European Office

VDMA position paper on the EU Commission's proposal for an Artificial Intelligence Act

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS COM(2021) 206 final

August 2021

Registration number in the register of representative bodies: 976536291-45

1. Introduction and general comments

For the European mechanical engineering industry, artificial intelligence is a key technology with strategic importance for competitiveness and sustainability: on the one hand, AI is an opportunity to ensure global product and technology leadership. AI helps to increase efficiency and develop new business models. Factories can be optimized; machines and services are enhanced with intelligent functions through embedded AI solutions. On the other hand, AI also holds considerable potential for using materials and energy more efficiently, making better decisions and thus overcoming challenges such as resource scarcity and climate change.

Mechanical engineering companies are primarily users and integrators of AI technologies: as providers of industrial solutions, they play a central role in the dissemination and application of AI in industrial value chains. Their machines and plants bring AI solutions as embedded AI to a variety of customers and industries - in the EU domestic market, but also worldwide as an export-strong industry.

The VDMA therefore supports the goal of creating harmonized rules for the use of AI throughout the EU and avoiding national fragmentation of the EU single market. A harmonized legal framework in the EU is a prerequisite for catching up and keeping pace with global competition in AI. Fundamental rules for the use of AI are also necessary to minimize the threat to fundamental rights and to create acceptance for this technology.

The risks of AI vary with the application: It is therefore positive that a differentiating approach has been chosen in the proposal of the AI Act, which attempts to consider the different applications of AI. In principle, the gradation of the risk classes and the intensity of regulation assigned to these classes seems appropriate. The ban of certain socially and ethically unacceptable AI applications is consistent and the division into further three classes for critical AI systems, for AI systems that require a certain degree of transparency and for AI systems that are harmless seems purposeful. The model of the "risk pyramid" corresponds to reality: a small number of critical applications, and many less critical or completely harmless applications. It is particularly positive that the EU Commission's proposal does not provide for any general authorization obligations, because this would have a massive negative impact on the innovation and widespread use of AI applications in the EU.

However, these four risk classes can only represent a rather rough classification. For each use case, a specific assessment of the respective application and choice of measures appropriate to the risk must be possible. For this, economic actors need flexibility when implementing the legal requirements. In this aspect, the proposal has a weak point: it offers little scope for a risk-based implementation of the requirements and does not offer a suitable methodology for case-specific risk assessment (Article 7 does set out a number of criteria for Annex III adjustments, but these criteria only apply to the regulatory adjustment process and do not serve a risk assessment in the context of compliance with the law). The draft act is only risk-based in a limited sense because the risk assessment is primarily carried out ex-ante by the legislator and leaves little room for action for the economic actors. It would therefore be desirable if the future AI act were more limited to essential requirements. In addition, the real autonomy of the overall system should serve as a criterion for risk classification. Classification via the type of AI technology and areas of application carries the risk that non-decision-making, subordinate AI systems will be in the scope and that even non-critical AI will be subject to burdensome conformity procedures. The approach of continuing to carry out risk assessment and classification via delegated acts of the EU Commission in the future also appears to be insufficiently flexible and future-proof for a technologically and socially very rapidly developing field such as AI.

From the point of view of innovation policy, it is also regrettable that the EU Commission's proposal emphasizes the risks of AI in reasoning and wording. The term "high risk" alone gives the impression that these AI systems pose immediate and great dangers to life, limb and human rights. However, this impression is wrong: many of the AI applications classified as "high risk" in the AI Act are controllable and rather to be classified as "sensitive" or "critical", but hardly as "high risk".

This applies in particular to the industrial use of AI in machines and production equipment. At the current time, there are no indications that AI in industrial application causes problems in terms of operational safety, mainly because not every use of AI increases the autonomy of the systems. In addition, there is already technology-neutral product regulation in place that clearly subordinates the use of AI to safety objectives. In the view of the VDMA, it would not have been necessary to classify AI in industrial machinery that is already subject to harmonized EU safety regulations (such as the Machinery Regulation) as a "high-risk application". Industrial applications that are already subject to harmonized safety legislation should therefore be excluded from the scope.

Should the EU legislator maintain the view that already regulated products need to be covered additionally by AI-regulation, the overlap must be as small and targeted as possible. The envisaged restriction of the high-risk classification to safety-relevant AI software is a practicable approach to this end. It is therefore imperative that the high-risk classification of AI remains limited to safety functions. This criterion must be formulated even more clearly, to avoid legal uncertainty and an unclear interplay between the interweaved legal acts.

