European Parliament Proposals: GPAI / Value Chain

Compromise proposal on GPAI/Value Chain	Assessment / Comments
Recital 49 (49) High-risk AI systems should perform consistently throughout their lifecycle and meet an appropriate level of performance, robustness and cybersecurity in accordance with the generally acknowledged state of the art. ***Performance metrics and their expected level should be defined with the primary objective to mitigate risks and negative impact of the AI system. The expected*** level of ***performance*** metrics should be communicated ***in a clear, transparent, easily understandable and intelligible way*** to the deployers. ***The declaration of performance metrics cannot be considered proof of future levels but relevant methods need to be applied to ensure consistant levels during use. While standardisation organisations exist to establish standards, coordination on benchmarking is needed to establish how these standardised requirements and characteristics of AI systems should be measured. The European Artificial Intelligence Office should bring together national and international metrology and benchmarking authorities and provide non-binding guidance to address the technical aspects of how to measure the appropriate levels of performance and robustness.***	
Recital 60a (new) ***(60a) (new) General purpose AI systems, and in particular foundational models, are a recent development, in which AI systems are developed from algorithms designed with the intention to optimize for generality and versatility of output. Those systems can be trained on a broad range of data sources to accomplish a wide range of downstream tasks, including some for which they were not specifically developed and trained Those systems can be unimodal or multimodal, trained through various methods such as supervised learning or reinforced learning. General purpose AI systems are often the basis for various AI systems with specific intended purpose. These systems hold growing importance to many downstream applications combined with their complexity and unexpected impact, as well as the downstream operator's lack of control over the AI system's development and consequent power imbalance. Therefore, due to their particular nature and in order to ensure a fair sharing of responsibilities along the AI value chain, such systems should be subject to proportionate and more specific requirements and obligations under this Regulation while ensuring a high level of protection of fundamental rights, health and safety. AI systems developed for a limited set of applications that***	

cannot be adapted for a wide range of tasks such as components, modules, or simple multi-purpose AI systems should not be considered general purpose AI systems for the purposes of this Regulation.	
Recital 60b (new) ***(60b) (new) Providers of general purpose AI systems must be subject to independent oversight through independent experts in close cooperation with the AI Office . Requirements for general purpose AI systems are selected so as to be broadly applicable (e.g. independent of distribution channels, modality, development methods), to address risks specific to general purpose AI systems and complementary to measures for high-risk AI systems, and which can be coherently implemented taking into account industry state- of-the-art practices. These requirements include risk management, extensive analysis and testing of the general model for unforeseen vulnerabilities, including by independent evaluators.***	A new independent oversight provision broadly applicable to all GPAI is not tailored to risk. National supervisory authorities and the AI Office already together have extensive oversight powers under the Act.
Article 3 **Definitions** For the purpose of this Regulation, the following definitions apply: ***(1a) (new) 'general purpose AI system' means an AI system that is trained on broad data at scale, is designed for generality of output, and can be adapted to a wide range of tasks;***	Critical here is that the EU limit the requirements around general purpose AI to high risk use cases, as discussed below. As drafted this definition is overly broad and runs the risk of capturing many types of AI/ML technology. If the concern is generative AI (such as large language models), the focus should be on creative output. But, if the concern is systems like translation or object detection, the Council definition is preferred.
Article 28 Responsibilities ***along the value chain*** 1. Any distributor, importer, ***deployer*** or other third-party shall be considered a provider ***of a high-risk AI system (AM 2026)*** for the purposes of this Regulation and shall be subject to the obligations of the provider under Article 16, in any of the following circumstances: (a) they place on the market or put into service implement a high-risk AI system in their operations under their name or trademark ***(b)*** they ***make a substantial modification to*** a high-risk AI system already placed on the	This draft includes the "deployer" concept, which is valuable in capturing parties' roles in the AI value chain. However, this draft continues to impose most obligations on the provider. The party that deploys an AI system in a high-risk way is best positioned to identify that it's a high-risk system, manage those risks, and meet the requirements of the Regulation. Thus, recommend updating throughout to use "deployer" instead of "provider" as the primary party with obligations and put the provider as the party to provide assistance where appropriate (as already contemplated below). Recommend

