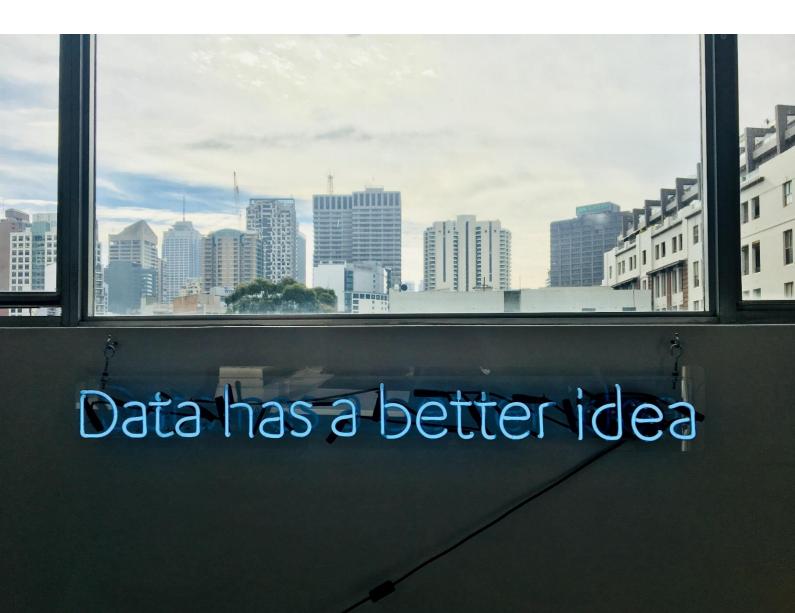Cornerstones of a European legal framework for the safe use of AI

On the safety of AI-based systems

At a glance

Artificial intelligence (AI) is playing an important role in ever more areas of our lives – be it in smart homes, automated driving or medical technology. The effects on our lives are likely to be considerable and cannot be fully foreseen at the current time.

On the one hand, AI has the potential to bring about major improvements; on the other hand, it harbours a series of possible risks. In order to adequately address these risks and exploit the potential, clear guidelines are needed for the regulation of AI-based systems[1] on both the national and international levels. The European Commission also emphasises the importance of an appropriate regulatory framework in its White Paper on AI published in February 2020.

> "A solid European regulatory framework for trustworthy AI will protect all European citizens and help create a frictionless internal market for the further development and uptake of AI as well as strengthening Europe's industrial basis in AI."

White Paper on Artificial Intelligence of the European Commission | February 2020

Our position

The TÜV Association is of the opinion that the applicability of the existing legislation to AI-based systems must urgently be reviewed. Reviewing legislation will allow the existing (safety) requirements to be adapted and/or new ones formulated. That being said, it is clear that not all AI-based systems must meet the same requirements. In line with the European Commission, the TÜV Association advocates a risk-based approach and a classification of AI-based systems into risk categories according to clear criteria. The use of AI-based systems in high-risk areas will require particular scrutiny. However, certain fundamental requirements that apply for all AI-based systems can also contribute decisively to safe usage in areas of lower risk. This creates greater trust and transparency for users.

78% Consumers in Germany also demand greater transparency and safety in the use of AI: of survey respondents said that the German government should pass laws and regulations to regulate Artificial Intelligence.[2]

---

1 Unless indicated otherwise, the term "AI-based systems" used in this paper refers to machine learning and/or neural networks. It is synonymous with all possible types of AI (products, services, etc.).
2 TÜV study on safety and artificial intelligence (in German only), 2020. Representative Ipsos survey of 1,000 people aged 16 to 75 years, www.vdtuev.de/news/ki-studie.

Our key demands

1. **Define requirements for AI-based systems**
   The European regulatory framework currently in place does not take the challenges AI faces in many areas into account sufficiently. Therefore, an in-depth review must be conducted of its appropriateness and suitability for AI-based systems. Only a coherent and uniform legal framework can ensure a stable basis for economic activity. Fundamental requirements for all AI-based systems must be addressed through a horizontal legislative approach. The supplementation or specification of sector-specific requirements must additionally take into account the respective characteristics.

2. **Classify AI-based systems into risk categories**
   AI-based systems must be classified into different risk categories. This division into risk categories on the sector level must be based on clearly defined criteria. A regulatory framework oriented to the risk-based approach defines the scope of the review according to the corresponding risk, i.e. the combination of the likelihood of damage occurring and the severity of this damage.