The approach to use existing harmonized EU legislation and the proven principles of the New Legislative Framework (NLF) is positive, as well as the attempt to choose less invasive options and, for example, to dispense, where possible, with the burdensome option of third-party conformity assessment for the applications listed in Annex III.

The requirements, however, such as those relating to transparency, data management and human supervision go too far and partly contradict not only the nature of AI systems, but the nature of software systems in general. For example, it is hard to guarantee that training data for AI-systems is error-free or to fully explain how machine learning methods produce results. It is equally difficult to ensure for non-AI-systems that test data and the programmed behavior is 100%-error free. At this point, to enable realistic applicability, the requirements should be reviewed and formulated rather as essential requirements. Detailed technical provisions according to the state of the art must be described in the corresponding standards.

The efforts to establish "common specifications" as an alternative to harmonized standardization and to authorize the EU Commission accordingly should also be viewed critically. This would jeopardize the standardization processes which has been tried and tested for many years. Especially regarding the international level and cooperation with ISO and IEC, such a specific European solution would be a major step backwards. The use of technical specifications should therefore be an exception and subject to strict conditions.

Regarding the treatment of AI in the supply chain, the proposal leaves some questions open: This concerns above all the roles of "provider", "product manufacturer" and "user", which are increasingly being reshuffled in the context of the use of AI (and digitalization in general). A more precise definition of the roles and obligations would be desirable.

The aim of creating a horizontal law and at the same time integrating existing legislation has resulted in a proposal that is in principle purposeful, but also complicated. Not least the multitude of annexes and references shows this complexity, which will be a challenge

for companies and authorities. Some ambiguities and very broad definitions bring the risk of regulating far more than the objectives of the law require.

Especially for smaller companies and for applications with lower scaling potential, there is therefore a danger that the AI Act might lead to uncertainty and hamper the widespread use of AI. The legislators are now called upon to simplify wherever possible, to slim down and by no means to include more cases or protection goals. If the AI Act is not to become a "bureaucratic monster", the focus must be on safeguarding fundamental rights and protecting life and limb. Before it enters into force, the core act must also be supplemented by an official guideline.

2. Comments in Detail

To make the present proposal more legally secure and innovation-friendly, the VDMA believes that there is a need for clarification and improvement. This concerns the following aspects in particular:

Scope, Definitions and Classifications (Title I I, II and III Chapter 1, Article 1 to 7)

Article 3 (1) Definition of "AI system": The AI-techniques in Annex I that classify software as an "AI system" are extensive and contain methods that do not constitute AI in the narrower sense when used individually, such as the expert systems and statistical procedures mentioned under b) and c). Even though these methods can play a decisive role in automated decision-making processes in critical applications, the question of measurability and possible thresholds arises especially in the case of these non-AI methods. The listing of techniques does not answer the question at what point the use of the methods mentioned qualifies as artificial intelligence. To sharpen the focus of the law and eliminate ambiguities, the VDMA proposes a limitation to the AI methods listed under a).

Article 3 (14) Definition of “safety component of a product or system”: The definition of safety component is crucial for the classification as "high-risk" AI with risks to life, limb, and fundamental rights. It therefore goes beyond the objectives of the AI-act if, regarding a failure or malfunction of the AI system, the definition also includes the risk to property. The criterion "property", especially if used without threshold values, leads to a far-reaching high-risk classification, which would then also affect, for example, purely technical processes (e.g., "predictive maintenance") without relevance to the safety of humans or fundamental rights. In terms of consistency, this definition also raises questions: The definition of safety component in the Machinery Regulation, for example, does not include property damage. The term "property" should therefore be deleted from the definition.

Article 6 (1) a) Classification rules for high-risk AI systems: The classification of "High-Risk" via the reference to existing harmonized EU legislation in Art. 6 (1) raises questions as to how the interaction between the provisions should be made. The wording *"the AI system is intended to be used as a safety component of a product covered by the Union harmonization legislation listed in Annex II or is itself such a product"* extends the classification beyond safety components to software products if they are products in the sense of the respective harmonized legislation. In principle, this is purposeful. However, since this is an essential interface between the regulations, the reference to safety components and safety-relevant software products must be formulated in a legally secure and unambiguous manner (for example, by expanding recital 30).

