BUSINESSEUROPE

POSITION PAPER

The Artificial Intelligence Act (AI Act)

KEY MESSAGES

1. **We welcome the Commission's risk-based approach outlined in the AI Act and share the ambition to ensure that AI is safe, lawful and in line with EU fundamental rights.**
2. **We recommend carefully addressing all potentially unwanted consequences and administrative burden for industry which could discourage investment in the development of AI systems and hurt EU competitiveness in the long term.**
3. **The proposed definition of "AI systems" is too broad. We recommend using the definition proposed by the High-Level Expert Group on AI, focusing on AI systems that display intelligent behaviour and take actions with some degree of autonomy.**
4. **The proposed classification rules for high-risk AI should be refined to ensure consistency with sectoral legislation in Annex II. The AIA should only regulate high-risk AI applications in areas where a clear regulatory gap has been demonstrated.**
5. **We agree that some AI use-cases in the areas listed in Annex III will require to undergo specific requirements, but we recommend adjusting the scope of application based on objective and clear criteria and to have a differentiation between applications of AI according to the actual risk they pose to fundamental rights and/or health and safety.**
6. **Responsibilities of different actors in the AI value chain must be reassessed and clarified to ensure obligations are allocated to the actors that can ensure compliance.**
7. **We support measures that can promote trustworthy AI in Chapter 2. However, we recommend reviewing the compliance framework to ensure 1) a proportionate risk-burden balance, 2) clear allocation of responsibilities, and 3) sufficient flexibility to adapt to new knowledge and evidence.**
8. **We welcome the possibility to conduct internal-control checks and the use of consensus-based harmonised standards to demonstrate compliance. We recommend aligning with existing and ongoing international standardisation activities and certifications issued under a EU cybersecurity scheme.**
9. **We recommend safeguarding the experimental nature of sandboxes schemes and converting their voluntary nature into an obligation, with well-established criteria to ensure an effective access to businesses, particularly SMEs.**

BUSINESSEUROPE a.i.s.b.l.
AVENUE DE CORTENBERGH 168 – BE 1000 BRUSSELS – BELGIUM
TEL +32 (0)2 237 65 11 – FAX +32 (0)2 231 14 45 – E-MAIL main@businesseurope.eu
WWW.BUSINESSEUROPE.EU – Follow us on Twitter @BUSINESSEUROPE
EU Transparency register 3978240953-79

COMMENTS

CONTEXT

AI can strategically support Europe and help us answer many societal challenges that we face in almost every area. The potential for Europe to derive these benefits will rely on the abilities for companies to research, test, have a skilled workforce, a vibrant data economy, appropriate infrastructure, and a beneficial framework to exist within.

As a collection of technologies and not a policy area itself, AI is already regulated in several policy areas at European (e.g., the General Data Protection Regulation (GDPR), the Product Liability Directive (PLD), the General Product Safety Directive e (GPSD); discrimination/equality legislation) and national level through ancillary law. A range of potential risks linked to the use of AI technologies are essentially addressed in Union product safety legislation, which ensures that products placed on the single market meet high health and safety requirements and that such products can circulate freely. While these do not explicitly address all new challenges and risks of emerging technologies, they remain a very robust framework and are generally fit for purpose. Therefore, it is necessary to articulate the proposed Regulation with existing and upcoming data protection, product liability, and product safety European legislation to ensure consistency. In addition, as AI comes to be increasingly deployed, policy makers must consider the consequences of not using it. Therefore, while it is vital to minimise mistakes as far as possible, the EU must factor the cost of not using AI into policy debates.

TITLE I: GENERAL PROVISIONS

We concur that the focus should be on applications of AI systems which pose an actual high risk of causing damage to the health and safety of humans or have a detrimental impact on European fundamental rights and values, based on objective, clear and unambiguous criteria. We believe that clarifications of the definitions and adjustments to the scope will be crucial to ensure the new rules are targeted towards high-risk AI systems, in a proportionate and legally clear manner and that they lead to the desired policy outcomes. More specifically, we believe that the current definition of AI systems, the criteria for determining prohibited practices and the classification of high-risk AI systems, should be clarified to focus on where most widespread and significant societal damage is likely to arise.