market or put into service ***and in a way that it remains a high-risk AI system in accordance with Article 6; (AM 133)*** ***(ba) they make a substantial modification of an AI system, including a general purpose AI system, which is not high-risk and is already placed on the market or put into service in such manner that the AI system becomes a high risk AI system in accordance with Article 6 (AM 132, 134, 2031, 2032)***	clarifying the definitions of provider (developer of an AI system) and deployer accordingly.
2. ~~***Where the circumstances referred to in paragraph 1, point (a) to (ba) or ((AM 135), 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 of that specific AI system for*** the purposes of this Regulation***. This former provider shall, without compromising its own intellectual property rights or trade secrets, provide the new provider with the technical documentation and all other relevant information or documentation, as well as with the relevant and reasonably expected capabilities, technical access or other assistance based on the generally acknowledged state of the art that are required for the fulfillment of the obligations set out in this Regulation. (AM2033).***~~ ***To the extent a former provider consents to the use of its AI system as a high-risk system by a new provider, and without compromising its own intellectual property rights or trade secrets, the former provider shall, by written agreement with the new provider, specify the information, capabilities, technical access, or other assistance, such as the examples referenced in Annex IXa, that the former provider shall provide in order to enable the new provider to comply with the obligations under this Regulation.*** ~~***3.***~~ ~~***The provider of a general purpose AI system shall take into account the information listed in Annex IXa in order to comply with this obligation.***~~ ~~***In the case of general purpose AI systems using API access, such contracts cooperation shall extend throughout the lifetime of the downstream high risk AI system, in order to enable appropriate risk mitigation, unless the provider of the general purpose AI system transfers the model object as well as extensive and appropriate information on the datasets and the development process of the system or constricts the API access in such a way that the downstream provider is able to fully comply with this Regulation without futher support from the original provider of the general purpose AI system***~~**.**	First, the "provider consents" language is to ensure the provider is aware and agrees to the AI system's use in a high risk way and the provider is prepared to provide such compliance assistance. Second, strongly recommend providing that the providers can contract for their respective obligations. Paragraph 2 is unnecessary. Paragraph 1 already requires that the parties will enter into a contract enabling the deployer to comply with obligations under the Act (regardless of whether the system involves API access or not). This level of precision regarding technology may not stand the test of time and creates confusion over whether providers have differing obligations to assist deployers depending on how AI system capabilities are delivered.

4. ~~***The provider of a high risk AI system and the third party that supplies tools, services, components or processes that are used or integrated in the high risk AI system shall, by written agreement and without compromising intellectual property rights or trade secrets, specify the information, capabilities, technical access, and or other assistance, based on the generally acknowledged state of the art, that the third party must provide in order to enable the provider of the high risk AI system to fully comply with the obligations under this Regulation***~~. ***To the extent a third party that supplies tools, services, components or processes consents to the use of those tools, services, components or processes in a high-risk system developed by a provider, and without compromising its own intellectual property rights or trade secrets, the third party shall, by written agreement with the provider, as relevant, specify the information, capabilities, technical access, or other assistance, such as the examples referenced in Annex IXa, that the third party shall provide in order to enable the provider to comply with the obligations under this Regulation.*** ***The Commission shall develop and recommend non-binding model contractual terms between providers of high-risk AI systems and third parties that supply tools, services, components or processes that are used or integrated in high-risk AI systems in order to assist both parties in drafting and negotiating contracts with balanced contractual rights and obligations, consistent with each party's level of control.***	Similar to above.
~~***Article 28(a) (new)***~~ ~~***Unfair contractual terms unilaterally imposed on a micro, small or medium-sized enterprise***~~ ~~***1. A contractual term concerning the supply of tools, services, components or processes that are used or integrated in a high risk AI system or the remedies for the breach or the termination of related obligations which has been unilaterally imposed by an enterprise on a micro, small or medium-sized enterprise as defined in Article 2 of the Annex to Recommendation 2003/361/EC shall not be binding on the latter enterprise if it is unfair.***~~	Burden shifting depending on risk may be appropriate and a term like this will have a significant chilling effect. The size of an enterprise has no meaningful bearing on the risk its systems or components may pose to fundamental rights and/or safety. If a micro, small or medium enterprise develops a component that leads to a damaging impact, a deployer or downstream developer that incorporates or leverages it should be able to rely on contractual mechanisms for recourse, especially when it arises from that MSME's non-compliance with its obligations under other EU legislation.
~~***2. A contractual term is unfair if it is of such a nature that its use grossly deviates from good commercial practice in the supply of tools, services, components or processes that are used or***~~	

