POSITION | DIGITAL POLICY | ARTIFICIAL INTELLIGENCE

BDI-Comments on the proposal for a European AI Regulation

Ensuring the competitiveness of the European industry through innovation-friendly rules.

8. November 2021

Executive summary

Artificial Intelligence (AI) is one of the most important key technologies in the industry. Against this background, unbureaucratic and innovation-friendly framework conditions for the use of AI are a key prerequisite for securing the innovative capacity and competitiveness of the German and European industry in the long term.

It is the right approach that the proposal for a European AI Regulation, presented by the European Commission on 21 April 2021, focuses on AI systems that can be associated with high risks. However, there is still considerable need for improvement in many areas of the proposal. Essentially, it is important to avoid an overregulation of industrial application fields of AI. Otherwise, there is the risk that the development of innovative applications of the key technology AI will be weakened from the outset.

As the design of the legal framework for the use of AI has thus far-reaching consequences for the competitiveness of European companies, the industrial application perspective of AI must be given equal consideration in the further legislative process. A legal definition of Artificial Intelligence that clearly distinguishes AI from conventional software is also urgently needed. If the legal framework for the use of AI in Europe is designed in an innovation-friendly way, European companies - in the combination of their industrial strength with the possibilities of AI - can gain a decisive advantage in international competition.

Key demands of the German industry:

1. The category of 'high-risk AI systems' should be limited to AI systems that are associated with high risks and not covered by existing European and national product safety legislation. On the other hand, industrial AI systems that are already regulated by existing law, should be excluded from the scope.

2. The requirements for 'high-risk AI systems' should be amended at numerous points detailed in this position paper in such a way that they are more proportionate to the risks addressed by the regulation and can be implemented in practice by companies realistically and with reasonable efforts.

3. The innovation-promoting instrument of AI regulatory sandboxes should be designed in such a way that it is also accessible to small and medium-sized enterprises (SMEs) and start-ups in a low-threshold way.

Table of Contents

General provisions and legal system

Articles 1-7 of the draft regulation define the subject matter and scope as well as central legal terms of the European AI Regulation. In this context, the definitions of 'AI system and 'high-risk AI system', which are examined in more detail in the following section, are of central importance for the industry. From the perspective of the German industry, there is still considerable need for improvement on these points. With regard to the other legal definitions in the text of the regulation, consistency should be ensured with the definitions in existing legal acts based on the New Legislative Framework (NLF). For reasons of legal systematics, it should also be examined in the further course of the legislative process whether - as envisaged by the European Commission - 'users' of AI systems should be covered by the regulation, too. This question arises since according to point 2.1. of the explanatory memorandum, the legal instrument pursues the 'proper functioning of the internal market' as its 'primary objective'.

Definition of 'AI system' and 'high-risk AI system'

The notion of AI ('*artificial intelligence system*'), on which the draft regulation is based, is defined in Article 3(1) in conjunction with Annex I of the draft regulation. In principle, the BDI welcomes that the European Commission refers to the OECD in this context[1] and thus takes up an existing debate on the development of definition criteria for AI. However, the definition criteria chosen by the Commission in the draft regulation, in particular the techniques and approaches listed in Annex I ('statistical approaches', 'search and optimization methods'), would mean that conventional software would fall within the scope of the regulation, too. In order to avoid legal uncertainties for market participants and to ensure a specific and clearly delimitable scope of the regulation, the term AI must be defined much more narrowly. In addition, for reasons of legal certainty, it should be examined in the further course of the legislative process whether the definition of AI - analogous to the approach of the OECD - should refer to the level of the 'system' (including hardware).

In addition, any amendments of the legal definition that may be necessary after the entry into force of the regulation should not - as provided for in Article 4 of the draft regulation - be made by means of a delegated act. Since the definition of AI is an essential provision of the regulation, amendments should only be adopted in an ordinary legislative procedure.