Extraterritoriality (Art. 2)

We support an extraterritorial legal regime to maximise the safety of EU citizens and to ensure a level-playing field between European and non-European AI providers and users, from the moment they offer AI solutions in Union. However, BusinessEurope believes that the proposed scope of AI providers and users outside the EU should be

clarified in order to ensure legal certainty for companies operating internationally. For example, Recital 11 states that '*certain AI systems should fall within the scope of this Regulation even when they are neither placed on the market, nor put into service, nor used in the Union'*. Further clarity on the extraterritorial applicability of the AIA and on future collaboration with EU international partners regarding the global governance of AI will be key. Given that certain AI systems may fall within the scope of this Regulation even if they are not used in the European Union, there should be a clear framework relating to the applicability of the Regulation.

Definitions (Art.3)

We agree that the definition of AI needs to provide for flexibility to accommodate future technological developments. However, we believe that the definition proposed by the Commission of '*Artificial Intelligence System*' in Art. 3(1) as well as the list of techniques listed in Annex I is too broad. As currently drafted, the definition of AI would include most contemporary software and applications that use pure statistical and knowledge-based approaches for conventional data analysis that have little impact on individuals, such as AI methods for internal modelling needs (e.g., Asset and Liability Management models for the banking sector), for corporate scoring or for industrial issues. To avoid legal uncertainties for market participants and to ensure a specific and clearly defined scope of application of the Regulation, we recommend focusing on intelligent AI systems that can take actual decisions with a certain degree of autonomy. We therefore recommend using the definition suggested by the High-Level Expert Group on AI[1].

Furthermore, use of the same definitions throughout the legislative framework is a must to ensure consistency between the horizontal New Legislative Framework (NLF) acts and complementary legislation. BusinessEurope is concerned that the proposed AI Regulation explicitly modifies key concepts and definitions of the NLF for products (e.g., concepts of '*putting into service*'; '*provider*', etc.) which risks causing interpretational issues for EU manufacturers that need to comply with the AIA and sector-specific legislation. For example, the definition of "***safety component"*** under Art.3 (14) should be further clarified and consistent with the relevant EU harmonisation legislation in Annex II. It would also be helpful to have guidance on the legal standard or process to determine '*reasonably foreseeable misuse*' as defined in Art. 3(3). As currently worded, it would cause significant uncertainty on the development and deployment of AI systems, that are not intended to be used in a certain manner.

Amendments to Annex I (Art. 4)

Any adjustments to the legal definition that may become necessary after the Regulation enters into force should not be made by means of a delegated act, as provided for in Art. 4 of the draft Regulation. Delegated acts may only relate to supplementing or amending

[1] A definition of AI: Main capabilities and scientific disciplines High-Level Expert Group on Artificial Intelligence, AI HLEG (2019)

'non-essential' provisions in EU basic acts (Art. 290(1) TFEU). Since the definition of AI is an essential provision of the Regulation, adjustments should only be made by way of an ordinary legislative procedure, so that the principles of the rule of law and certainty are upheld and may not be introduced or modified later by delegated acts (with full inclusion of stakeholders in the legislative making process).

TITLE 2: PROHIBITED ARTIFICIAL INTELLIGENCES PRACTICES

Prohibited Practices (Art. 5)

We understand the Commission's ambition to limit the use of certain very high-risk applications of AI that represent a clear threat to the health and safety of humans or EU fundamental values and see it as a key provision to enhance trustworthy AI. However, before determining whether such prohibited practices are acceptable, further clarification is needed as to how Art. 5(a) has been drafted in relation to systems '*deploying subliminal techniques'* and references *to 'psychological harm*'. To support legal certainty, we recommend further specifying prohibited practices, i.e., to clarify, for instance, what is meant by '*deploying subliminal techniques', 'detrimental or unfavourable treatment' and 'psychological harm'* to prevent wrong classifications of High-risk AI systems (e.g., *Remote* biometric identification systems).

TITLE 3: HIGH RISKS AI SYSTEMS

CHAPTER 1: CLASSIFICATION OF AI SYSTEMS AS HIGH RISKS

Classification rules for high-risk AI systems (Art.6)

BusinessEurope welcomes the risk-based approach outlined in the AI Act. This is a pragmatic start to achieve trust and excellence while enabling early AI development to flourish, as we highlighted in our earlier comments to the White Paper on AI.[2] However, the current classification of high-risk AI applications in Art. 6 will lead to legal uncertainty and hamper the uptake of innovative and beneficial AI applications, including AI applications in the industrial domains and AI solutions in the field of employment.

a) Safety components of regulated products (Annex II)

Annex II provides a list of EU harmonisation legislation under which products and/or integrated AI '*safety components'* of products undergoing third-party conformity would be classified as high-risk. BusinessEurope believes that EU harmonisation legislation in Annex II already provides for comprehensive safety requirement, including for risks linked to certain applications of AI in the industrial domains. As currently drafted, the classification under Art. 6 would force EU manufacturers to align with (conflicting)