Article 6 (1) b) Classification rules for high-risk AI systems: An additional criterion for the high-risk classification of AI systems according to Annex II is the "third party

conformity assessments pursuant Union harmonization legislation". This initially appears to be a pragmatic approach, but it leads to problems in the interplay of the legal acts: The method of conformity assessment must be a consequence of the risk assessment and therefore cannot itself serve as a criterion for risk classification. This intertwining of criteria makes it difficult to have appropriate rules on conformity assessments in the respective legal acts. The fact that the criterion "third party assessment" is used as a criterion in the AI-Act leads to a restriction of flexibility regarding the third-party assessment obligation in the vertical legal acts. In principle, however, a third-party assessment obligation should always be waived with a view to innovation-friendliness if the risk assessment allows it. Particularly in mechanical engineering, where often customized solutions are commercialized, a third-party audit is very obstructive, triggers high avoidable economic burdens and can become an unnecessary barrier to the use of AI. In the view of the VDMA, the legal acts must therefore be unbundled and the question of the type of conformity assessment must be regulated in the respective laws independently and with the lowest possible depth of intervention. It should be examined whether the safety criterion in Art 6 (1) a) can be considered sufficient as a criterion for high-risk AI.

The option of manufacturer self-declaration mentioned in Art 43 (3) last paragraph is to be welcomed and should be retained.

Article 6 (2) / Annex III: With the "high risk" classification of certain "stand-alone" AI systems with relevance for fundamental rights (Annex III), the proposal breaks new ground: for the first time, software is subject to product regulation and corresponding CE marking. In principle, it is to be welcomed that the tried and tested NLF approach is being used here. It can be seen as innovation-friendly that a third-party conformity assessment is not generally requested. The list of areas in Annex III includes areas that involve the assessment of people, and which are therefore correctly classified as critical. However, the description under point 4 b) is too broad and could also cover applications that are not relevant to fundamental rights (such as operational task assignments that are within the scope of a job description). At this point, it must be considered that humans are also part of value chains that can be optimized by artificial intelligence. A general regulation of IT-supported operational optimizations without relevance to fundamental rights and without risk of discrimination must be avoided. Therefore, a differentiation of point 4 b) is needed.

Requirements for high-risk AI systems (Title III, Chapter 2, Articles 8 to 15)

In terms of content, the requirements for AI systems in the proposal go in the right direction and are often formulated in a neutral and flexible way (e.g., Article 9 on "risk management system" is exemplary and, in the interest of simplification, it should be examined whether Article 9 does not already cover many requirements of this chapter). However, many requirements are technically too prescriptive, too far-reaching and, in some AI applications, difficult to implement. There is a danger that necessary differentiations are not possible and that unnecessary or excessive regulations will result. The requirements should better be formulated as essential principles, leaving detailed prescriptions to standards or guidelines.

Article 10 Data and data governance: In principle, it is right to require a minimum quality for AI data in critical AI systems. However, the requirements in Article 10 go into too much detail to be suitable as a horizontal provision. In particular, the requirements in Art. 10 (2) e), (3) and (4) go too far and cannot be met for many AI applications in this form. This applies in particular to applications that continue to learn with field data after

being placed on the market, such as machines that "train" the AI system in the field with the help of reinforcement learning. The VDMA therefore proposes that the requirement for data quality should be anchored in the AI Act as an essential requirement and that details and the state of the art should be described in application-specific guidelines or on standards.

Article 11 Technical documentation: The requirements go far beyond those described in NLF legal acts and seem excessive for many AI applications. For example, it is incomprehensible why the technical documentation of non-learning AI applications must also be kept up to date by (Art. 11 (1)) or why a single technical documentation is required (Art. 11 (3)). At this point, more freedom of action should be left for case-specific measures and implementation by the manufacturer. The amendment of a conformity assessment procedure by delegated acts provided for in Art. 11 (3) should be rejected.

