of distributors, importers, users or any other third-party	PT: (Comments): It refers to “other third parties”, but who are they are: users, distributors, suppliers? PL: (Comments):

	Under analitical consideration CZ: (Comments): We suggest either moving this Article or renaming the title of this Article as it is sort of a general obligation applicable to all key parties of this Regulation, in case they act in a manner prescribed by this Article. As this Article is a sui generis edition to the obligation of providers, it might make more sense if this is structured together with the provisions on the obligation of providers. DK: (Comments): We agree that obligations should follow the right actor in the value chain, however, at the moment, we foresee some difficulties and unclarity with this article. We are concerned that we could create a scenario where a provider would define the intended use very strictly in order not to be liable for other use cases, thereby, making article 28 the rule rather than the exception. If a user becomes a provider, it will then mean that the now provider must go through a new conformity assessment. In many cases, especially for SMEs, this would probably not be feasible and the regulation might stiffle AI-uptake among SMEs which would be contrary to the Commission's proposal for 2030 digital targets. In this respect, we are still reflecting on this article.

1. Any distributor, importer, user or other third-party shall be considered a provider 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:	**DELETED**
(a) they place on the market or put into service a high-risk AI system under their	FR: (Drafting): (a) they place on the market or put into service a high-risk AI system under their name or trademark,

name or trademark;	**except in cases where a distributor or importer enters into an agreement with a provider whereby the provider is identified as such on the label and is responsible for meeting the requirements placed providers in this Regulation**;
(b) they modify the intended purpose of a high-risk AI system already placed on the market or put into service;	PT: (Comments): The topic is unclear about the intended purpose change. Perhaps the definition is too broad and therefore brings uncertainties PL: (Comments): art. 28 (1) (b) - in accordance with Art. 2 clause 3 the use of AI systems for military purposes is excluded from the scope of the regulation. If a system produced and used for military purposes (e.g. an explosives analysis system) will be handed over to law enforcement agencies, e.g. the police, to perform its tasks, and therefore will the AI system, specified in Art. 28 sec. 1 lit. b, whether the police will have to comply with the requirements for high risk systems as set out in ch. 2. And whether it will be necessary again in such a situation, eg training of data taking into account the new purpose of the system? **DELETED**

	DELETED SE: (Comments): The difference between the definition of "substantially modify" as stated in the first paragraph of art. 3.23, and the obligations following art. 28.1(b) "modify" is too ambiguous. Art. 28.1(b) should state "**substantially** modify".
(c) they make a substantial modification to the high-risk AI system.	PT: (Comments): The article is unclear about the "substantial change". Perhaps the definition is too broad and therefore brings uncertainties **DELETED**

	DELETED EE: (Comments): There may be a significant number of situations where due to data protection, security or other considerations, the user is not interested in or is restricted in making available to the provider all data related to the use of the AI system that would be needed for the provider to ensure compliance with its obligations laid out in Article 16. For such situations, EE encourages to establish a right enabling the user to assume obligations of the provider, even if the development of any modifications of the AI system remains with the original provider. FR: (Drafting): (c) they make a substantial modification to the high-risk AI system**, in such a way that compliance with the applicable requirements may be affected**.

	ES: (Drafting): (d) they modify the intended purpose of one or more general purpose AI systems that is available in the market in order to deploy a high-risk AI system. (e) they use a high-risk AI system without introducing modifications to it, but combine it with other AI systems or with other software component, resulting in a new software solution. In cases where the original provider made available its AI system to a third party for the purpose of placing a new AI system on the market or into service using the frist one, the original provider will offer due information and support to the new provider with the purpose of allowing it to achieve an effective compliance with the requirements set out in Chapter II of Title III of this Regulation. ES: (Comments): Practical example: if a provider uses an existing AI model or a general purpose AI model of Google or Microsoft (for example) via API, it will be necessary for the developer to have the information and support concerning, among other things, training, techniques used or accuracy in order to comply with obligations.

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.	**DELETED**
Article 29 Obligations of users of high-risk AI systems	PL: (Comments): Under unalitical consideration CZ:

	(Comments): CZ would like to learn more details from the Commission on the practical implementation of this entire provision. We do understand, that for sake of legal certainty, the Regulation tries to cover all key parties which in any matter somehow interact and are involved in developing, placing in the market and use of high risk AI systems. For this reason, the regulation stipulates 4+ key categories (providers, distributors, importers and users), and provides for a basic set of obligations. However, in real life, the 4 basic categories may not only merge in one but they may also change and develop in time. This means that a user of a high risk AI system can also, in some cases, be a provider or distributor and vice versa. Thus how does the Regulation treat such categories? It would be useful to have this clearly explained in the text. MT: (Comments): Malta notes that since AIs are integrated in most of the medical devices and the innovative solutions with relevant IPAs, thereby, relevant safeguards linked to MDR are also more exhaustive than the latter, need to be in place so as not to jeopardise safety and quality.
1. Users of high-risk AI systems shall	

use such systems in accordance with the instructions of use accompanying the systems, pursuant to paragraphs 2 and 5.	
2. The obligations in paragraph 1 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	PT: (Comments): With regard to the problem of "explainability", Article 13 specifies that "high risk" AI systems must be developed and designed to be sufficiently transparent to ensure the user's ability to interpret and use the results of the system. **However, it does not include an explicit obligation on the user to communicate such information to the persons targeted by the decision supported by Artificial Intelligence** (the only transparency obligation towards these persons is stipulated in Article 52, but limited to the duty to inform them of the fact that an Artificial Intelligence system is being used). **The Proposal does not, as such, include obligations on users of Artificial Intelligence to explain or justify the decisions they take to those affected by them, let alone a corresponding right of these individuals to demand i**t. While they may be protected by the general right to a reasoned decision under Article 41(2c) of the Charter to fill this gap, the specific challenges its application raises when public bodies rely on these systems in their decision-making would

implementing the human oversight measures indicated by the provider.	justify the inclusion of additional safeguards**. Therefore, to avoid any doubt regarding the applicability of this right in the context of Artificial Intelligence it should be made clear in the text of the Regulation and the references used to assess compliance with this right should be duly included in the text of the Proposal itself.** As these aspects are central to the review, by the person targeted by decisions supported by these technologies, it would be important not to leave their densification to supervening disputes. EE: (Comments): EE encourages to further assess whether a limitation would be warranted to enable Member States to introduce transparency or other obligations for users of low-risk AI systems in situations where such systems are used by public sector actors (or on their behalf) for executing public tasks or providing public services. Without such limitation, wouldn't the Regulation undermine the possibility for MS to translate the abstract constitutional safeguards applicable to public procedure (e.g. transparency/explainability requirements) under the MS law into AI-specific requirements, in cases where low-risk AI is used within public procedure?
3. Without prejudice to paragraph	PT: (Drafting):

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.	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. **When using AI systems in their decision-making processes, public authorities or others acting on their behalf shall inform the persons affected by them whether or not other available information was used and if alternative results were considered.** PT: (Comments): Concerning the issue of "algorithmic bias", it is important to avoid that decisive importance is given to the result suggested by an algorithm while neglecting other available information, in which case the public authority can make the mistake of basing a decision on the argument "it is so because the machine determined it". To this effect, Article 14 of the Proposal requires that human supervision must be ensured in order to allow the person assigned this task to correctly interpret the results and be aware of the potential bias. While welcoming the explicit consideration of such matter, we believe it would be important to combat it more effectively by requiring additional safeguards, for example by obligating the public authority that relies on AI systems for its decision-making to report whether or not it has used other available information or considered alternative results in issuing its decision.