3. **Build trust through independent third-party assessment**
   The involvement of an independent conformity assessment body is indispensable, particularly for high-risk AI-based systems. An independent assessment will thus be conducted on whether the AI-based systems meet the legal requirements and are safe to use. The conformity assessment bodies must be competent, neutral and objective.

4. **Develop conformity assessment procedures further**
   For all types of AI (to varying degrees), there is an urgent need to define the legal, technical and ethical requirements. Existing procedures and methods for conformity assessment must moreover be developed further or, where necessary, new procedures and methods established. The evolving nature of AI-based systems must be taken into account by monitoring conformity through iterative determination or periodic repetition of the conformity assessment (where necessary, in combination with regular monitoring).

5. **Devise an appropriate European data strategy**
   Data plays a major role in AI. Hence, it is imperative to always consider the topics of AI and data in conjunction. Among other aspects, the availability and quality of data are decisive to the development and use of AI-based systems. A European data strategy is required for the appropriate regulation of AI.

Define requirements for AI-based systems

> Create a coherent and uniform legal framework for the regulation of AI-based systems in Europe

> Define fundamental requirements for all AI-based systems through horizontal legislation

> Supplement or specify sector-specific requirements to cater to the different sectors and their respective characteristics

The European regulatory framework currently in place does not take the challenges AI faces in many areas into account sufficiently. An in-depth review must therefore be conducted of its appropriateness and suitability for AI-based systems. Horizontal legislation formulating fundamental requirements for all AI-based systems should follow the principles of existing legislation for the European Single Market, particularly the New Legislative Framework (NLF). Such legislation should summarise and define overarching regulatory aspects. The legal framework for the regulation of AI-based systems in Europe must be coherent and uniform, and offer industry stakeholders a stable and reliable basis for forward-looking entrepreneurial activities.

Some industries or product sectors will require additional specific AI regulatory measures, which are not covered by the fundamental horizontal legislation. The suitability of the existing European product legislation for AI must be reviewed and adapted for this as necessary. In line with the overarching principles, appropriate legislation and additional provisions can be included in or added to existing legislation.

Classify AI-based systems into risk categories

> Orientation to a risk-based approach

> Classify AI-based systems into risk categories on the sectoral level

> Clearly defined criteria for the risk categories

AI-based systems should be considered in terms of their risk. In its White Paper on Artificial Intelligence, the European Commission proposes a dual criteria system, which the TÜV Association in principle welcomes. Consideration of the sector on the one hand and the concrete application on the other hand can lead to classification in the "high" risk category. The TÜV Association believes that a substantial risk exists if the physical integrity of the user or third parties, their privacy or the confidentiality, integrity or availability of their data or non-discrimination is at risk.

However, for AI-based systems that are considered less risky according to this dual criteria system, mandatory essential safety requirements should also be prescribed by law.

Build trust through independent third-party assessment

> Independent conformity assessment is necessary to verify (independently of the manufacturer) that AI-based systems meet the legal requirements and are safe to use

> The European lawmakers must ensure through a risk-based approach that the conformity assessment procedure is in line with the risk potential of the AI-based system

> A conformity assessment must be mandatory as soon as a substantial risk exists

Compliance with legal requirements is key to ensure the trustworthiness of AI-based systems. The TÜV Association believes it must be clear that the European legislator ensures by means of a risk-based approach that the conformity assessment procedure is in line with the risk potential of the respective AI-based system. Within this, it is also clear that an independent conformity assessment must be mandatory if a substantial risk exists.

To ensure that AI-based systems meet the requirements formulated and that they are safe to use, the conformity assessment must be conducted by an independent party. The conformity assessment bodies must be competent, neutral and objective. Fulfilment of these attributes is ensured through official recognition and accreditation and monitored continuously by the government. This will ensure that the independent conformity assessment bodies throughout the EU afford the necessary expertise. Accreditation in responsibility of the public administration is a guarantee of reliability, credibility and confidence. An independent conformity assessment body is therefore absolutely indispensable for high-risk AI-based systems. Even for AI-based systems that are not high risk, a voluntary labelling system by the manufacturers (like the one envisaged by the European Commission, for example) does not go far enough. In addition to the need to define fundamental safety requirements for all AI-based systems, compliance with these requirements must be mandatory – rather than just voluntary. With regard to evidence whether the requirements for AI-based systems of lower risk are fulfilled, manufacturers and operators should be able to choose between an independent conformity assessment that is visible to the market and the authorities by means of a test mark or quality label, and a self-declaration by the manufacturer or operator, indicated by the appropriate.