[2] BusinessEurope's position paper: AI: A European Approach to Excellence and Trust

requirements and definitions from both sector-based regulation and the new AI framework. The AI Regulation should only regulate high-risk AI applications in areas where a clear regulatory gap has been demonstrated. This should be done following a risk-based approach, focusing on whether the intended use of AI in the sector involves significant risk, rather than the entire sectors. This is crucial to ensure provisions are targeted, legal clarity is supported and AI development is encouraged. In addition, it should be ensured that the proposed classification under Art. 6 does not lead to the promotion of mandatory third-party conformity assessment, which would undermine the development of innovative applications of AI that grant EU companies a competitive edge globally.

b) Stand-alone high-risk AI applications (Annex III)

We concur that some stand-alone AI use-cases in the areas listed in Annex III will require to undergo specific requirements, but our main concerns relate to the very broad definition of these areas. Deeming any AI system used in the areas listed in Annex III high-risk would disproportionately overregulate this technology and bring a high-level of legal uncertainty to businesses attempting to determine whether they are covered. Whether an application of AI should be considered of risk will depend on the specific context (e.g., whether it includes risk mitigation by effective technical or operational countermeasures) and on situations where the AI system takes the final decisions – a blanket approach is not appropriate and not consistent with a risk-based approach. We therefore recommend limiting the scope of application based on objective and clear criteria and differentiating between applications of AI according to the actual risk (and harm) they pose to fundamental rights and/or health and safety.

For example, the very broad definition of AI used in '*employement, self-employement or workplace context*' would notably slow down AI applications in Human Resources, which can effectively and safely increase productivity of enterprises and well-being of the workforce at the same time and use smart and cognitive functionality to boost our own abilities and skills. As previously addressed, we recommend differentiating between applications according to risk they pose to fundamental rights. Furthermore, the European Social Partners' Autonomous Agreement on digitalisation already sets out some direction and principles of how and under which circumstances AI is introduced in the world of work.[3] In the same vein, the broad definition of '*AI systems used to evaluate the credit score or creditworthiness of natural persons'* would slow down the process for accessing small loans for individuals and small businesses and undermine the competition between large providers and smaller entities providing financial services as auxiliary features.

Amendments to Annex III (Art.7)

[3] European social partners framework agreement on digitalisation

We welcome and support the ambition to create a legal framework that is future-proof and resilient to disruption. However, we fear that the dynamic adaption of the scope will cause great unpredictability for the market and risks undermining AI rollout in the future. We are mostly concerned about the vague criteria listed in Art. 7, which empowers the Commission to update the list in Annex III by adding high-risk AI systems under certain conditions, notably in cases of *'adverse impact on fundamental rights*' (Art. 7(b)). To support legal certainty and market predictability, we welcome further clarity on specific triggers or conditions that would enable the European Commission to update the list of high-risk AI systems, and introducing explicit provisions for Member States and industry involvement in any future process for updating the list (e.g., by renewing the mandate of the High-Level Expert Group on AI).

CHAPTER 2: REQUIREMENTS FOR HIGH-RISK AI SYSTEMS

BusinessEurope welcomes the possibility to demonstrate compliance through internal control checks. This is crucial given the early phase of the regulatory intervention and the lack of expertise for auditing certain AI systems.

Any market access conditions (requirements) set for high-risk AI systems should recognise that AI is evolving rapidly and that many AI systems continue learning after being placed on the market. Several of the proposed requirements in Chapter 2 are still topics of active research and concrete approaches for achieving these requirements might not be available depending on the specific AI technique. BusinessEurope believes that it is important to adjust the requirements to ensure 1) a proportionate risk-burden balance, 2) a clear identification and allocation of responsibilities along the AI value chain and for each stage of the development life cycle of AI systems, and 3) sufficient flexibility to adapt to new knowledge and evidence as well as to different organisational structures across AI value chains. As currently drafted, the proposed compliance framework will create complex bureaucracy and unbearable costs for many businesses, which may severely impact the uptake of AI in Europe. We recommend introducing additional support and flexibility to ensure their easy adoption by SMEs and small-scale providers – which is key to ensure a level playing field. In addition, we believe that the mandatory requirements on high-risk AI systems should be eased if risks are sufficiently and properly eliminated or reduced with built-in 'fail safe' designs in high-risk AI systems and operational countermeasures.