4. Users shall monitor the operation of the high-risk AI system on the basis of the instructions of use. When they have reasons to consider that the use in accordance with the instructions of use may result in the AI system presenting a risk within the meaning of Article 65(1) they shall inform the provider or distributor and suspend the use of the system. They shall also inform the	

provider or distributor when they have identified any serious incident or any malfunctioning within the meaning of Article 62 and interrupt the use of the AI system. In case the user is not able to reach the provider, Article 62 shall apply mutatis mutandis.	
For users that are credit institutions regulated by Directive 2013/36/EU, the monitoring obligation	CZ: (Comments): We suggest the deletion of the Annex III 5 (b) and incorporation of the Annex III to the main legislative text. If this Article aims also to other applications than those listed in Annex III 5 b), it should be specified. Also similar exemption should be considered for a broader range of financial institutions

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.	regulated and overseen by relevant authorities. Additional requirements for credit institutions regarding AI risk assessment and compliance specific requirements in the draft AI regulation could be, especially in light of their other obligations, overly burdensome for these institutions. This should be discussed and evaluated on the appropriate platform. Given that the EC proposal amending the CRD is due to be discussed at ECOFIN on 9 November, it would be preferable to remove references to the CRD from the draft AI Regulation and discuss the proposed obligations. **DELETED**
5. Users of high-risk AI systems shall keep the logs	PL: (Comments):

automatically generated by that high-risk AI system, to the extent such logs are under their control. The logs shall be kept for a period that is appropriate in the light of the intended purpose of the high-risk AI system and applicable legal obligations under Union or national law.	art. 29 (5) - a request for clarification of what is meant by "a period appropriate to the purpose of a given high-risk AI system"? ES: (Drafting): 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. The logs shall be kept for a period that is appropriate in the light of the intended purpose of the high-risk AI system and applicable legal obligations under Union or national law and never inferior to xxx years. ES: (Comments): It is important to set a minimum value to ensure proof existence for administrative issues (penalties, etc.) or even if liability or penal trials appear.
Users that are credit institutions regulated by Directive 2013/36/EU shall	CZ: (Comments): We suggest the deletion of the Annex III 5 (b) and incorporation of the Annex III to the main legislative text. If this Article aims also to other applications than those listed in Annex III 5 b), it should be

maintain the logs as part of the documentation concerning internal governance arrangements, processes and mechanisms pursuant to Article 74 of that Directive.	specified. Also similar exemption should be considered for a broader range of financial institutions regulated and overseen by relevant authorities. Additional requirements for credit institutions regarding AI risk assessment and compliance specific requirements in the draft AI regulation could be, especially in light of their other obligations, overly burdensome for these institutions. This should be discussed and evaluated on the appropriate platform. Given that the EC proposal amending the CRD is due to be discussed at ECOFIN on 9 November, it would be preferable to remove references to the CRD from the draft AI Regulation and discuss the proposed obligations in the context of the CRD legislative process.
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	PL: (Comments): -art. 29 (6) - whether it is assumed that data processing that may result in a high risk of violating the rights and freedoms of natural persons referred to in art. 27 (1) LED (Directive 2016/680) will apply to all systems understood as high-risk systems under the AI regulation? What will be the difference between the risk management system provided for in Art. 9 as one of the provider's obligations to assess the effects of planned processing operations on the protection of personal data provided for in Art. 27 (1) LED as one of

assessment under Article 35 of Regulation (EU) 2016/679 or Article 27 of Directive (EU) 2016/680, where applicable.	the user responsibilities. It seems that the data protection impact assessment should be part of a wider risk management system, including planning of remedial measures. What is the rationale for formulating similar obligations at provider and user level? Is there no duplication risk? If the provider will also be a user, will he be able to assess the effects of the planned processing for data protection under the risk management system referred to in Art. 9? MT: (Comments): Malta welcomes more clarity on the interface between the GDPR and the draft regulation, particularly in instances, like for example, when we will have a High-risk Ai design with massive data protection angles (which is a human right). This might be captured by the GDPR under the data protection by design and default principles as well as the conformity assessment under the draft AI regulation. Potentially in case of breach it might also attract fines from both regimes, Malta would welcome more clarity to avoid unnecessary overlaps. SE: (Comments): Is the intention that the requirements of Article 13 shall form a "part" of the data protection impact assessment?

	PL: (Comments): It is postulated to introduce Art. 29a laying down requirements for suppliers in terms of transparency and making information available to users. The aim of the change would be to provide entities whose legal position depends on the operation of artificial intelligence systems with information about the features, possibilities and limitations of the effectiveness of the high-risk artificial intelligence system to the extent relevant from the perspective of a given service.
ANNEX I ARTIFICIAL INTELLIGENCE TECHNIQUES AND APPROACHES referred to in Article 3, point 1	**DELETED**

	DELETED SK: (Comments): **SK:** See comments on article 3 (1) – definition of AI system above. CZ: (Drafting): ~~ANNEX I~~ ~~ARTIFICIAL INTELLIGENCE TECHNIQUES AND APPROACHES~~ ~~referred to in Article 3, point 1~~ CZ: (Comments): Including the essential part of the definition of the AI system into Annex is fundamentally problematic.