From an industry perspective, the definition of 'high-risk AI systems' in Article 6 of the draft regulation is also viewed very critically. Again, the Commission chooses a very broad definition, that assigns AI used in a variety of areas to the high-risk category. This definition is clearly too broad, as it means that non-critical industrial AI applications are also regarded as 'high-risk AI systems'. The consequence would be disproportionate regulatory requirements for providers and users of industrial AI, which would ultimately inhibit innovation. Moreover, the existing national and European product safety law already lays down comprehensive safety requirements that also cover AI as a risk issue. Against this background, there is a risk of double regulation. Therefore, the European AI Regulation should only cover areas for which a regulatory gap has been demonstrated. Industrial AI systems on the other hand that are already regulated by existing law should be excluded from the scope of the regulation. In areas where a regulatory gap exists, additional criteria should be used to classify AI systems as high-risk. These criteria include, for example, human supervision of an AI system or the existence of technical

---

[1] Cf. definition of 'AI system' at https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449

control mechanisms, as these factors can have a significant impact on the level of risk posed by an AI system.

With regard to Article 7 that lays down rules for the amendment of annexes, referenced in Article 6 ('Classification rules for high-risk AI systems'), there is also a need for a more precise specification of the transition periods to be applied in these cases.

Territorial scope

The draft regulation also makes a comprehensive extraterritorial claim. According to Article 2(1)(c) of the draft regulation, the regulation shall also apply to providers and users of AI systems that are established or domiciled in a third country if the result produced by the system is used in the EU. According to the Commission's intention, this is intended to ensure a level playing field and the protection of rights and freedoms in the Union (see, inter alia, recital 10). In particular, this provision is intended to prevent the circumvention of the legal requirements of the regulation. In principle, this objective is welcomed. Nevertheless, there is no specification of how this provision is to be applied and how it could affect international data transfers of personal and non-personal data. Furthermore, it is not conceptually clear what is meant by '*output*' or 'result' and how this provision would affect, for example, the results of analysis of large international data sets. In order to make the provision more manageable for companies in practice, these terms should be defined more precisely. In any case, an obligation for AI users to trace the origin of an AI result in the value chain should be excluded.

NLF nomenclature and relationship with other legal acts

The BDI expressly supports the EU Commission's approach of using the principles of the New Legislative Framework (NLF) and thus relying on existing procedures. The strength of the NLF lies in particular in the interaction between legal requirements and harmonised European standards, i.e. standards drawn up by the European standardisation organisations on the basis of a mandate from the Commission to implement harmonisation legislation in accordance with Regulation (EU) 1025/2012, which are listed in the *Official Journal of the* EU following examination by the Commission.

The process is open to all interested stakeholders via national mirror committees. The progress of standardisation is transparent for all, so that there is a high degree of predictability on all sides. Decisions are taken by consensus, enjoy broad acceptance and are relevant for the entire internal market. This division of work relieves the European legislator of the burden of drafting detailed regulations, the legal framework is kept flexible and the resulting standards are practical and thus easy to implement by companies. The BDI is convinced that the NLF offers a suitable approach to create a regulatory basis for AI in the EU internal market.

The regulation of AI applications that are not covered by existing national and European product safety legislation should be carried out via general horizontal requirements that have to be taken into account equally in all sectors concerned. With regard to the implementation of the horizontal requirements, it must be ensured however that they can be specified in sector-specific terms or be transferred to existing sector-specific regulations. As a result, it must be ensured that only one conformity assessment procedure needs to be carried out and a duplication of processes is avoided.

Prohibition of certain AI practices

Article 5 of the draft regulation describes AI practices that should be prohibited in the future. As set out in recital 15, the aim is to prohibit practices that contradict fundamental values and rights of the European Union. The BDI welcomes this objective in order to strengthen confidence in the use of artificial intelligence sustainably. For reasons of legal certainty, however, the AI practices covered by Article 5 should be specified more clearly, as the provision currently includes a large number of indeterminate legal terms (e.g. 'subliminal techniques'). Especially against the background of the high level of sanctions according to Article 71 of the draft regulation (up to 6 percent of the worldwide annual turnover) a sufficient specification of the requirements is imperative in order to prevent legal grey areas and to create legal certainty for companies.