Risk management system (Art. 9)

BusinessEurope welcomes the Commission's intention to provide guidance on how to implement risk management systems for high-risk AI systems in Art. 9. However, we believe that EU harmonisation legislation should align with the core new legislative framework (NLF) principles[4], meaning that it should focus on essential requirements and

[4] Aims to improve the internal market for goods by improving market surveillance and boosting the quality of conformity assessments.

leave their technical realisation to product-specific and state-of-the-art voluntary standards developed by stakeholders. We therefore recommend focusing on the desired outcome of risk management and assessment systems, and explicitly leaving to industries the task of designing their system and adapt them to their internal operations and structure, notably through state-of-the-art standards. In addition, Art. 9 offers no guidance on what specific risks need to be considered by the risk management system. While several recitals (e.g., Recitals 27, 43) indicate that the goal of the Regulation is to mitigate risks to *'health, safety and fundamental rights,'* Art. 9 itself does not specify the types of risks providers should consider when assessing and taking steps to mitigate risks. Further clarity is also needed regarding the interplay between the risk-management system and other requirements set in chapter 2.

Credit institutions are allowed under Art. 9(9) of the draft Regulation to integrate the required risk management system into risk management processes prescribed by the sector-specific legislation. The possibility to integrate the risk management for systems classified as high-risk AI into existing risk management processes should be granted to all affected sectors to avoid unnecessary bureaucracy.

Data and data governance (Art. 10)

We welcome measures in Art. 10 for enhancing the quality training of data. As previously addressed, we recommend focusing on the general output of the AI system and its compliance with legal requirements, rather than laying out the specifics of their technical realisation. This would help avoid inconsistencies with front-line practices by industry experts. For example, as currently phrased, Art. 10(3) mandates that '*training, validation and testing data sets shall be relevant, representative,* ***free of errors and complete*****',** which would be unworkable in practice, as it fails to take into consideration the degree of variance in data sets and would prevent the use of real-life data. Chasing 'zero-risk' circumstances is unrealistic and will not foster excellence in European AI, especially in view of the higher penalty in the event of non-compliance. In addition, it should be considered that often AI systems will be built using data sets provided by third parties, including those open sourced. In this regard, assessing compliance with Art. 10 may rise some questions such as how much reliance can be placed on representations made by the creators of the data sets.

With regards to bias monitoring, a workable solution could be achieved by abiding by state-of-the-art security and privacy-preserving standards with regards to data management. For example, with regards to the quality of data, reference to existing standards such as ISO/IEC 25024 '*Measurement of data quality*', ISO/IEC 25012 '*Data quality model*' and ISO/IEC 24745 '*Performance testing of biometric template protection schemes'* could prove useful.

Technical documentation (Art. 11)

BusinessEurope believes that technical documentation requirements should be appropriate to the use case. Data quality and data provenance vary, and thorough

documentation is not always possible or necessary to mitigate risks. In addition, technical specifications stipulated prior to market entry might not be relevant at later stages throughout the AI's lifecycle since operational environments of AI applications are not constant and vary greatly based on context. Moreover, the contents of technical documentation specified in Annex IV are very far-reaching. For example, the detailed description of the '*elements of the AI system'* required under item 2b), which includes algorithms, may constitute trade secret. Therefore, the requirements must be carefully weighed against the need to protect confidential information.

Record keeping (Art. 12)

We agree that keeping of records, documentation and, where relevant, data sets need to be retained, as indicated in Art. 12. However, for specific and identified high risk uses cases only and for a limited time to ensure effective enforcement of this legislation and to avoid burdensome and costly data storage requirements. For example, datasets used to generate a model collected in the early stages will not be pertinent when the damage occurs, since it will have been consequently altered, modified, or even removed in the meantime. Accordingly, the storage period and requirements should be determined based on business needs, business capabilities, and informational value. However, if a time period is stipulated, and in conformity with established auditing standards and existing sectoral practices, we propose that the retention periods should not exceed at maximum 10 (ten) fiscal years.

Transparency and provision of information to the users (Art. 13)

BusinessEurope doubts whether very detailed and technical information (e.g., regarding the test data used) offers practical information value for the users of the corresponding AI system. To keep the information for use manageable and comprehensible in practice, the catalog of requirements contained in Art. 13 (3) of the draft Regulation should be limited to essential and intelligible information (e.g., special risks in the event of non-intended use of the AI system). Indeed, most factors will depend in part on the quality of data input by users, the circumstances of its use, and the ways in which users operate the system. Therefore, Art. 13 should limit the provider's obligations to providing users with adequate and complete information to help them test the accuracy of the system in a deployment setting.