	DK: (Comments): In line with our comments concerning the definition on AI, we find that techniques and approaches set out in b) and c) are too broad categories including traditional software which in our view cannot be considered as AI. BE: (Comments): This definition can be considered as very broad. It includes a lot of techniques that are not stricto-sensu AI. This large definition of AI can be problematic when combined with Annex III (High Risk systems referred to Art.6 (2) – 6(g) ES: (Comments): **General comments: a number of techniques (Bayesian estimation, statistical approaches) may raise confusion on what an AI really is (even though it was explained that the definition must be read as a whole of art. 3 and annex I). Clearly mentioning what is tried to be described on each point (learning, reasoning, modelling, interaction) would be useful. Additionally, it would be necessary to refine wording in order to ensure that AMD is not under the scope of the regulation.** SE:

	(Comments): Depending on the outcome of discussions on the definition of AI in art. 3.1 and the amendments to Annex I (delegated act) in art 4. SE sees a need for a review to ensure that the specification in the appendix does not allow for a broader definition than on the basis for the purpose of the proposal. The listed techniques in Annex I are too broad, and it includes techniques that are more related to data driven software development in general than AI (especially (b) and (c)).
(a) Machine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning;	**DELETED** CZ: (Drafting): ~~(a) Machine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning;~~ EE:

	(Drafting): (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;	PL: (Comments): In this category is needed to miss linear logic, statistic, and algorithms techniques not being consist for AI System. **DELETED** CZ: (Drafting): ~~(b) Logic- and knowledge-based approaches, including knowledge representation, inductive (logic)~~

	~~programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems;~~ EE: (Drafting): (b) Logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning ~~and expert systems;~~ EE: (Comments): Some of the techniques and approaches covered here should not be considered as AI. DK: (Drafting): ~~(b) Logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems;~~ FR:

	(Drafting): ~~Logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems;~~ FR: (Comments): The proposed definition is too broad. We could potentially remove point b completely in order to narrow the definition (or, at least, only for the applications covered under annex II where we already have some sectorial regulations)
(c) Statistical approaches, Bayesian estimation, search and optimization methods.	PL: (Drafting): ~~Statistical approaches~~, Bayesian estimation, ~~search~~ and optimization methods. **DELETED**

	CZ: (Drafting): ~~(c) Statistical approaches, Bayesian estimation, search and optimization methods.~~ EE: (Drafting): ~~(c) Statistical approaches,~~ Bayesian estimation~~, search and optimization methods.~~ EE: (Comments): Some of the techniques and approaches covered here should not be considered as AI, for instance "statistical approaches" is too wide to simply consider as AI. DK: (Drafting): ~~© Statistical approaches, Bayesian estimation, search and optimization methods.~~
	ES: (Drafting): (d) Game theory, social choice, Negotiation, Argumentation, Semantic alignment, Normative

	approaches (INTERACTION/COOPERATION). ES: (Comments): - we miss a fourth category, regarding systems interaction. Right now, there are three categories of techniques: Learning, Reasoning and Modelling. A third one involving INTERACTION techniques should be considered. A text is suggested for this purpose.
ANNEX II **LIST OF UNION HARMONISATION LEGISLATION** **Section A – List of Union harmonisation legislation based on the New Legislative Framework**	SK: (Comments): **SK:** See comments to article 6 above. MT: (Comments): Malta notes that on the basis of the analysis carried out thus far, the way in which the AI proposal will interact with the legislation listed in Annex II, further clarification needs to be sought. Whilst the Commission's Communication on the interplay between the AI proposal and the Machinery proposal is certainly a step in the right direction in this regard, further aspects would still require further clarification. As an example of such aspects, Malta notes how the proposal would consider the manufacturer of a product (captured within the scope of Annex II) which contains/incorporates an AI system to be

	responsible for compliance of the product with the AI Regulation, even though the product manufacturer is not in fact the manufacturer of the AI system. Malta stresses that whilst it may be acceptable that a certain degree of responsibility is placed on said manufacturer, particularly in terms of due diligence duties, it seems both reasonable and appropriate that the main responsibilities for the AI system in question are placed on the AI system manufacturer. With reference to the proposal's aim to regulate AI systems (whether standalone or incorporated in another product) which may, inter alia, cause physical and psychological harm, clarification should be sought on what category of physical harm is being targeted. In more defined terms, clarification should be provided on whether the proposal is targeting direct physical harm, indirect physical harm (e.g. harm resulting from damages suffered by the user usually due to malicious use by third parties) or both.
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);	
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);	
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);	
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 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).	
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);	
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 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); 3. 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);	
7. 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), 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.	
ANNEX III HIGH-RISK AI SYSTEMS REFERRED TO IN ARTICLE 6(2)	PL: (Comments): Preference: is amending Annex III in the form of a review and amendment of the regulation or implementing act, not a delegated act. SK:

	(Comments): **SK:** The use cases of AI systems operating certain forms of mobility and transportation, insurance products and services, protection of environment, tools of attention economy, journalism and creation and selection of content (beyond practices forbidden in article 5), including deep audio and textual/language fakes, health and safety protection in sensitive environments, biotech solutions (e.g. AI interacting with biological/organic systems) are not contained in this annex. The critical infrastructure appears too narrowly defined (for instance, it does not cover food, digital networks security and other fields). Moreover, the Digital Services Act does not seem to specifically address deployment and use of AI systems, therefore adequate safeguards need to be introduced into this proposal by including relevant use cases in this annex. All the above use cases need to be carefully considered in light of the criteria contained in article 7. See also comments to article 5 and 6 and Title III Chapter 2 and 3. CZ: (Drafting): ~~**ANNEX III**~~ ~~**HIGH-RISK AI SYSTEMS REFERRED TO IN ARTICLE 6(2)**~~ CZ:

	(Comments): Including the list of high-risk systems into Annex is fundamentally problematic and we ask for its incorporation into the legislative text so that it can only be changed by the standard legislative process. AT: (Comments): Irrespective of our scepticism regarding the amendments in Annex III through delegated acts, a more precise definition and more exact delimitation of the high-risk areas of application would be desirable in any case. Additionally, there should be a transition period for AI systems that are newly included in Annex III. EE: (Comments): EE encourages to clarify – in the text itself or the recitals – whether multifunctional AI systems (e.g. GPT-3) qualify as high-risk systems if they do not have a predominant "intended purpose" or if their primary function is not to be used in the manner specified in Annex III, but they nonetheless can be used for purposes indicated therein without requiring modifications. DK:

	(Comments): As outlined in our comments related to article 6, we find that the different use cases deserve further discussion in order to understand their scope and associated risks. BE: (Comments): Cf. comment on requirements for high-risk AI systems. FI: (Comments): The list in Annex III of high risk AI systems referred to in Article 6 (2) should be clarified. Especially point 5 Access to and enjoyment of essential private services and public services and benefits is very vague. As it reads now, it could be interpreted as to include mandatory insurance run by private insurance companies, which can sometimes in certain member states be classified as being part of social security (eg. motor insurance, workers´ compensation). It is probably not the intention to include such mandatory insurance as high risk AI systems. We ask that this would be clarified in the wording of the annex or at least in a recital.