Provisions for high-risk AI systems

Requirements for high-risk AI systems

Article 8 et seq. of the draft regulation define the requirements that are relevant for the conformity of high-risk AI systems. Overall, the requirements proposed by the Commission are very extensive and associated with a high level of bureaucracy. The development of AI systems for fields of application that fall into the high-risk category would be inhibited as a result. In addition, it is not clearly stated in the draft regulation how single requirements of the AI Act (e.g. for the recording of log data) relate to the requirements set out in other EU legal acts (e.g. the General Data Protection Regulation). Therefore, from the perspective of the German industry, there is a considerable need for improvement and clarification in this context, too.

Article 9 of the draft regulation specifies concretely the requirement to establish a risk management system for high-risk AI systems. For reasons of legal certainty, the notion of risk contained in Article 9(2)(a) of the draft regulation should be specified with regard to the types of risk to be addressed by the risk management system (based on the overarching regulatory objectives of the AI Act, these would be health and safety risks as well as risks relating to the fundamental rights of natural persons). With regard to the implementation of a risk management system for respective AI systems, credit institutions are permitted under Article 9(9) of the draft regulation to integrate the required management system into risk management processes required by a sector-specific directive (Directive 2013/36/EU). The possibility to integrate the risk management for high-risk AI systems into existing risk management processes, which may also apply globally depending on the company, should be granted to all affected sectors in order to avoid unnecessary bureaucracy.

In addition, Article 10 of the draft regulation formulates requirements for training, validation and testing data sets as well as their governance that are overall very extensive. Single requirements, such as the request in Article 10(3) of the draft regulation that data sets shall be free of errors, are de facto impossible to implement in practice. Therefore, greater emphasis should be placed in this context on the implementation of processes that ensure a systematic and rule-based handling of training, validation and testing data sets. From BDI's perspective, there are also tensions with the requirements of the European data protection legislation in this context. Since the training of AI systems requires as much data as possible, the sharing of data sets is in practice of particular importance. However, the applicable provisions for the processing of personal data make it difficult to share data. This is especially the case when, for example, mixed data sets exist. This tension must be taken into account when implementing an innovation-friendly legal framework for the use of AI in Europe.

Among the key requirements of this chapter is also the obligation to draw up a technical documentation set out in Article 11 of the draft regulation. The content of the technical documentation that is specified in Annex IV is also very extensive. One example is the detailed description of the 'elements of the AI system' required under point 2(b), which include algorithms. As the relevant information may constitute trade secrets, a particularly careful balancing of the interests of the addressees of the technical documentation and the protection needs of the company concerned is needed at this point.

Article 12 of the draft regulation also contains an obligation to record logs. With regard to the implementation of the record-keeping, Art. 12(1) of the draft regulation refers to relevant standards. The BDI explicitly welcomes this reference. For biometric identification procedures listed in Annex III, point 1(a), Article 12(4)(c) also provides for a mandatory logging of the input data. Since the storage of sensitive input data may itself entail risks, it should be questioned whether this provision is appropriate. Moreover, the extensive requirements set out in Article 12 of the draft regulation could have the effect that AI is not used in certain areas for economic reasons (bureaucracy). Negative effects like that have to be prevented in order to support the breakthrough of AI in all sectors of the economy.

With regard to Article 13 of the draft regulation that sets out the requirements for instructions for use that shall accompany high-risk AI systems, it is questionable from an industry's perspective whether the partly very detailed and technical information (e.g. concerning the used test data) really offers practical value for users of respective AI systems. To keep the instructions for use manageable and easy to understand in practice, the list of requirements defined in Article 13(3) should be limited to essential information (e.g. on special risks in the event of a non-intended use of the AI system). Furthermore, the obligation in Article 13(3)(b)(ii) to provide information on the expected level of accuracy, robustness and cybersecurity of an AI system is seen particularly critically. Such information should be limited to a general description of measures implemented to ensure an adequate level of accuracy, robustness and cybersecurity. On the other hand, a claiming of product attributes such as the 'expectable' level of cybersecurity, that are not fully within the sphere of responsibility of the provider of an AI system, is strictly rejected, among other things for reasons of liability law.