~~***integrated in a high-risk AI system, contrary to good faith and fair dealing. A contractual term is also unfair if it has the effect of shifting penalties referred to in Article 71 or associated litigation costs across parties to the contract, as referred to in Article 71(8) (new).***~~	
Article 28b (new) ***Obligations of the provider of a general purpose AI system*** ***1. Without prejudice to Articles 5 and 52 of this Regulation; a provider of a general purpose AI system used in a high risk AI system shall, prior to making it available on the market or putting it into service, ensure that it is compliant with the following requirements***~~***, regardless of whether it is provided as a standalone model or embedded in an AI system or a product, or distributed through open source, API or both, as well as other distribution channels***~~***. When fulfilling those requirements, the generally acknowledged state of the art shall be taken into account, including as reflected in relevant harmonised standards or common specifications. Providers can experiment in fulfilling these requirements provided they make their best efforts to ensure an equivalent level of compliance.*** ***(a) objective of this Regulation of ensuring safety and respect of existing law on fundamental rights and Union values. This shall be demonstrated through appropriate design, testing and analysis that ensure identification, reduction and mitigation of use-agnostic risks in line with Article 9, mutatis mutandis, prior and throughout development, and documentation of non-mitigable risks remaining after development and reasonably foreseeable misuse.*** ***(aa) the data on which the general purpose AI systems used in a high risk AI are developed shall be subject to appropriate data governance measures, including:*** ***(i) the relevant design choices;***	It is critical that the requirements in this article apply only to general purpose AI systems used in high risk applications. Deviation from this risk-based approach will significantly impact low risk, useful, and widely accepted technology, such as functionality to fast forward through commercials, provide subtitles, or translate every-day business documents. This would be a sea change for businesses and consumers, and is a significant departure in how the Act has been framed up until this point. To the extent the substantive requirements throughout Article 28b mirror the existing high-risk requirements, they are duplicative and unnecessary here. The text regarding the ability to "experiment in fulfilling these requirements" has been moved from subsection 2 below to apply more broadly given the flexibility needed for general purpose AI systems to meet certain high risk requirements.

(ia) formulation of assumptions, notably with respect to the information that the data are supposed to measure and represent; (ii) assessment of the suitability of the data sets; (iii) examination in view of possible biases and appropriate mitigation measures; (iv) the identification of possible data gaps or shortcomings; (v) measures to ensure that the data are representative and appropriately vetted for errors;	
~~(a)~~ General purpose AI systems used in a high risk AI shall be designed and developed in such a way as to ~~achieve~~ enable throughout their lifetime, provided they are deployed in accordance with provider instructions, ~~use-agnostic~~ consistent levels of ~~statistical performance, predictability, interpretability, corrigibility, safety and cybersecurity~~ performance in line with Article 15 of this Regulation. ~~These levels shall be assessed through model evaluation by competent external independent experts selected in consultation with the AI Office and documented analysis and testing during conceptualisation, design, and development, in line with the latest assessment and measurement methods, reflected notably in benchmarking guidance and capabilities referred to in Article 58a (new).~~	A separate quality management process involving external experts is not appropriately tailored to risk. The specifics around this requirement are extremely vague and unclear – level of involvement, duration, methodology, metrics, and outcome. Further, adding such a significant layer of responsibility for AI offices, particularly for such rapidly developing technology, would have the effect of substantially slowing down innovation. The Act's existing high-risk requirements provide appropriate protections to Europeans.
(b) General purpose AI systems used in high risk AI systems shall be accompanied by intelligible instructions in line with Article 13.2 and 13.3, mutatis mutandis, in order to enable prospective providers comply with their obligations pursuant to Article 28.2.	
(c) When trained to be used to generate, autonomously or on the basis of limited human input, complex text content that would falsely appear to a person to be human generated and authentic, such as news articles, opinion articles, novels, scripts, and scientific articles, general purpose AI systems shall in addition be subject to the obligations outlined in Article 10 and Article 52(x), with the exception of such AI systems used exclusively for content that undergoes human review and for the	Preferred approach is to delete this provision. Recognizing that may not be feasible, recommend moving this to a separate Article since it more specifically relates to generative AI and deleting Article 10. Article 10 isn't targeted to the risks contemplated in this paragraph, and policymakers should take an approach that is