Article 14 Human supervision: Continuous and detailed human supervision of AI systems is not always possible because the logic of decisions is not always comprehensible and the speed of automated AI systems is too high (in certain cases, operational supervision would even contradict the principles of ergonomics). AI systems are used especially in applications where they are superior to human decisions, including where they produce less errors. The requirements in Article 14 therefore are not appropriately reflecting the potential and risk of AI systems. Some of the requirements are not relevant in certain application scenarios or cannot be implemented at all. This concerns above all the requirements in paragraph (4) a) *("fully understand the capacities and limitations of the high-risk AI system"*) and paragraph (4) *e) ("stop button"*). Interpretability and control by humans are important criteria for the acceptance and legal assessment of AI. However, the importance depends very much on the application and must be assessed for each use case. Furthermore, the explainability of AI is still the subject of intensive research and adaption will be necessary. To avoid a technology ban in certain critical applications, it must be possible in principle to qualify and use AI in critical applications as well. In addition, the possibility of higher-level technical supervision by "non-AI" technologies must be explicitly provided for in the AI Act (for example, through a formulation such as "*also with suitable technical systems or tools of a human-machine interface*"). In the view of the VDMA, the AI-Act should not provide for a general requirement for "human oversight". Such supervision should only be requested in cases in which fundamental rights are directly affected, technical safeguarding is not possible, and the human decision is ethically indispensable.

Article 15 Accuracy, robustness, and cybersecurity: This article contains a number of requirements that go beyond the objectives of the AI Act and go into too much detail. For example, specifying accuracy metrics is hardly suitable as a general requirement for all AI systems covered. The statements in Article 15 (3) on "biased output" are unclear and rather an attempt to create technical specifications. Cybersecurity requirements should be described in a separate horizontal legal act.

Obligations of providers and users of high-risk AI systems and other parties (Title III, Chapter 3 Articles 16 to 29)

Article 20 Automatically generated logs: Obligations arising from contractual agreements and not from legal requirements are superfluous in an EU regulation. The sub-sentence “a contractual arrangement with the user” should be deleted.

Article 29 Obligations of users of high-risk AI systems: The way of describing the obligations for users are not in line with the NLF approach. The AI Act unfortunately

leaves many questions open in this perspective. A precise definition of the obligations of the actors would therefore be desirable.

Standards, conformity assessment, certificates, evaluation, registration (Title III, Chapter 5, Articles 40 -51)

Article 40 Harmonized standards: The presumption of conformity in case of application of harmonized standards is purposeful and relieves the burden on companies and authorities. However, it is unclear to what extent the existing harmonized standards cover the requirements of the AI-Act. It is therefore necessary to identify the need for standardization in cooperation with industry in advance and to initiate the corresponding standardization mandates.

Article 43 Conformity assessment: In principle, it is welcomed that the conformity assessment procedures of the respective sectoral regulations are acknowledged, and that standardization is assigned a central role.

- Paragraph (3): It is positive that no additional conformity assessment and no independent CE mark is necessary for AI systems according to Annex II. However, the wording does not exclude duplication: If, for example, safety-relevant AI software is integrated into a machine according to Annex 1 of the Machinery Regulation, according to Position 24 of Annex 1, this AI software is already subject to conformity assessment by a third party. If this software is then integrated into a machine, this machine has an embedded AI system that is safety relevant. Therefore, the machine is also subject to assessment by a third-party, see position 25 of Annex I. For such cases, there is a need for clear provisions that avoid duplicate tests of AI systems (these may also not be carried out by the same notified bodies, as otherwise the same object would be assessed tested several times by the same body). It is very positive, however, that the manufacturer's self-declaration is in principle also possible under certain conditions for AI systems covered by Annex II.
- (5) and (6): The EU Commission is authorized to amend the elements of the conformity assessment procedures as well as points (1) and (2). This is to be rejected. Conformity assessment procedures are the core element of regulation and must be amended through a regular legislative procedure.

Article 51 / Article 60: Registration: The added value of central registration is unclear; however, it creates additional effort and barriers to innovation. This is especially true for applications with low scaling potential.

Post-market monitoring by providers and post-market monitoring plan for high-risk AI systems (Title VIII, Chapter 1)

Article 61 Post-market monitoring: The general obligation to establish a system for post-market monitoring and continuous evaluation of compliance of AI systems with the requirements is burdensome. Furthermore, it is not purposeful for all use cases and cannot always be implemented in practice. In particular, the exchange of the necessary data with the user is unlikely to be possible in all cases. The AI systems covered by the legal acts listed in Annex II should only be subject to the monitoring obligations set out in these legal acts. Paragraph (4) should be phrased more clearly in this respect.

Sharing of information on incidents and malfunctions (Title VIII, Chapter 2)

Article 62 Reporting of serious incidents and of malfunctioning: The reporting obligation for providers of high-risk AI systems in the event of serious incidents seems excessive. The added value is unclear.