Other provisions include the requirement in Article 14 of the draft regulation to design and develop high-risk AI systems in such a way that they 'can be effectively overseen by natural persons'. However, an ongoing and detailed supervision of AI systems by humans is not possible in all cases, as the logic of decisions is not always immediately comprehensible and the speed of automated AI systems is too high in many cases. The reason is that AI systems are used in particular in areas where they are partially or completely superior to human decisions. The provisions of Article 14 should therefore be limited to basic requirements for human oversight. Detailed rules that in practice cannot be implemented realistically should be avoided on the other hand. In addition, the requirements of Article 14 should be clearly limited to the decision-making elements of AI systems. Furthermore, technical systems with which the objectives addressed in Article 14 can also be achieved should be mentioned as equivalent safeguarding mechanisms in the Article.

The requirements for accuracy, robustness and cybersecurity defined in Article 15 of the draft regulation are described generically, so that companies are basically given the necessary flexibility to implement the requirements. However, instead of referring to the indeterminate legal term 'appropriate level' of accuracy, robustness and cybersecurity, compliance with the requirements for the accuracy, robustness and cybersecurity of a high-risk AI systems should be linked to the implementation of 'state of the art' measures that are appropriate to the particular risks and customary in the particular market segment or field of application of the AI system.

Obligations of providers of high-risk AI systems

With regard to the provider obligations specified in Article 16 et seq. it is first of all absolutely necessary that the regulation provides for a clear delineation of roles. In particular, taking into account the complexity of value chains in the area of artificial intelligence (cf. also recital 60), it must be clearly determined when or under which conditions a company is considered a 'provider' of a high-risk AI system.

In the present version, the draft regulation does not adequately cover case constellations in which a provider of 'high-risk AI' purchases technology (e.g. pre-trained data models) from a supplier. In this case, the provider does not automatically possess all the necessary data needed to comply with the requirements (e.g. Article 10) of the regulation. Access to the necessary data would depend solely on the contractual arrangements between the business partners. Therefore, in such case constellations the regulation should also provide for a fair distribution of responsibilities within the supply chain.

At the same time, it should be avoided that several companies within a supply chain are considered as 'providers' of one and the same AI system. This would lead to an unnecessary and costly duplication of obligations.

From the perspective of the German industry, it must also be ensured in general that the obligations from Article 16 et seq. of the draft regulation can actually be fulfilled by the providers in practice. While Article 16 itself refers to obligations set out elsewhere in the legislative proposal, Article 17 of the draft regulation contains the requirement to implement a quality management system to ensure compliance with the European AI Act. We explicitly welcome the proportionality clause in Article 17(2) of the draft regulation, according to which the implementation of the requirements in Article 17 shall be proportionate to the size of the company. According to Article 17(1)(g), the risk management system required under Article 9 of the draft regulation constitutes an element of the quality management system. Analogous to the provisions for credit institutions, companies across all sectors should have the possibility to comply with Article 17 by integrating the required elements and processes into existing quality management systems.

For providers of high-risk AI systems, Article 20(1) of the draft regulation specifies the retention period of logs to be recorded pursuant to Article 12. From BDI's perspective, the retention of log data must be proportionate to the purpose of the respective AI system in order to avoid disproportionate efforts on the part of companies. Article 20(1) of the draft regulation provides for such adequacy. However, the criterion of technical feasibility urgently needs to be added to Article 20(1), as in practice technical restrictions may prevent the retention of log data to the extent and for the period required by the draft regulation. One example is edge computing, where the processing of data is decentralised, i.e. taking place at the level of the individual components of a network (e.g. end devices, sensors or microcontrollers). For technical reasons, in particular due to limited storage capacities, a comprehensive retention of log data is usually not possible in such cases. The envisaged requirements would therefore inhibit innovation in areas where Europe has particular strengths - namely in the area of edge computing and edge AI. Similarly, there is also a need for improvement with regard to the provisions for the retention of logs for users of high-risk AI systems according to Article 29(5) of the draft regulation. This requirement also needs to be designed in such a way that it can realistically be fulfilled in practice.