High-risk AI systems pursuant to Article 6(2) are the AI systems listed in any of the following areas:	PT: (Comments): We highlight the definition of the 'intended purpose' that "means the use for which an AI system is intended by the provider, including the specific context and conditions of use". This annex ignores totally the "conditions of use", and we consider that this should be mentioned whenever possible to avoid grey zones in any of the points listed. AT: (Comments): DK: (Comments): We would like to reflect that besides falling within one of the listed areas, systems listed herein should also entail high-risk pursuant to the risk assessment, thereby linking the list directly to the concrete risk assessment. FR: (Comments):

	Ongoing work by FR experts.
1. Biometric identification and categorisation of natural persons:	MT: (Comments): Malta welcomes the emphasis placed in the Artificial Intelligence Act to protect vulnerable social groups such as children deeming subliminal messaging techniques as illegal practices due to the harmful effect on children's behaviour, choices, and actions. This Ministry also notes the emphasis placed on the privacy of citizens in the use of AI systems for 'real-time' remote biometric identification in publicly accessible spaces and the exceptional rights granted to law enforcement working on missing children cases. AT: (Drafting): 1. Biometric techniques ~~identification and categorisation of natural persons~~: AT: (Comments): **Point 1** should be extended to biometric techniques in general and cover also emotion recognition systems where those systems are to be used for preparing decisions that may have legal effects or similarly

	significantly affect him or her. FR: (Comments): Ongoing work by FR experts.
(a) AI systems intended to be used for the 'real-time' and 'post' remote biometric identification of natural persons;	AT: (Drafting): (a) AI systems intended to be used for the ~~'real-time' and 'post'~~ remote biometric identification of natural persons data that are not prohibited according to Art. 5; **Option** (a) AI systems intended to be used for the 'real-time' ~~and 'post'~~ remote biometric identification of natural persons; AT:

	(Comments): The use of AI systems for the biometric real-time identification of persons in public places seems fundamentally questionable; from a data protection perspective, the time-delayed analysis of biometric data is similarly intrusive as a real-time analysis; accordingly, Annex III in point 1a) would have to be adapted. Facial recognition is used to identify the unknown perpetrator after premeditated criminal acts have already been committed, if facial images ("trace image") of the unknown perpetrator are available, by comparing them with facial images of known persons stored in databases. FR: (Comments): Ongoing work by FR experts.
	AT: (Comments): **Point 1** should be extended to biometric techniques in general and cover also emotion recognition systems where those systems are to be used for preparing decisions that may have legal effects or similarly significantly affect him or her.

2. Management and operation of critical infrastructure:	MT: (Comments): Malta welcomes the addressing of critical systems, as these require their due attention, no matter whether it involves the use of AI or not. Malta believes that a risk-based approach should be introduced to regulate such critical systems. Malta notes that the EU should mandate that the technology undergoes audits and has various technology assurances in place. BE: (Comments): A definition of "critical infrastructure" is needed to make sure this area is sufficiently circumscribed, for example by making a reference to the annex of the future CER Directive. FR: (Comments): Ongoing work by FR experts.
(a) AI systems intended to be used as safety components in	DK: (Comments):

the management and operation of road traffic and the supply of water, gas, heating and electricity.	We would like to specify what is meant by management and operation, as this needs to be related to the specific supply. FR: (Comments): Ongoing work by FR experts. SE: (Drafting): (a) AI systems intended to be used either as management and operational systems in services provided by essential entities, in accordance with the meaning of that term in directive 2020/0359(COD), or as safety or security components in the management and operation of ~~road traffic and the supply of water, gas, heating and electricity.~~the services provided by such entities. SE: (Comments): To harmonise with “essential entities” defined in the NIS 2-directive. Safety component indicates operational reliability. Add the term security to include AI-based security solutions.

3. Education and vocational training:	NL: (Comments): ?
(a) AI systems intended to be used for the purpose of determining access or assigning natural persons to educational and vocational training institutions;	**DELETED** SE: (Comments): Needs to be reviewed and specified. In many ways AI-systems can protect from human errors and discrimination. It is advantageous if systems are developed within the EU, not only reflecting European values but also reducing our dependency on foreign solutions. Hence the AI Act should promote and not hinder innovation and development in Europe. The use of AI does and should not withdraw an educator/institutions/university of responsibility under applicable national nor international laws and

	regulations. Should there be insufficient regulation in certain areas, these should be complemented rather than implementing regulation targeted specific technology.
(b) AI systems intended to be used for the purpose of assessing students in educational and vocational training institutions and for assessing participants in tests commonly required for admission to educational institutions.	**DELETED** AT: (Comments):

	A general classification of AI applications in the education and training sector as "high-risk AI systems" seems excessiv. AI not only makes it possible to offer individualised learning individualised learning offers in terms of content and learning formats and learning aids, but also contributes to the improvement of the educational formats. EE: (Drafting): (b) AI systems intended to be used for the purpose of assessing students in educational and vocational training institutions and for assessing participants in tests commonly required for admission to educational institutions **or programmes within the educational institutions.** EE: (Comments): This should be broader and include access to particular programmes of study. SE: (Comments): Needs to be reviewed and specified. In many ways AI-systems can protect from human errors and discrimination. The use of AI does and should not withdraw an employer of responsibility under applicable national nor international laws and regulations. Should there be insufficient regulation in

	certain areas, these should be complemented rather than implementing regulation targeted specific technology.
4. Employment, workers management and access to self-employment:	MT: (Comments): Malta notes that from an employment perspective, the PES (Public Employment Services) network is set to discuss the AI package and its effects on PES at the end of June. This will help better explain the potential impact of the proposal on PES network. In the meantime, a cautious approach is advised from a PES perspective. Malta notes that from a public procurement perspective, the key participants across the AI value chain include providers and users of AI systems that cover both public and private operators. Accordingly, public procurement might indirectly be part of an AI system should a Contracting Authority decide to invest in the development and adoption of such systems. Malta stresses that as long as any necessary procurement activity adheres to the relevant Procurement Directives, there should not be any negative implications. To the contrary, it should be a positive measure as the EU would be enhancing a Digitised Europe. Furthermore, the Regulation shall be encouraging SMEs and start-ups to partake in AI since the Regulation contains measures to reduce the regulatory burden. FI: (Comments):

	FI also considers it important that the rights of employees and jobseekers are safeguarded even when artificial intelligence is used in decision-making.
(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;	PL: (Drafting): 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 PL: (Comments): Limit this point to systems for making decisions about employment, or directly supporting such a decision if recruitment high-risk application is automatic listed as its. It could block innovation, and trustworthy compliance seem to be enough. **DELETED**

	DELETED AT: (Drafting): (a) […], or for evaluating candidates ~~in the course of interviews or tests~~; AT: (Comments): Minor amendments have also been suggested with regard to Point 4 in order to capture, e.g., social media harvesting in the employment context. FR: (Drafting): (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; FR: (Comments): Not all task allocation should fall under high risk. SE:

	(Comments): Needs to be reviewed and specified. In many ways AI-systems can protect from human errors and discrimination. The use of AI does and should not withdraw an employer of responsibility under applicable national nor international laws and regulations. Should there be insufficient regulation in certain areas, these should be complemented rather than implementing regulation targeted specific technology. Considering the broad definition of AI-system this means all IT-systems used for recruitment will be classed high-risk.
(b) AI intended to be used for making decisions on promotion and termination of work-related contractual relationships, for task allocation and for monitoring and evaluating performance and	**DELETED**

behavior of persons in such relationships.	**DELETED** DK: (Comments): We are still unsure of the scope in terms of task allocation and are questioning whether this would entail high-risk. As employment is a horizontal area, this could potentially affect a lot of different applications, even applications not entailing a high risk. Furthermore, we would like to have concrete examples of evaluation of performance and behaviour, where this would entail high risks. FR: (Drafting): AI intended to be used for making decisions on promotion and termination of work-related contractual relationships, for task allocation **based on individual behavior** and for monitoring and evaluating performance and behavior of persons in such relationships. SE: (Comments):

	Needs to be reviewed and specified. In many ways AI-systems can protect from human errors and discrimination. The use of AI does and should not withdraw an employer of responsibility under applicable national nor international laws and regulations. Should there be insufficient regulation in certain areas, these should be complemented rather than implementing regulation targeted specific technology.
5. Access to and enjoyment of essential private services and public services and benefits:	AT: (Drafting): 5. Access to and enjoyment of essential private services and public services and benefits, including access to products: AT: (Comments): With regard to consumer interests, it is of utmost importance to add, in Point 5, a number of applications that imply a comparable fundamental rights risk as credit scoring does. These applications include individual risk assessment in the insurance context, customer rating according to complaint history and similar factors, and personalised pricing. With regard to the exception for small scale providers there should be a clarification that it includes only small scale providers who are at the same time the

	'providers' (within the meaning of the AIA) of the relevant AI systems. SE: (Drafting): 5. Access to and enjoyment of essential ~~private services and~~ public services and benefits: SE: (Comments): The area of "essential private services" is too vaguely formulated when compared with other points and considering the very large area of private services. The current wording is not in line with the interest of proportionate, well defined provisions and leads to a severe lack of predictability and potential negative impacts on investement and innovation for providers of AI systems established inside and outside of the EU. It could also weaken EU possibilities to counteract similar vaguely provision in third countries legislation which might have purely protectionst motives with negative consequences for EU service exporters.
(a) AI systems intended to be used by public authorities or	**DELETED**

on behalf of public authorities to evaluate the eligibility of natural persons for public assistance benefits and services, as well as to grant, reduce, revoke, or reclaim such benefits and services;	DK: (Drafting): (a) AI systems intended to be used by public authorities or on behalf of public authorities to evaluate the eligibility of natural persons, with potential disadvantage for these persons, for public assistance benefits and services, as well as to grant, reduce, revoke, or reclaim such benefits and services; DK: (Comments): We find that the formulation is too generic, as it would probably categorize most of existing public sector AI systems as high-risk systems. This would place an unnecessary administrative burden on systems which should not be included as a high-risk system in the first place. This is also interlinked with the needed changes in the definition of AI, where we need to establish that AI operate with a level of autonomy and that systems which exclusively implements the automation of rules-based actions with defined inputs and outputs based on objective and logic criteria are not within the scope. As of now, it is unclear when the evaluation procedure will actually begin, for example, it seems with the current formulation that even an AI system prioritising e-mails, part of a procedure, could be seen as a high-risk system. Therefore, it needs to be specified that systems intended for administrative activities, administrative tasks or allocation of resources should not be seen as high-risk. Furthermore, we need to target only those systems which can put the citizen at a disadvantage and can have a direct impact on the final decision of the evaluation. SE:

	(Comments): Needs to be reviewed and specified. In many ways AI-systems can protect from human errors and discrimination. The use of AI does and should not withdraw public authorities/stakeholder on behalf of public authorities of responsibility under applicable national nor international laws and regulations. Should there be insufficient regulation in certain areas, these should be complemented rather than implementing regulation targeted specific technology. FI: (Comments): Category 5 seems to cover widely different AI systems used by public authorities. It is important to specify which AI systems belong to this category in order to ensure the clarity of the regulation. FI notes that regarding the use of high-risk artificial intelligence systems that support human user's judgment, need more clarification on how and to what extent such systems are considered high-risk systems, for example, in the case of assessment in education.
(b) AI systems intended to be used to	PL: (Comments):

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;	In the case of Art. 6 sec. 2 in conjunction with Annex III point 5 lit. (b) the deletion of the provision qualifying as a high-risk artificial intelligence system to assess the creditworthiness of individuals or to establish their credit scores appears to be considered. Systemically, it should be assumed that the qualification or a given system is a high-risk system should not be listed in advance in the regulation (Annex 3), but rather be assessed on the basis of a risk based approach. the institution. We propose adding to point 5 lit. b (Annex III) "as well as assessments of the underwriting capacity of natural persons" after the phrase "assessing the creditworthiness of natural persons or establishing their creditworthiness scores". CZ: (Drafting): ~~(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;~~ CZ: (Comments): The assessment of creditworthiness is already addressed in the Mortgage Credit Directive (MCD) and the Consumer Credit Directive (CCD). New CCD proposal, which was published in 2021 states in article 18 (b), that *"Where the creditworthiness assessment involves the use of profiling or other automated*

	processing of personal data, Member States shall ensure that the consumer has the right to: request and obtain human intervention, request and obtain a clear explanation of the assessment of creditworthiness, including on the logic and risks involved in the automated processing of personal data as well as its significance and effects on the decision and express his or her point of view and contest the assessment of the creditworthiness and the decision." The MCD also details the creditworthiness assessment, inter alia, in its Chapter 6. Article 18 (5) (b) and (c), which stipulates the need to communicate information about working with databases and inform that a negative decision was made due to the result from the database. Both regulations take into account the ongoing digital transformation of the financial market. As part of the revision of MCDs and CCDs, the use of artificial intelligence systems in connection with credit assessments is appropriately addressed and it is not desirable to fragment this regulation and include it extensively also within the new AI regulation. The inclusion of these AI systems as high-risk AI systems involves a number of obligations specified in the draft regulation. The current wording of the draft regulation underlines the diversity of access to credit institutions regulated by Directive 2013/36/EU on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms (CRD IV) and to creditors, which are not a credit institution, even if in the product part of the legislation on the granting of the consumer credit, both categories are subject to the same regulation. The proposal does not a priori take into account the different requirements for credit institutions and other financial providers, but subjects, who are using creditworthiness assessment would be supervised by different supervisors under the draft regulation. This division poses a risk of a different approach in supervision, where there should be similar treatment. It is therefore crucial to consider