Confidentiality and penalties (Title X)

Article 71: Penalties: The maximum fines of 6% and 4% required in paragraphs (3) and (4) respectively are excessive. In particular, the level of sanctions for breaches of Art. 10 is inappropriate in the context of an emerging technology characterized by a high level of uncertainty. It is to be expected that penalties in this dimension will unsettle many potential developers and users and will especially hinder AI-applications in SMEs and in use cases with smaller scaling potential.

3. Summary and Key Messages

For the European mechanical engineering industry, artificial intelligence is a key technology for competitiveness and sustainability. We therefore support the EU Commission's plans to create a reliable EU legal framework and thus avoid national fragmentation, while at the same time increasing acceptance for AI technologies by regulating the risks.

It is right that a graduated approach has been chosen that in principle differentiates according to risks and does not treat AI systems equally. We also support the use of the principles of the "New Legislative Framework" ("NLF") and of harmonized standards.

On the other hand, the high-risk classification and depth of intervention go too far. There is a risk that many applications will be regulated that should not fall under the protective goals of the planned act because their decision-making autonomy is low, or the risks are already regulated. The proposed act runs the risk of creating a complicated and overly prescriptive legal framework that will hamper AI innovation. In our view, the AI Act must therefore be fundamentally streamlined by focusing more consistently on the protection of fundamental rights, whilst excluding already regulated areas and leaving the details to standardization. In this way, more leeway for a risk-based implementation of the requirements can be created without lowering the ambition. Especially in industrial applications, AI must not be over-regulated now if the technological sovereignty of the EU is not to be endangered and digital sovereignty is to be increased. We therefore see a need for improvement above all in the following points:

VDMA key messages

- **Exclude already regulated industrial AI from the scope:** There is no evidence at this stage that AI in industrial application causes problems in terms of operational safety. Autonomy of industrial AI is limited and AI in machines is covered by technology-neutral product regulation. Industrial AI applications that are already subject to harmonized safety legislation and do not have a relevance for human rights should be excluded from the scope.
- **Limit "high risk"-category of embedded AI to safety-relevant components:** If AI embedded in industrial machines remains within the scope of the AI Act, the classification as "high risk" should remain limited to safety-relevant components.
- **Streamline the AI act, improve regulatory efficiency:** In principle, the approach of defining four risk classes goes in the right direction. However, the requirements - such as those relating to transparency, data management and human

supervision - go too far, are too prescriptive and partly contradict the nature of AI systems and software systems in general. The provisions in the AI Act should be limited to the essential requirements and allow for a more risk-based and efficient implementation. Definitions and scope need to be more focused and sharpened. No additional regulation cases, risk classes or protection goals should be included.

- **Sharpen definition of AI in Annex I:** To sharpen the focus of the act and remove ambiguities, the procedures listed in Annex 1 should be limited to the AI methods in the narrower sense listed under a).
- **Make autonomy a criterion:** To avoid regulation of non-decision-making AI functions, a cross-cutting "autonomy criterion" should be introduced n for defining the scope of the regulation.
- **Sharpen definition of "safety component":** The extension of the protection goal "safety" on “property” expands the definition of "high risk" far beyond the protection of fundamental rights, for example to industrial processes without any human rights implication. The criterion "property" should be deleted from the definition in Article 3.
- **Simplify classification rules for high-risk AI systems under Annex II:** The criterion "third party conformity assessment" mentioned in Art 6 (1) b is inappropriate because it unnecessarily refers to this burdensome conformity assessment procedure. It should be examined whether the criterion mentioned in Art 6 (1) a is sufficient for categorization as "High-Risk".
- **Maintain and expand the use of manufacturer self-declaration:** Third-party conformity assessment is costly and inhibits innovation. The option of manufacturer self-declaration („internal control”) must be retained and made possible for AI systems in accordance with Annex II.
- **Remove mandatory registration:** The added value of central registration is unclear. However, it creates additional effort and barriers to innovation.
- **Support developers and users and strengthen the standards landscape:** To facilitate the implementation of the requirements, the EU Commission must provide accompanying official guidelines. In addition, to enable efficient conformity assessments, the need for standardization must be identified in cooperation with industry and standardization mandates must be initiated.

VDMA contacts:

Kai Peters
VDMA European Office
+322 7068219
E-Mail kai.peters@vdma.org

Guido Reimann
VDMA Software and Digitalization
Coordinator Competence Network Artificial Intelligence
+49 69 6603 1258
E-Mail guido.reimann@vdma.org

Kai Kalusa
VDMA Informatics
+49 30 3069 4624
E-Mail kai.kalusa@vdma.org