The information providers of AI have to disclose to supervisory authorities is described in Article 23 of the draft regulation. As trade secrets might be affected at this point, a careful balancing of the information interest of supervisory authorities and the protection needs of companies is necessary in this context, too. In order to take adequate account of these protection needs, supervisory authorities

should not be allowed to request relevant information 'on suspicion'. Instead, in the event of a legitimate request issued by an authority, companies concerned should be given in the first instance the opportunity to provide, at their own discretion, information that allows from their perspective for a response to the request of an authority.

According to Article 24 of the draft regulation, the manufacturer of a product that contains a high-risk AI system shall take 'the responsibility of the compliance of the AI system' and is also, with regard to the AI system, subject to the provider obligations of the AI Act. However, in such cases product manufacturers should be exempted from obligations that can realistically only be fulfilled by the provider of the implemented AI system. This includes, for example, the requirement in Article 16 of the draft regulation (Obligations for providers of high-risk AI systems) to draw-up the technical documentation of a high-risk AI system, since the information required for a technical documentation usually remains (in particular for reasons of protecting trade secrets) with the provider and is not passed on to the product manufacturer. In addition, the provisions of Article 24 of the draft regulation should not result in a requirement to conduct a double certification of AI systems.

Obligations for other market actors

Article 28 of the draft regulation defines case constellations in which a 'distributor, importer, user or [any] other third-party' is considered a provider within the meaning of the European AI Act and accordingly is subject to the provider's obligations set out in Article 16 of the draft regulation. This provision refers to the category of high-risk AI systems. In order to create a level playing field, distributors, importers, users or other third parties that modify an AI system of another category, which has already been placed on the market or put into service, into a high-risk AI system within the meaning of the European AI Act, should also fall under the scope of Article 28 of the draft regulation.

The case constellations covered by Article 28 of the draft regulation include cases in which the mentioned actors 'place on the market or put into service a high-risk AI system under their name or trademark'. In practice, these constellations appear frequently, as companies also license their AI technologies to customers (e.g. SMEs). The provisions envisaged in Article 28 would have the consequence that the licenser would have to grant its licensee comprehensive access to data (e.g. test and training data) necessary to comply with the obligations of providers set out to Article 16 of the draft regulation.

With regard to the obligation to keep automatically generated logs, set forth in Article 29(5) of the draft regulation, the adequacy provision contained in paragraph 5 must be, analogously to Article 20, complemented urgently by the criterion of technical feasibility, as in practice technical restrictions may prevent the retention of log data to the extent and for the period required by the draft regulation (cf. for details our comments on Article 20 of the draft regulation).

Notifiying authorities and notified bodies

The notification of conformity assessment bodies and the framework for notified bodies are specified in Chapter 4 of the draft regulation. As sufficient testing capacities of notified bodies are an essential precondition for a rapid market access of AI systems, policymakers and economic actors must work in time towards the goal that the requirements of the AI Act are consistent with the available testing capacities.

Conformity assessment

With regard to the requirements for high-risk AI systems, Article 40 of the draft regulation establishes a presumption of conformity when harmonised standards are applied. This principle is expressly welcomed. However, the existing standards currently only cover a part of the requirements for high-risk AI systems defined in Chapter 2 of the draft regulation. Since the development of harmonised standards requires a standardisation mandate from the European Commission, the Commission should identify timely and with high priority the specific needs for standardisation in the various areas together with the industry and issue on this basis standardisation mandates before the regulation enters into force. This is because the existence of harmonised standards is an essential precondition for the operationalisation of the requirements of the AI Act by companies.

Article 41 of the draft regulation empowers the Commission in certain cases - e.g. in the absence of relevant harmonised standards - to adopt common specifications by means of implementing acts. These activities should not compete with ongoing standardisation processes. Moreover, the development of harmonised standards should always have priority or be the preferred option compared to common specifications. If the adoption of common specifications in accordance with the procedures set out in Article 41(1) of the draft regulation is actually necessary in justified exceptional cases, the Commission has to ensure that all stakeholder groups concerned are given the opportunity to participate in this process.