	whether there should be a breakdown of supervision by type of institution (AI Act mentions three, i.e. credit institutions; EU law harmonized financial institutions, e.g. payment institutions, and non-harmonized entities, e.g. non-bank providers) and not by the type of AI system used (same supervision for all creditors who are using creditworthiness assessment). It does not seem appropriate for AI systems to be supervised separately in countries where non-bank providers are supervised by financial supervision. Given the adequacy of the current regulation of the sector and on the basis of consultation with the market, the Ministry of Finance considers it redundant to rank creditworthiness assessments and credit scoring among high-risk artificial intelligence systems. With the exclusion of these AI systems from Annex III, point 5 (b) of the draft regulation, it is fully sufficient to support the development of sectoral codes of conduct in accordance with Title IX of the draft regulation. However, if the creditworthiness assessment and credit scoring remain classified as a high-risk AI system, the Czech Republic requests the deletion of part of Article 43, point 2 in order to ensure that for all the AI creditworthiness assessment and credit scoring systems it would sufficient enough to undergo the conformity assessment procedure based on the internal control in accordance with article 43, point 1 (a) of the draft regulation. AT: (Drafting): (b) AI systems intended to be used i) to evaluate the creditworthiness of natural persons or establish their credit score,

ii) to evaluate the behaviour of natural persons with regard to complaints or the exercise of statutory or contractual rights in order to draw conclusions for their future access to private or public services,

iii) for making individual risk assessments of natural persons in the context of access to essential private and public services, including insurance contracts, or

iv) for personalised pricing within the meaning of Article 6 (1) (ea) of Directive 2011/83/EU,

with the exception of AI systems put into service by small scale providers of AI systems for their own use;

AT:

(Comments):

With regard to consumer interests, it is of utmost importance to add, in Point 5, a number of applications that imply a comparable fundamental rights risk as credit scoring does. These applications include individual risk assessment in the insurance context, customer rating according to complaint history and similar factors, and personalised pricing. With regard to the exception for small scale providers there should be a clarification that it includes only small scale providers who are at the same time the 'providers' (within the meaning of the AIA) of the relevant AI systems.

However, the use of AI systems for creditworthiness assessments and credit scoring by credit institutions is already regulated by the provisions of Regulation (EU) No 575/2013 (CRR). Overlapping or

	contradictory regulations must be avoided, and sector-specific legislation such as CRR should be respected. SE: (Comments): Needs to be reviewed and remade.
(c) AI systems intended to be used to dispatch, or to establish priority in the dispatching of emergency first response services, including by firefighters and medical aid.	
	AT: (Comments):

	New Point 5a: What is missing entirely in Annex III is AI systems intended for use by consumers. The AIA as it currently stands seems to assume that systems intended for consumers are covered by Article 6 (1) in conjunction with NLF product safety legislation. However, this is not necessarily the case as NLF product safety legislation fails to cover a number of high-risk AI systems, or may not subject them to third-party conformity assessment. This is why it is suggested to insert a new area, which could be titled 'Use by vulnerable groups or in situations that imply vulnerability to fundamental rights risks' and that would include, for the time being, virtual assistants used for making important decisions (e.g. a shopping assistant, be it provided as a standalone digital service or embedded in devices such as a home assistant device or a smart fridge) and particular AI systems specifically intended for children.
6. Law enforcement:	BE: (Comments): The categorisation as "high risk" of some of those "use cases" can be exaggerated or even inappropriate. As a general comment, the real high risk uses case should be more narrowly defined. When evaluating the risk that those AI use cases represent, one should also compare with the practice in absence of such AI use. In some specific cases, the use of AI, although not perfect, might give similar or even better results than conventional "human" practices. For examples (E.g.), refer to point (a), (c), (e), (g)
(a) AI systems	BE:

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 or the risk for potential victims of criminal offences;	(Comments): E.g. : AI-based risk assessments tools warning police officers of potential risks for specific victims could be complementary to their judgment based on knowledge and experience. **DELETED** SE: (Comments): Using AI as a tool in a sub-step in your analysis could be more efficient and can protect from human errors and discrimination compared to a manual search. There is a risk that the tools will not be used due to the high-risk classification.

(b) AI systems intended to be used by law enforcement authorities as polygraphs and similar tools or to detect the emotional state of a natural person;	FR: (Comments): Ongoing work by FR experts.
(c) AI systems intended to be used by law enforcement authorities to detect deep fakes as referred to in article 52(3);	EE: (Comments): Why are these solutions labelled as high-risk solutions? What risks do such solutions pose, especially considering that section (d) already covers cases where deep fake detection is used for evaluating evidence or in the course of investigation or prosecution of criminal offences? BE: (Comments):

	E.g. : AI systems detecting deep fakes can outperform human experts, so instead of considering this as "high risk", these AI systems could be considered as extra assistance in addition to human expertise. FR: (Comments): Ongoing work by FR experts.
(d) AI systems intended to be used by law enforcement authorities for evaluation of the reliability of evidence in the course of investigation or prosecution of criminal offences;	AT: (Drafting): ~~(d) AI systems intended to be used by law enforcement authorities for evaluation of the reliability of evidence in the course of investigation or prosecution of criminal offences;~~ AT: (Comments): Deletion suggested because it would otherwise be disadvantageous for the work of law enforcement authorities (below some examples where such AI systems would be used): - 3D laser scanner - For the processing of crime scenes, 360° scans are made, which are then processed with a software and combined into a visual 3D model.

	- AI based search for similar shoe tracks from various crime scenes. Used to search for crime connections via shoe prints worn at the crime scene. EE: (Comments): **DELETED**
(e) AI systems	BE:

intended to be used by law enforcement authorities 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;	(Comments): E.g. : combined with the broad definition of AI, this could imply that e.g. risk-labelling of known offenders based on their past criminal behaviour (e.g. violent, firearms user, etc.) that are used to warn police officers before interacting with these persons also become "high-risk use". These risk warnings are already applied nowadays but are mainly based on human judgment (not necessarily in a very consistent way). FR: (Comments): Ongoing work by FR experts.