publication of which a natural or legal person is liable or holds editorial responsibility.	focused on identifying risks and putting in place safeguards to mitigate those risks.
(d) Before placing on the market or putting into service a general purpose AI system used in high risk AI systems, providers of that system shall register that general purpose AI system used in high risk AI systems in the EU database referred to in Article 60, in accordance with the instructions outlined in Annex VIII paragraph C.	
2. A provider of a general purpose AI system used in high risk AI systems shall establish a quality management system as described in Article 17 and draw up technical documentation as referred to in Article 11 to ensure and document compliance with this Article, and can experiment in fulfilling these requirements provided they make their best efforts to ensure an equivalent level of compliance. ***3. For the purpose of complying with the obligations set out in this Article, providers of such systems shall follow the conformity assessment procedure based on internal control set out in Annex VI, points 3 and 4.*** ***4. Providers of such systems shall also keep the technical documentation referred to in paragraph 2 at the disposal of the national competent authorities for a period ending ten years after the general purpose AI system is placed on the Union market or put into service in the Union.***	
Article 15 ***Accuracy, robustness and cybersecurity*** ***1a. (new) To address the technical aspects of how to measure the appropriate levels of accuracy and robustness set out in paragraph 1 of this Article, the AI Office shall bring together national and international metrology and benchmarking authorities and provide guidance on the matter as set out in Article 56, paragraph 2, point (a).***	
Article 58 **Tasks of the Office** ***(ca) (new) provide interpretive guidance on how the AI Act applies to the ever evolving typology of AI value chains, and what the resulting implications in terms of accountability of all the entities involved***	For (ca), no comment. To better align with a risk-based approach, have provided changes to apply the provision to GPAI used in high risk AI systems. Have provided for intellectual property and trade secrets to be protected.

will be under the different scenarios based on the generally acknowledged state of the art, including as reflected in relevant harmonized standards; (cb) (new) provide particular oversight and monitoring of of general purpose AI systems used in high risk systems ~~as well as as well as AI systems that make use of such AI models industry~~ and industry best practices for self-governance; (cc) (new) engage in and facilitate exchanges with providers of general purpose AI systems used in high risk AI systems. Without compromising the intellectual property rights or trade secrets of relevant providers, deployers, or other third parties, Any such meeting shall be open to national supervisory authorities, independent experts, notified bodies and market surveillance authorities;	
Article 58a (new) Benchmarking The European authorities on benchmarking referred to in Article 15 (1a) and the AI Office shall, in close cooperation with international partners, jointly develop cost-effective guidance and capabilities to measure and benchmark aspects of AI systems, and notably of general purpose AI systems, relevant to the compliance and enforcement of this Regulation based on the generally acknowledged state of the art, including as reflected in relevant harmonized standards.	
ANNEX VIII Section C - The following information shall be provided and thereafter kept up to date with regard to general purpose AI systems used as high risk AI systems to be registered in accordance with Article 28b (e). 1. Name, address and contact details of the provider; 2. Where submission of information is carried out by another person on behalf of the provider, the name, address and contact details of that person; 3. Name, address and contact details of the authorised representative, where applicable; 4. AI system trade name and any additional unambiguous reference allowing identification and traceability of the AI system; 5. Description of ~~the capabilities and limitations of~~ the intended purpose of the ~~general purpose~~ high risk AI system, including reasonably foreseeable misuses ~~and measures taken to mitigate significant risks arising from such misuse;~~ ~~6. A description of the measures taken by the provider to comply with the obligations set out in~~	The obligations should be limited to general purpose AI systems that are used as high risk systems. Applying these obligations to low risk system does not meaningfully protect EU citizens against risk and adds significant burden to both companies and administrators of reporting mechanism. The substantive requirements should be similar to those placed on high risk systems, and the edits here reflect that.