The presumption of conformity in Article 42(2) that refers to the requirements on cybersecurity set out in Article 15 of the draft regulation should not apply exclusively to certifications pursuant to regulation (EU) 2019/881. An equivalent presumption of conformity should also apply to other European and international certification schemes, norms and standards that already exist or will be published in the future and also cover the cybersecurity requirements of the European AI Act.

Article 43(4) of the draft regulation provides for an obligation to carry out a new conformity assessment procedure whenever systems classified as high-risk AI are 'substantially modified'. This indeterminate legal term should be specified in order to allow companies to interpret the provision with legal certainty. The extensive empowerments of the European Commission in paragraphs 5 and 6 to amend elements and areas of application of conformity assessment procedures should each be complemented by a provision that requires the comprehensive participation of stakeholders.

Requirements for AI systems of the category 'limited risk'

The German industry supports the objective that natural persons should be able to recognize whether they are interacting with an AI system, unless this is obvious from the circumstances. This is because transparency at this point makes an important contribution to strengthening people's trust in AI. In this context, it is important that the requirements set out in Article 52 of the draft regulation are in line with similar requirements specified in other legal acts, e.g. the requirements for transparency of digital services in the DSA.

Measures to promote innovation

The BDI expressly welcomes the approach of the Commission to complement the regulatory requirements of the AI Act with measures to promote innovation. Besides an innovation-friendly legal framework for the use of AI in the EU, these measures are another essential precondition for developing Europe into a leading global location for artificial intelligence.

In this context, the AI regulatory sandboxes envisaged by the Commission in Article 53 of the draft regulation are a key instrument for promoting innovation from which numerous companies will benefit. In order to ensure that the instrument is also accessible to small and medium-sized enterprises (SMEs) and start-ups in a low-threshold way, the support measures for SMEs provided for in Article 55(1)(a) of the draft regulation are expressly welcomed, too.

The legal basis for the establishment of AI regulatory sandboxes should already be clearly stated in Articles 53 and 54 of the draft regulation. Moreover, the measures should be in line with the Council's activities in this area and include flexible experimentation clauses. If technical details are to be defined under the procedure set out in Article 53(6) of the draft regulation, companies and research institutions should be fully involved in this process.

Governance

In order to counteract market fragmentation within the European Union and to provide companies with the necessary legal certainty, it is crucial in the process of implementing the governance structure provided for in Title VI of the draft regulation to ensure a uniform legal application of the provisions of the AI Act within the EU. Public authorities must also be equipped with adequate resources and the necessary technical expertise to be able to adequately fulfil the tasks envisaged by the regulation. Furthermore, from an industry perspective, it is essential to ensure that the competent national authorities take a holistic view on AI, i.e. that they - in addition to the monitoring of the compliance with regulatory requirements - also actively implement and further develop the innovation-promoting instruments provided for in the regulation.

The European Artificial Intelligence Board provided for in Article 56 of the draft regulation will also play an important role in practice. Since the working results (guidelines etc.) of comparable committees in other areas of law have a high binding effect in practice, a comprehensive stakeholder participation in the work of the European Artificial Intelligence Board is of high importance. The optional formulation concerning stakeholder participation in Article 57(4) of the draft regulation should therefore be replaced by a binding requirement to consult interested third parties on a regular basis.

With regard to the 'national competent authorities' established in Article 59 of the draft regulation, the German industry believes that there is still the need for a more precise clarification of the relationship to supervisory authorities established by other EU legal acts, in particular the NLF acts listed in Annex II of the draft regulation. Such a clarification is of high importance in order to avoid overlapping competences, associated interface problems and duplicated efforts for companies.

Post-market monitoring, information sharing and market surveillance

Post-market monitoring of high-risk AI systems

According to the provisions of Article 61 of the draft regulation, providers of high-risk AI systems shall set up a system for monitoring the AI system after it has been placed on the market in order to continuously analyse the compliance as well as the 'performance' (defined in Article 3(18) of the draft regulation as the 'ability of an AI system to achieve its intended purpose') of the AI system.