Human oversight (Art. 14)

We agree that the objective of trustworthy, human-centric AI can only be achieved by ensuring appropriate level of human oversight. However, the complex instructions to users and strict requirements to enable the user to '*fully understand the capabilities*' of the systems more than necessary seem disproportionate and overly ambitious, and therefore not very useful to the user. Selecting the most prudent combination through determining the form and stage of human oversight will rely on a holistic assessment of how best to ensure that an acceptable output is made. This will depend on the intended

use and effects that it could have on safety and performance of the task at hand. An optimum level of safety based on understandable trade-offs should be reached that is acceptable for society and in the work context. A more workable requirement would be to require users to have '*an appropriate understanding of the capacities and limitations*' of the systems.

In addition, certain AI controlled machine have proven that they can provide higher safety and lower accident rates with built-in risk prevention measures compared to having human oversight. Human oversight requirements will also rely on qualified workforce, of which there is a notable lack in the European Union.[5]

Accuracy, robustness, and Cybersecurity (Art. 15)

We agree that trust for AI will also rely on ex-ante consideration of the risks they may generate. However, determining the entire potential of the AI's lifecycle ex-ante doesn't reflect AI which learns continuously. Many AI systems placed on the market learn from the end user, and most often the influence shifts from the business considering risks at the ex-ante phase to the end-user or even operator. Therefore, we recommend reviewing requirements in Art. 15 (1) to further consider the evolving nature of AI and the shift in influence. Compliance with such requirements should be linked to the implementation of measures in accordance with the 'state of the art' (appropriate to the risks and in accordance with the respective market segment or field of application). Furthermore, BusinessEurope would recommend addressing Cybersecurity risks separately to avoid a patchwork of different cybersecurity requirements across EU legislation. For this reason and in accordance with Art. 42, the compliance for High-risk AI systems that have been certified or for which a statement of conformity has been issued under a cybersecurity scheme pursuant to Regulation (EU) 2019/881 of the European Parliament and of the Council shall be assumed.

CHAPTER 3: OBLIGATIONS FOR PROVIDERS AND USERS

Obligations of providers of high-risk AI systems (Art. 16)

We suggest adjusting and clarifying the balance of responsibilities between various actors in the AI value chain, particularly for general purpose Application Programming Interface (APIs) and open-source AI models. As opposed to the legislation based on the New Legislative Framework (NLF) for products, obligations placed on 'providers' under Art. 16 appear to extend beyond the placing on the market throughout the entire lifecycle of the AI system. This is challenging for providers that do not exercise control over the products/AI systems throughout their lifecycle, as well as companies providing general purpose APIs and open-source systems that are not specifically intended for high-risk AI systems but are nevertheless subsequently used by third parties in a manner that could

[5] https://www.bruegel.org/2020/08/europe-has-an-artificial-intelligence-skills-shortage/

be considered high risk and in scope for compliance (e.g., open deep fake detection API that is used by law enforcement). We recommend that obligations to comply with mandatory requirements, including those set in Chapter 2 of the draft Regulation, should lie with the legal or natural person building on the AI system that actually controls the purpose and use of the AI system, and where realistically feasible.

Quality Management systems (Art. 17)

The current duplication of work envisaged by ensuring a robust risk management system (as required in Art. 9) in addition to a quality management system (as stipulated in Art. 17) will add excessive costs to the development of AI applications. Warranting quality and its proper management is both overtly and tacitly assumed within the admit of Art. 9 and it is the risk management system. We therefore propose that issues of quality management are foreseeably included within risk management systems. Analogous to the provisions for credit institutions, it should also be possible for all companies across all sectors to implement the required elements by integrating corresponding processes and measures into existing quality management systems.

Automatically generated logs (Art. 20)

Control of the logs will vary between the users and providers, depending on the type of systems that is used (e.g., users are in control of the logs in most typical cloud systems). Furthermore, for certain systems it may not be practically possible to record all the data generated by the system. This is the case for edge computing, where data processing is decentralised. Therefore, we recommend clarifying this provision to take into account technical feasability and specificities of the system.

Cooperation with competent authorities (Art. 23)

The information to be disclosed by AI providers to supervisory authorities is described in Art. 23 of the draft regulation. Since business' secrets may be affected, a thorough weighing of the supervisory authorities' interest in information with the companies' need for protection is also required. In order to take appropriate account of these protection needs, it should not be possible for the supervisory authorities to request the relevant information 'on suspicion'. Instead, in the event of a justified request by the authorities, the companies concerned should be given the opportunity to provide the information that they believe will enable them to respond to the authorities' interest in information.