~~Article 28b(a), 28b(b), and, where relevant, 28b(d)~~ ~~7. The technical documentation referenced in Article 28b(c)~~ 8. Member States in which the general purpose AI system used as a high risk system is or has been placed on the market, put into service or made available in the Union; 9. URL for additional information (optional).	
ANNEX IXa (new) EXAMPLES OF INFORMATION AND OTHER ASSISTANCE BY THE ~~GENERAL PURPOSE AI~~ PROVIDER OR OTHER THIRD PARTIES TO DOWNSTREAM OPERATORS The following are examples of the information capabilities, technical access, or other assistance ~~shall be taken into account by the provider of a general purpose AI system to comply with the obligations~~ laid down in Article 28 paragraph 2 of this Regulation: To enable compliance with downstream providers' risk management obligations under Article 9 of the Regulation: • Information about the capabilities and limitations of the general purpose AI system, including a description of the functionality it offers ; • Instructions for how the general purpose AI system should be used; • A detailed description of any relevant testing that has been done by or on behalf of the provider of the general purpose AI system with respect to the system's performance, including a summary of the testing methodology used; • Information about steps taken by the provider of the general purpose AI system to identify and mitigate the known and reasonably foreseeable risks that can be reasonably mitigated through the development or supply of the general purpose AI system, as applicable; • Any relevant information to assist providers of high-risk AI systems conducting performance testing as required by this Regulation.	Expanded to cover various parties responsible to provide assistance, as noted above. Items listed here should be examples, to avoid prescriptive requirements that do not accurately reflect the nature of the parties relationship, the use case, or the technology. Examples below must more closely track to the obligations of the Act to avoid confusion. For example, for training data (second bullet in Art. 10 section), Act requires a data collection process, not a disclosure of how the specific data was actually collected. It should be sufficient for a AI component supplier to provide their process and confirm this data was collected in accordance with that process.

To enable compliance with downstream providers' data governance obligations under Article 10 of the Regulation: • ***An overview of the relevant design choices as well as a summary of the data sources on which the general purpose AI system was trained, as applicable;*** • ***An overview of how the training data was collected and processed,*** • ***The formulation of relevant assumptions in relation to the data, notably with respect to the information that the data are supposed to measure and represent;*** • ***An assessment of known or reasonably foreseeable biases in the data;*** • ***The identification of known possible gaps or shortcomings in the data and how they may be addressed.***	
To enable compliance with downstream providers' technical documentation obligations under Article 11 of the Regulation: • ***The name of the general purpose AI system provider, registered trade name or registered trademark, the address at which it can be contacted;*** • ***The date and version of the general purpose AI system, how its architecture interacts or can be used to interact with hardware or software that is not part of the AI system itself, versions of relevant software or firmware, the description of hardware on which the AI system is intended to run;*** • ***The design specifications, including the general logic of the general purpose AI system and its algorithms, its key design choices including the rationale and assumptions made, and the main classification choices;*** • ***The expected lifetime of the general purpose AI system and any necessary maintenance and care measures to ensure the proper functioning of that system, including as regards software updates;*** • ***The known or foreseeable circumstance, related to the envisioned use of the general purpose AI system at the time of design and training, which may lead later to risks to the health and safety or fundamental rights, democracy and rule of law or the environment, as well as installed mitigation measures based on the generally acknowledged state of the art to manage the risks associated with the design of the system.***	

To enable compliance with downstream providers' record keeping obligations under Article 12 of the Regulation: • ***Documentation about the nature and format of the general purpose AI system's input and output data.***	
To enable compliance with downstream providers' transparency and human oversight obligations under Articles 13 and 14 of the Regulation: • ***Relevant and appropriate information to help providers draft instructions that allow a trained deployer to understand the system's output and perform human oversight;*** • ***An overview of the design and development choices that could have an effect on the potential inclusion of human oversight mechanisms in a high risk AI system.***	
To enable compliance with downstream providers' accuracy, robustness, and cybersecurity obligations under Article 15 of the Regulation: • ***A detailed description of any relevant testing that has been done by or on behalf of the provider of the general purpose AI system with respect to its performance, including a summary of the testing methodology used;*** • ***Any relevant information to assist providers of high-risk AI systems with conducting performance testing as required by this Regulation.***	
To enable compliance with relevant aspects of the downstream providers' obligation to establish a quality management system under Article 17: • ***A description of design, design control, design verification, quality control, quality assurance, examination, test and validation actions or procedures carried out before, during and after the development of the general purpose AI system, in accordance with generally acknowledged state of the art in these domains;***	

• ***Where relevant, such as when the general purpose AI system is provided through an API, risk management measures and procedures undertaken by the general purpose AI system provider while the AI system is in use as well as measures and procedures for the general purpose AI system provider to report serious incidents of the general purpose AI system.***	
Other relevant information downstream providers' require in order to comply with its obligations, including the obligation to undertake a conformity assessment under Article 43 of this Regulation, or take corrective actions under Articles 21, 65 or 67 of this Regulation.	