From BDI's point of view, this extensive requirement for providers of high-risk AI systems can hardly be implemented in practice, as the preconditions listed in Article 61(2) of the draft regulation, in

particular the availability of the data necessary to comply with the requirement, are often not given. This applies, for example, to frequently existing case constellations in which the operational data of an AI system remains, for reasons of confidentiality, entirely with the user.

The same applies when a product manufacturer places a high-risk AI system in one of its products on the market or puts it into operation in accordance with Article 24 of the draft regulation. In this case, only the product manufacturer usually receives the field data of its end product, but not the provider of the high-risk AI system. Against this background, the provisions of Article 61 of the draft regulation should be limited to requirements that can typically be fulfilled by a provider of high-risk AI systems.

Incident Reporting

Article 62 of the draft regulation provides for a reporting obligation for providers of high-risk AI systems in the event of 'any serious incident or any malfunctioning'. However, it is not clear from the article and the explaining chapters of the draft regulation (e.g. Chapter 5.1. of the explanatory memorandum) how the supervisory authorities will deal with relevant incident reports and what follow-up process is envisaged in this context. From the industry's point of view, it is therefore necessary in the further legislative process to significantly increase transparency at this point.

Market Surveillance

Article 64 of the draft regulation, which regulates the access of authorities to data and documentation of AI systems, should be complemented by the requirement that the mentioned authorities entitled to receive information have to justify their requests for information to the market actors. In particular this should ensure that no more sensitive data (e.g. information of the category trade secrets) is requested than is actually needed.

From the perspective of the German industry, the right of market surveillance authorities set out in Article 67 of the draft regulation to require under certain preconditions amendments of AI systems that comply with the requirements of the AI Act, is very extensive. In particular the envisaged option to require a withdrawal of an AI system from the market would lead to massive legal uncertainties on the side of companies.

In order to ensure a uniform application and interpretation of the provisions of the AI Act throughout Europe, it is also necessary from an industry perspective to ensure a uniform and coordinated approach by the competent authorities when exercising market surveillance functions. This also applies to the designation of national supervisory authorities in the single member states as regulated in Article 59.

Confidentiality provisions and sanctions regime

Confidential treatment of information provided by market actors

The confidential treatment of data provided to authorities and notified bodies by companies in order to meet the requirements of the AI Act is of central importance for the protection of sensitive data and trade secrets. However, the relevant provisions in the draft regulation, the provisions set out in Article 70, are rather unspecific, as Article 70 of the draft regulation, apart from the definition of general protection goals (e.g. the protection of 'intellectual property rights' in Article 70(1)(a)), does not specify any technical and organisational requirements that receiving authorities and notified bodies must comply

with in this context. From the perspective of the industry, the permission clause contained in Article 70(4) of the draft regulation for the exchange of information with third countries is also viewed critically. The requirements for the data exchange at this point are also formulated very unspecifically (e.g. the criterion '*where necessary*' in Article 70(4) of the draft regulation). From our point of view, there seems to be no adequate protection of information in this context.

Sanctions

According to Article 71(3) of the draft regulation, fines of 6 percent of a company's worldwide annual turnover may be imposed in the event of non-compliance with the prohibition of the practices referred to in Article 5 and in the event of non-compliance pursuant to Article 10 of the draft regulation, and up to 4 percent of the total worldwide annual turnover in the event of non-compliance with other require-ments and obligations of the draft regulation. Since 4 percent of the annual turnover is the highest possible penalty according to Article 83(5) GDPR, the sanction rules of the AI Regulation again exceed this sanction framework. The BDI sees no justification for adopting fines in an amount that is at best known from competition law in the present case for a completely new innovation. The preliminary effect of the threat of sanctions must under no circumstances become a brake on innovation for the devel-opment of AI in Europe. This is because the complexity of the requirements, combined with the high threat of sanctions, could also become a stumbling block for smaller and medium-sized suppliers. The level of fines should therefore be adjusted. Otherwise, it is to be feared that the trend towards ever stricter regulation combined with strict enforcement instruments will stifle innovation and prove detri-mental to the internal market. Particularly in view of the high threat of sanctions, the regulation must be legally secure, and the requirements must be sufficiently specific. Furthermore, it is imperative to guarantee a uniform interpretation and application of the regulations throughout the Union in order to avoid a fragmentation of the internal market through a different application of the law. In this sense, it makes sense for the European Data Protection Supervisor to take over the supervision of the national authorities (cf. Article 72 of the draft regulation). The system (e.g. the treatment of groups/affiliated companies) based on which fines are set in practice should also be disclosed. The same applies to the proposed sanction levels below the maximum sanction level listed in the draft regulation.