Obligations of product manufacturers (Art. 24)

According to Art. 24 of the draft regulation, the manufacturer of a product in which a high-risk AI system is installed "*takes the responsibility of the compliance of the AI system with this Regulation*". In these cases, however, product manufacturers should be exempted from obligations that can realistically only be fulfilled by the provider of the installed AI system. This includes, for example, the requirement to prepare technical

documentation as described in Art. 16 of the draft regulation, since the information required usually remains with the provider and is not passed on to the product manufacturer.

Obligations of distributors, importers, users or any other third-party (Art. 28)

We welcome the ambition to clarify the allocation of responsibilities in the AI value chain in specific circumstances under Art. 28. However, we believe that further clarification is needed to fully reflect the realities of complex AI value chains and distribution. Responsibilities of different actors must be clarified to ensure that obligations are allocated to the actors that can ensure compliance. The methodology to shift responsibility from providers to other parties should be clarified, notably for general purpose tools and APIs that users train with their own data and develop into an AI system for a high-risk intended use. Furthermore, and keeping in line with NLF principles, the regulation should leave operators in the AI value chain freedom to allocate responsibilities through contractual obligations.

CHAPTER 4: NOTIFYING AUTHORITIES AND NOTIFIED BODIES

BusinessEurope believes that sufficient testing capacities represent a central prerequisite for rapid market access of AI systems. Therefore, policy makers and industry must work at an early stage to ensure that the requirements of the AIA are in line with the available testing capacities.

CHAPTER 5: STANDARDS, CONFORMITY ASSESSMENT, CERTIFICATES, REGISTRATION

Harmonised standards (Art. 40)

The existence of harmonised standards is an essential prerequisite to operationalise the requirements of the AIA. The Commission should, timely before the entry into force of the Regulation and with high priority, identify together with industry the concrete need for standardisation in the different areas. While the Commission has a legitimate role in requesting the development of harmonised standards and validating the outcomes, its ambition specify the content, form, and timeline of these deliverables in detail and to examine harmonised standards in a legalistic manner should not result in either detailed requirements regarding the content of the standard or in disproportionate verification schemes that would cause significant delay in listing in the Official Journal. In addition, any standardisation activity at European level must align with existing and ongoing international AI standardisation activities.[6]

Common specifications (Art. 41)

[6] https://www.businesseurope.eu/sites/buseur/files/media/position_papers/internal_market/2021-08-09_be_comments_standardisation_strategy_roadmap.pdf

Art. 41 empowers the European Commission to adopt common specifications, by the means of implementing acts, in respect of the requirements set out in Chapter 2. We strongly recommend prioritising the well-established New Legislative Framework (NLF) route of the consensus-based harmonised standards as well as international standards over technical specifications in implementing acts. Such an alternative approach would only be acceptable when used exceptionally and under strict and clear criteria, in reference to topics for which standardisation is not appropriate. In the exceptional case the common specifications are adopted, all relevant stakeholders must be consulted and involved in the development of such common specifications.

Conformity Assessment (Art. 43)

We welcome the conformity assessment procedure based on internal control referred to in Art. 43. However, as opposed to a well-established conformity assessment infrastructure for products, the relevant expertise for auditing standalone AI systems is just about to be accumulated by industry experts. In addition, existing competent authorities might also face difficulties in auditing the compliance of certain AI systems with the existing legislation due to the specific technological features of AI. To ensure effective compliance, we recommend further flexibility to take into account the lack of actual expertise and infrastructure in the overall compliance assessment framework for AI, to avoid disparities in enforcement across the single market.

As regards the concept of '*substantial modification*' that is referred to in Art. 43 (4), under which a new conformity assessment is required, we would welcome more clarity and a more legally certain definition, based on robust criteria, since most AI systems continue to learn after being placed on the market or put into service.

CE marking of conformity (Art. 49)

We support the need and proposition of creating CE markings of conformity. However, the language of Art. 49 (1) is based on traditional product safety requirements. We propose adapting the CE marking to the AI technology more specifically and its digital nature.

Registration (Art. 51)

BusinessEurope questions the need for an obligation to register high-risk AI systems as provided in Art. 51 and Art.60. Such a registration obligation is neither an element of conformity assessment under the NLF nor is it necessary or proportionate, considering the information that must be provided together with the registration according to Annex VIII. In addition, such data base would provide a target for cyberterrorism. Nevertheless, where registration of AI systems is considered essential and when they provide real added-value information to consumers/users, we encourage the cooperation of Member States according to Art. 60 as well as the use of the Business Registries according to the Directive 2012/17/EU.