(f) AI systems intended to be used by law enforcement authorities 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;	
(g) AI systems intended to be used for crime analytics regarding natural persons, allowing law	MT: (Comments): Data Sets or Parameters in specific fields of implementation such as Law Enforcement, Education, the Government and others need to be provided as initial guidelines. Differences and possible ethical issues

enforcement authorities to search 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.	in specific data sets/parameters should be explained to understand what, which and how to collect such information. This will assist and provide something to consider when designing/developing AI solutions. AT: (Drafting): ~~(g) AI systems intended to be used for crime analytics regarding natural persons, allowing law enforcement authorities to search 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.~~ AT: (Comments): It would no longer be possible to graphically visualize the preferences of offenders for individual time periods and thus to set effective action planning. Temporal correlations and geographical priorities can no longer be identified. Likelihoods crimes being part of series of crimes can no longer be determined. Examples: - Predictive policing (PredPol) refers to the identification and prediction of potential criminal activities within a temporal and spatial framework based on police data using mathematical and analytical techniques. Prediction is intended to enable the police to anticipate crime-specific developments and to

	implement police intervention and prevention strategies. In AT, PredPol has been used for the past seven years as part of the annual priority measures to combat burglary, evaluated annually, adapted and now implemented fully automatically. - Large amounts of data (Terabyte) need to be analysed in the course of financial investigations. This only leads to more efficient evaluation of legal case data but not to inadmissible grid searches or problematic profiling. EE: (Comments): It should be reviewed that this definition would not cover all analytics used by law enforcement, including for example doing statistics on crime rates. BE: (Comments): ➔ See comments Annexe I. The combination of the broad AI definition and the broad high-risk category (6(d)) implies that a lot of data processing and analytics, with longstanding use, might become high risk (with all the compliance requirements as a consequence) For instance:

	• 'intelligent' search engine; not only presenting an exact match but also suggesting potentially related information • processing of communications based on specific ontologies or a machine learning model • Geographic profiling techniques • Indicator/rule-based risk scoring (e.g. for potential life-threatening risks in domestic violence situations) Users might abandon the use of these techniques to avoid the administrative burden related to the High-Risk AI practical requirements. **DELETED**

	DELETED SE: (Comments): With reference to the comments already stated on art. 3.1 and the art. 6.2, the definition of "AI-system" in combination with the rules stated in p.6(g) of Annex III would put unnecessary restraints on the development and use of certain small scale AI-system used in law enforcement. Practically all R&D within the area of law enforcement is conducted for the purposes of those accounted for in p.6(g), as well as most "basic operation procedures". Thus, the regulation would have too serious impact on LEA:s abilities.
	PT: (Drafting): **(h) AI systems which do not explicitly rely on personal data used by law enforcement authorities to determine law enforcement resource deployment or policing prioritisation**

	PT: (Comments): In our opinion, the list included in point 6 of Annex III is mostly focused on systems that have natural persons as their subjects and by doing so seems to fail to identify optimisation systems that use geospatial data to determine law enforcement resource deployment as high-risk systems (otherwise known as 'predictive policing,' or 'crime hotspot analytics systems'). Despite not relying on personal data of natural persons, the fundamental rights implications of these systems are important because they are used to determine who can be subject to increased police intervention (based on geographical location), how these interventions occur, and with what frequency. Used without due safeguards, these systems may lead to over-surveillance of specific geographical locations and further aggravate existing problems with discrimination arising from racial and socio-economic biases in some existing policing datasets. As such, including law enforcement AI systems that do not explicitly use personal data (e.g. crime hotspot analysis based on geospatial data) in the list of high-risk systems could be a way to tackle this issue.
7. Migration, asylum and border control management:	BE: (Comments): See comments Annexe III, point 6. (same reasoning).

(a) AI systems intended to be used by competent public authorities as polygraphs and similar tools or to detect the emotional state of a natural person;	FR: (Comments): Ongoing work by FR experts.
(b) AI systems intended to be used by competent public authorities 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	FR: (Comments): Ongoing work by FR experts.

or has entered into the territory of a Member State;	
(c) AI systems intended to be used by competent public authorities 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;	AT: (Drafting): ~~(c) AI systems intended to be used by competent public authorities 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;~~ AT: (Comments): Future use cannot be ruled out. Qualifying these AI systems as "high risk" therefore is a red line from AT's perspective. The associated administrative burden would reduce - if not eliminate - the added value gained from the system. BE: (Comments): See comments on Annexe III, point 6, (b).

	E.g. : AI systems for the verification of the authenticity of travel documents could outperform human experts, so instead of considering this use as "high risk", these AI systems could be considered as a "welcome extra help" in addition to human expertise. **DELETED** SE: (Comments): Does this include automated border control using biometric scanning and facial recognition, for example ABC gates? This would be problematic from a border management perspective.

(d) AI systems intended to assist competent public authorities 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.	AT: (Drafting): ~~(d) AI systems intended to assist competent public authorities 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.~~ AT: (Comments): Same reasoning as for Annex III art 7 lit c. Future use cannot be ruled out. SE: (Drafting): (d) AI systems intended ~~to assist~~ to be used by competent public authorities 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.
8. Administration of justice and democratic processes:	BE: (Comments):

	We agree that the sector of the administration of Justice is one where the use of AI systems could generate important risks.
(a) AI systems intended to assist a judicial authority in researching and interpreting facts and the law and in applying the law to a concrete set of facts.	PT: (Drafting): (a) AI systems intended to assist a judicial authority in researching ~~and~~ **or** interpreting facts and the law ~~and~~ **or** in applying the law to a concrete set of facts; PT: (Comments): The wording used in point 8 of Annex III needs to be clarified as it leaves some room for legal uncertainty, as it is clearly pointed out in document 11368/21: *«'researching **and** interpreting facts and the law **and** […] applying the law'*: the wording seems to indicate cumulative criteria. An AI system that only assists the judicial authority 'in researching facts' but not in 'interpreting' them or 'in applying the law' would thus not be considered high risk.» In order to avoid this, it should be made clear that the use of any AI system to "assist" the judicial authority in any of the indicated roles – regardless of whether its purpose is research, interpretation or application of the law – should be subject to the same guarantees, since these are essential, as they protect fundamental rights, avoid the "black box" effect and the problem of algorithmic bias. This would, of course, be in line with the wording in Recital 40, which excludes from the classification as "high-risk" « (…) 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'.» PL: (Comments): doubts are raised by the definition in Annex III, par. 18 lit. and relating to AI systems "intended to assist the judicial authority in the investigation and interpretation of the actual state of affairs and legal regulations as well as in the application of the law to a specific factual state. ". The helpful wording used is vague and may cause problems with interpretation AT: (Drafting): (a) AI systems intended to assist courts or ~~a~~ independent judicial ~~authority~~ authorities acting within the scope of their judicial functions in researching and interpreting facts and the law and in applying the law to a concrete set of facts with no possibility to ask for a human review of the decision that is performed by an AI system. AT: (Comments):