Authorisations for delegated and implementing acts

The draft regulation of the European Commission contains numerous authorisations for the adoption of delegated and implementing acts. Both the number and the regulatory content to be addressed by these legal acts are not appropriate from an industry perspective. Delegated acts may only relate to supplementing or amending 'non-essential' provisions in EU basic acts (Article 290(1) TFEU). All cen-tral requirements of the regulation must thus be defined in the legal act itself, so that the principles of the rule of law and certainty are respected and may not be introduced or amended later by delegated acts.[2] This applies particularly to the definition of AI.

Final provisions

According to Article 83(2) of the draft regulation, the provisions of the AI Act shall also apply to high-risk AI systems that were placed on the market or put into operation prior to the application of the

---

[2] Cf. judgment of the Court of Justice of the European Union of 13 December 2018 (T339/16, T352/16 and T391/16); paras 116-120.

regulation if 'from that date, those systems are subject to significant changes in their design or intended purpose.' The BDI rejects a subsequent inclusion of already existing AI systems, as this would cause disproportionately high subsequent adaptation efforts for the providers of concerned AI systems.

Addendum: Measures to promote a European AI ecosystem (Coordinated Plan-Review)

The BDI expressly welcomes the fact that the planned regulation of the use of certain categories of AI systems in the EU will be complemented by further measures to promote the competitiveness of European companies in the field of the key technology AI.

The 'Coordinated Plan on Artificial Intelligence 2021 Review' presented by the European Commission together with the regulatory proposal on 21 April 2021 is based on the 'Coordinated Plan on Artificial Intelligence' published by the Commission in 2018 and illustrates how artificial intelligence can be better established in society and its use promoted more quickly. To this end, it focuses on EU initiatives, but also on the cooperation with the member states and the implementation of AI strategies in the single countries.

The BDI welcomes the fact that the Coordinated Plan also includes numerous initiatives and proposals for the promotion of SMEs. In particular, the BDI welcomes the ambitious goal of mobilising private and public investments in AI of up to EUR 20 billion per year over the course of this decade.

According to the Commission's will, a special focus shall be placed on the harmonisation of AI strategies in the member states. The Commission should set the right framework conditions for this, because a uniform and coherent approach throughout Europe is particularly important when it comes to digitalisation. In all measures, it is also important to include the experience of companies in the process at an early stage. In the view of the BDI, it would also make sense in this context to subject the European and national strategies and their implementation measures to a regular effectiveness check in order to be able to better evaluate the success of the individual measures. In addition, legal hurdles for companies should be further reduced. This applies, for example, to obstacles under competition law, so that companies can engage in data and AI partnerships with legal certainty.

The shortage of skilled workers also poses major challenges for the German industry. The BDI therefore supports an advanced training and education initiative in the field of AI. Lifelong learning and the establishment of a training culture in companies are important cornerstones for counteracting the shortage of skilled workers in the long term. Therefore, the introduction of the Commission's *Digital Education Action Plan* is a good first step towards training more skilled workers in key technologies in the long term.

Imprint

Editors

Oliver Klein
Senior Manager Digitalisation and Innovation
T: +49 30 2028-1502
o.klein@bdi.eu

Stefanie Ellen Stündel
Senior Manager Digitalisation and Innovation
T: +3227921015
s.stuendel@bdi.eu