Develop conformity assessment procedures further

> Conformity assessment of AI-based systems must be oriented to existing procedures

> Legal, technical and ethical requirements urgently need to be defined for all types of AI

> Appropriate conformity assessment procedures must be developed (further) in terms of the different types of AI

The conformity assessment of AI-based systems must be oriented to existing conformity assessment procedures. Within this, a number of challenges relating specifically to AI must be borne in mind. The distinction between trained and continuously learning AI, static and dynamic AI, and online and offline learning AI plays an important role in certification, for example. For all types of AI (to varying degrees), there is an urgent need to define the legal, technical and ethical requirements. Existing procedures and methods for conformity assessment moreover must be developed further or, where necessary, new procedures and methods established. Given the evolving nature of AI-based systems, the monitoring of conformity through iterative determination or periodic repetition of conformity assessment (where necessary, in combination with periodic monitoring) is indispensable. Research and teaching or further and advanced training in the field of AI are further essential requirements for a qualified review and assessment.

Devise an appropriate European data strategy

> The appropriate regulation of AI must be linked to the European data strategy

> Access to high-quality data is essential for AI-based systems

> Data access must be included in future legislation

Particularly the use and further development of functions based on AI depends largely on how access to data can be ensured and its provision improved. The European Commission clearly emphasises the link between these two aspects through simultaneous publication of its AI White Paper and the European Data Strategy. It is also imperative to consider both aspects in parallel and to develop them further during the specification of future legislation. The use of self-learning systems represents a new paradigm in function development whose requirements and effects must be defined anew. Examples include the technical implementation and compliance with ethical frameworks, data protection and the quality of the large quantities of real data required for training and assessment purposes. In particular, the availability, use and exchange of high-quality data[3] must be ensured, along with the compliance with requirements such as confidentiality, transparency and non-discrimination. In order to review and evaluate the effectiveness of safety requirements, independent assessment organisations need a legal right to access the safety-relevant data of AI-based systems. For the mobility sector, the TÜV Association proposes the establishment of TrustCenters as a pragmatic solution.[4] As a trustworthy authority, TrustCenters could provide secure, neutral and non-discriminatory access to relevant data of connected vehicles in compliance with the GDPR for the technical monitoring of these vehicles.

---

3 Existing standards should be applied and the development of new standards encouraged to ensure the quality of the data used to train AI-based systems.
4 See also the TÜV-Association's position paper on automotive TrustCenters – "Remote Access to Vehicle Data for Ensuring Road Safety and Environmental Protection" (2019), available online at www.vdtuev.de/dok_view?oid=775511.

The safety of AI-based systems must be top priority

AI is not a new technology and technical progress and more powerful computer and data transmission capabilities mean that its importance is growing. However, Germans are sceptical of the use of Artificial Intelligence: 67 percent of survey respondents fear that AI-based systems will make mistakes in safety-critical applications, such as highly automated vehicles.[5]

85 %

of consumers in Germany believe that AI-based systems should only be released onto the market once their safety has been verified by independent bodies. This makes it clear: the safety of AI-based systems must be the top priority.

Independent assessment organisations boost the social acceptance of this technology through reliable conformity assessments based on binding legislation and enhance users' trust in the safety of AI-based systems. Hence, the TÜV Association participates in the debate on a European legal framework for AI and advocates the safe use of Artificial Intelligence.

[5] 5 TÜV study on safety and Artificial Intelligence (in German only), 2020. Representative Ipsos survey of 1,000 people aged 16 to 75 years in Germany, www.vdtuev.de/news/ki-studie.

Author and contact

Elisa Brummel
Head of Artificial Intelligence & Education
E-Mail: elisa.brummel@vdtuev.de
Tel. +49 30 760095 360
www.vdtuev.de

About the TÜV Association: The Association of Technical Inspection Agencies (TÜV Association) represents the policy and technical interests of its members within the spheres of politics, administration and industry, and vis-à-vis the general public. It is committed to technical and digital safety for products, systems and services through independent assessments and qualified training. The TÜV Association strives with its members to maintain the high level of technical safety in our society and to build trust in the digital world.