	Addition at the end of the paragraph suggested to ensure the development, testing and introduction of supporting AI systems (e.g. preparation of documents and metadata) in a practical manner in the future without great administrative effort. EE: (Comments): The corresponding recital 40 should be amended as follows: "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~~." The phrase "administrative tasks" is too vague and broad to be used as an exemption. Allocation of resources might impact which cases are prioritised or allocating judges and other resources in a particular proceeding, which may thus have material outcome on the case. Therefore, fully removing these examples

	from the applicability of this clause might not be justified. BE: (Comments): We fear however that this definition risks to create a grey zone. For some AI systems, it may not be immediately clear whether they fall under this definition; e.g. a system for the administration of hearings, or a system for case-law enhancement (see https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c, p 64) More fundamentally, this presupposes the acceptance of the principle that AI-systems could offer support/assistance with the taking of judicial decisions. This raises important questions, e.g. concerning the avoidance or at the very least limitation of potential biases in the data that are fed to the algorithms concerned, or concerning the desired level of explainability of the decisions reached with the assistance of AI-systems. Furthermore, this proposal does not seem to pay any particular attention to the remedies offered to persons (natural or legal) against decisions (judicial or other) taken with the assistance/support of AI systems, and the particularities that go with it. FR: (Drafting):

	(a) AI systems intended to assist a judicial authority ~~in researching and interpreting facts and the law and~~ in applying the law to a concrete set of facts. FR: (Comments): We thank COM for the explanations given, but we still believe this is not clear enough to be applied consistently by MS. SE: (Drafting): (a) AI systems intended ~~to assist a~~ to be used by judicial authority in ~~researching and~~ interpreting facts and the law and in applying the law to a concrete set of facts. SE: (Comments): The use of AI systems for searching and finding legal information such as case law, legal acts etc. can greatly improve and speed up the legal process and does not pose a risk to fundamental rights if used for example in search engines in legal databases.
	PT:

	(Drafting): 9. Healthcare a) AI systems intended to support the diagnosis; b) AI systems intended to monitor patient's vital signs; **AI systems intended to assist the competent authorities in decisions concerning the execution of sentences.** c) AI systems intended to automate the generation of treatments plans. PT: (Comments): In our opinion, it would probably be important to consider the insertion of a specific mention to the penitentiary sector, which does not seem to be sufficiently taken into account in the text, considering that some decisions related to the execution of sentences are not taken by judicial authorities and would therefore not fall under the 'administration of justice'. AT: (Drafting): ~~a) AI systems intended to assist a judicial authority in researching and interpreting facts and the law and in applying the law to a concrete set of facts.~~ AT:

	(Comments): Same comments as for Annex III art 6 lit d.
ANNEX IV TECHNICAL DOCUMENTATION referred to in Article 11(1)	SE: (Comments): Overall, too far reaching requirements for documentation. Not entirely clear what risks each respective provision is meant to mitigate**.**
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	EE:

description of the AI system including:	(Comments): We would like the COM to bring out concrete examples what a general description of different AI systems would look like.
(a) its intended purpose, the person/s developing the system the date and the version of the system;	EE: (Comments): There are often many people involved with developing a system, e.g. UX designer, developers, data scientists, people who label data, regular employees and others. Furthermore, in every solutions, there are various libraries/tools used that are developed by other people. Considering that, who are needed to be listed? What is considered under "date"? Typically, the development continues and is continuously delivered.
(b) how the AI system interacts or can be used to interact with hardware or software that is not	EE: (Comments): Providing such information could incur in risks to cyber security. What is intended to be achieved under such requirement? Where goes the line between AI system itself and other systems?

part of the AI system itself, where applicable;	DK: (Drafting): ~~(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;~~ DK: (Comments): This could lead to endless possibilities for the provider to describe.
(c) the versions of relevant software or firmware and any requirement related to version update;	EE: (Comments): Why is this information considered relevant?
(d) the description of all forms in which the AI system is	EE: (Comments):

placed on the market or put into service;	What is meant by "form"? If solutions are made publicly available as open source then it is impossible to know how solutions are placed on the market or put into service.
(e) the description of hardware on which the AI system is intended to run;	EE: (Comments): Why is such information considered necessary?
(f) where the AI system is a component of products, photographs or illustrations showing external features, marking and internal layout of those products;	EE: (Comments): Why is such information considered necessary? What is exactly meant here?

(g) instructions of use for the user and, where applicable installation instructions;	EE: (Comments): In which cases are installation instructions necessary? ES: (Drafting): (g) instructions of use for the user with ilulustrative examples and, where applicable installation instructions;
2. A detailed description of the elements of the AI system and of the process for its development, including:	EE: (Comments): What is considered as “detailed description of the elements of the AI system”?
(a) the methods	EE:

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;	(Comments): Why is such information considered necessary? What is exactly meant by “methods and steps”? SE: (Comments): The wording “pre-trained systems or tools” is very diffuse and may have to be more precise.
(b) the design specifications of the system, namely the general logic of the AI system and of the algorithms; the key design choices	EE: (Comments): What is considered under “design specifications of the system” and “key design choices”? ES: (Drafting):

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,	(b) the design specifications of the system, namely the general logic of the AI system and of the algorithms; the key design choices including the rationale and assumptions made, also with regard to persons or groups of persons on which the system is intended to be used and the domains to which they will be applied ; 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;

Chapter 2;	
(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;	EE: (Comments): What is meant under "computational resources used to develop…"?
(d) where relevant, the data requirements in terms of datasheets	MT: (Comments):

describing the training methodologies and techniques and the training data sets used, including information about the 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);	Malta notes that Training Data Sets that are used for Artificial Intelligence in Healthcare and Public Health need to take into consideration the needs of small member states with populations of less than a million citizens to allow for the use of training data sets from other member states or third-parties, or to provide support for these member states to ensure that they're able to have access to high quality training data sets. Malta notes that there should also be mechanisms in place that encourage Member States to implement fully integrated consent systems that make it easy for citizens to consent that their relevant health data (such as medical imaging data) could be used for research. Secure and robust anonymisation techniques need to be implemented and encourage EE: (Comments): In which cases are data requirements considered relevant to be described? ES: (Drafting): (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, information about their provenance ~~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 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	EE: (Comments): What type of information is needed to be provided on validation and testing data?

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, 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;	
4. A detailed description of the risk management system in accordance with Article 9;	
5. A description of any change made to the system through its lifecycle;	EE: (Comments): At what level would a description of changes needed to be provided?
6. A list of the harmonised standards applied in full or in part the references of	MT: (Comments): Malta notes that the Commission should look into and investigate ISO Standards Certification for AI

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;	Solution/AI Operated Machines to ensure that the solution/equipment developed are ethical and within the legal parameters (AI ISO Article, Standards and Committees referred).
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 Article 61, including the post-market monitoring plan referred to in Article 61(3).	
	ES: (Drafting): 9. A description of the mechanism included within the AI system that allows users to properly collect and store the logs to be kept according to article 29.5.

	End