TITLE IV: TRANSPARENCY OBLIGATIONS FOR CERTAIN AI SYSTEMS

Transparency obligations for certain AI systems (Art. 52)

Several businesses are already engaged in the positive practice of providing transparency for certain AI systems that are referred to in Art. 52. In general, we recommend that policy-makers ensure coherence and consistency with other relevant legal acts, notably the Digital Services Act Proposal (e.g., How transparency obligations apply in the context of digital services - see our position on the DSA here).Specifically, it would also be beneficial to clarify the scope of Art. 52 in relation to '*AI interacting with natural persons*' as how widely should it be interpreted given the fact that AI is integrated in many user-facing systems, from providing directions, recommendations, etc.

TITLE V: INNOVATION

BusinessEurope welcomes the Commission's ambition to support a thriving and innovative AI ecosystem in Europe. The aim of achieving trust in AI through policy needs to be achieved with the goal of enabling its excellence in Europe in mind. To this end, we urge the regulators to carefully address all potentially unwanted consequences and administrative burden for industry, that could discourage investment in the development of AI systems in Europe and hurt EU competitiveness in the long term. Particular attention should be given to SMEs and small-scall providers.

AI regulatory sandboxes (Art.53)

AI regulatory sandboxes can greatly improve framework conditions for innovative businesses in Europe, and by that enhance Europe's competitiveness in AI. For the society, regulatory sandboxes for AI mean faster access to European innovations that improve the quality of life and solve some of the most urgent societal problems, without compromising on important European values such as consumer protection and privacy, while offering an opportunity for capacity building within regulators.[7]

For an effective sandboxing scheme, national competent authorities referred to in Art. 59 that will oversee the regulatory sandboxes will require a sound infrastructure, good organisation, appropriate legal powers, and skilled staff. This requires considerable financial resources, which is generally lacking and largely unbalanced across Member States. To ensure uniform application across the Union, we recommend converting the voluntary nature of setting the sandboxes scheme into an obligation for Member States, with well-established criteria to ensure an effective and smooth access to businesses, particularly SMEs. Companies and research institutions should be comprehensively

[7] https://www.businesseurope.eu/sites/buseur/files/media/other_docs/regulatory_sandboxes_-_winnovation_analytical_paper_may_2020.pdf

involved in the elaboration of the modalities and conditions for the establishment of regulatory sandboxes provided for in Art. 53(6) of the draft Regulation. In addition, it is essential that all relevant national regulators are involved in regulated sandbox experiments

Furthermore, we recommend safeguarding the experimental nature of sandboxes schemes to ensure their practical usefulness, in accordance with the Council's communication (11/2020)[8]. Indeed, the current modalities would impose very high compliance requirements within the suggested sandboxes schemes, which would hamper effective innovation. Businesses must be able to experiment in a controlled manner and under the supervision of relevant regulators outside the strict application of rules in order to uncover regulatory obstacles laid by the same rules.

Measures for small-scale providers and users (Art.55)

BusinessEurope welcomes measures in Art. 55 to support small scale providers and users. Compliance costs should be kept to a strict minimum. Consideration should also be given to companies treating their IT innovation labs as start-ups.

TITLE VI: GOVERNANCE

Designation of national competent authorities (Art. 59)

BusinessEurope has frequently pointed out that the current lack of resources of national oversight bodies responsible for market surveillance and enforcement, and lack of common methodologies across the EU to ensure and monitor compliance distort the playing fields for compliant manufacturers. National competent authorities referred to in Art. 59 and the European AI Board should be granted appropriate powers within Chapter 1 of Title VI to effectively enforce this Regulation, particularly cross-border. Therefore, we implore Member States to uphold their political intentions and sufficiently fund their authorities and regulators responsible for enforcing the AI Act. Furthermore, we urge policy makers to facilitate effective joint supervision by the various relevant national supervisors, to avoid overlapping competences and conflicting requirements from different authorities. This is crucial to enhance legal certainty.

TITLE VIII: POST-MARKET MONITORING, INFORMATION SHARING, MARKET SURVEILLANCE

Post-Market monitoring by providers and post-market monitoring plan for high-risk AI systems (Art. 61)

[8] https://data.consilium.europa.eu/doc/document/ST-13026-2020-INIT/en/pdf

BusinessEurope questions the relevance and effectiveness of the proposed obligation of post-market monitoring by providers. As previously addressed, many AI systems placed on the market learn from the end user, and most often the influence shifts from the business considering risks at the ex-ante phase to the end-user or even operator. Post-market monitoring requirements for providers of high-risk AI systems can therefore hardly be fulfilled in practice. In addition, not all AI systems can be monitored, especially if it is a product with an integrated AI system. Against this background, the post-market monitoring obligations set in Art. 61 must be removed or at least limited to those requirements that can typically be fulfilled by a provider of high-risk AI systems.

Access to data and documentation (Art. 64)

Art. 64 enables market surveillance authorities to request '*full access to the training, validation and testing datasets used by the provider*' (Art. 64(1)), and to the AI system's source code upon a '*reasoned request'* (Art. 64(2)). Such proposed obligation to provide access to the source code of an AI system to regulators should be better tailored and calibrated to minimise the risk that Intellectual Property rights are affected. This is of great importance for maintaining innovation. Further guidance would also be helpful in relation to the definition of '*source code'*, which could for example be the code of the trained AI model or of the validated AI model.

Although these authorities must comply with confidentiality obligations and considering the provider might not retain control of the dataset over the AI lifecycle, providers should have the right to challenge the necessity and proportionality of such requests before an independent court. In addition, providers should never be required to violate EU, Member State, or applicable third-country laws in providing such access to Market Surveillance authorities.

Procedure for dealing with AI systems presenting a risk at national level (Art. 65)

Art. 65 and Art. 67 seem to enable market surveillance authorities in any Member State to order the withdrawal from the market of a high-risk AI system even if the system fully complies with the Regulation in case the system '*presents a risk to the compliance obligations under Union or national law intended to protect fundamental rights or to other aspects of public interest protection*' (Art. 67(1)). BusinessEurope is concerned by the vague legal language, as such provisions would enable national authorities to exclude products from the market for minor or technical violations of Union or Member State law. In addition, allowing authorities in each Member State to issue such orders would fragment the harmonised application of the AIA and put the Single Market at risk.

TITLE IX: CODES OF CONDUCT

We welcome measures in Art. 69 that support the drawing up of codes of conducts for AI applications that do not qualify as 'high-risk' to enhance trust in AI and foster its

uptake. However, we believe that these voluntary codes of conducts should not subject non- 'high-risk' AI to the same mandatory requirements for high-risk AI systems set out in Title III, Chapter 2 of the Regulation. Indeed, codes of conduct that use stringent legal requirements aimed at high-risk AI are likely to be inappropriate for lower-risk applications, become highly onerous, disincentivise participation and fail to provide clarity for users. Codes of conduct should be defined following a bottom-up approach, identifying minimum criteria to be used by public and private organisations participating in the same ecosystem. Given the pace of change, any technical specifications and solutions must be focused on the outcome to work as intended. Global standard that are designed to be flexible, boost innovation, and raise the bar in transparency, privacy, cybersecurity, safety, and resilience, could be used to avoid fragmentation.

TITLE X: CONFIDENTIALITY AND PENALTIES

Confidentiality (Art. 70)

The confidential treatment of data provided by companies to authorities and notified bodies in order to meet the requirements of the AIA is of central importance in order to protect sensitive data and trade secrets. Art. 70 of the Draft Regulation does not specify any technical and organisational requirements that receiving authorities and notified bodies must comply within this context, apart from the definition of general protection objectives (e.g., protection of '*intellectual property rights*' in Art. 70 (1) (a))). From the industry's point of view, the permission to exchange information with third countries contained in Art. 70 (4) of the draft Regulation is also critical, and needs to be consistent with provisions contained in EU trade agreements with third countries (e.g. The AIA seem to be in contradiction with EU-UK Trade Comprehensive Agreement as it prohibits the forced transfer of, or access to, source code of software with exemptions only for competition law, Intellectual Property and GPA).

Sanctions (Art. 71)

In our view the sanctions provided in the draft AIA, which exceed the sanction regime in the GDPR, are too strict (especially for low-margin businesses) and will unproportionally increase business risks related to the use and development of AI. The upstream effect of such sanction regime must under no circumstances become a brake for innovation for the development of AI in Europe. Furthermore, it is imperative to guarantee uniform interpretation and application of the sanction regime throughout the Union to avoid fragmentation of the internal market through different application. In this sense, we recommend further definition of acts and omissions which shall be sanctioned as well as mitigating and aggravating circumstances, similarly as in the GDPR.

***