DIGITALEUROPE

12 JUNE 2020

DIGITALEUROPE comments on the European Commission's AI White Paper

Introduction

DIGITALEUROPE welcomes the European Commission's White Paper on AI and the opportunity to provide feedback via the public consultation phase. As member of the High-Level Expert Group on AI, we are pleased to see the Commission continue this open engagement with stakeholders in the development of the right policy and investment framework for AI.

Our membership represents an incredible variety of organisations, all of them affected by AI-related technologies. This includes large industrial companies analysing data gathered through IoT networks on the factory shop floor; start-ups partnering with hospitals to apply AI for faster diagnosis of diseases; and firms with international supply chains, optimising their logistics to be more fuel-efficient and reduce their carbon footprint.

And now, in view of the ongoing COVID-19 pandemic, the potential of digital technologies for society and economy is unquestionable, and needed more than ever for Europe's economy recovery. AI adoption can be part of the response to slowed productivity, helping to tackle challenges of climate change and aging populations. The positive and trustworthy use of AI will be a cornerstone of a renewed, more resilient and stronger 'digital Europe'.[1]

In this contribution to the White Paper consultation, we present and develop our approach towards a balanced yet effective regulatory framework. We provide recommendations on how to best invest, where policy-makers should prioritise, and how to reinforce our skills and education systems. We advocate for the use of digital technologies with European values, to create European value.

[1] For an overview of our policy recommendations in light of COVID-19, please see: https://www.digitaleurope.org/policies/coronavirus/

DIGITALEUROPE
Rue de la Science, 14A, B-1040 Brussels
T.+32 (0) 2 609 53 10 / www.digitaleurope.org / @DIGITALEUROPE
EU Transparency Register: 64270747023-20

Executive summary

Ecosystem of excellence:

To encourage more **SMEs** to use AI, we need to support them by:

- Improving access to finance, know-how and talent through cooperation between SMEs, schools and larger firms, possibly coordinated through Digital Innovation Hubs.
- Investing in digital infrastructure, connectivity and improving access to computing resources.

Europe's **skills** framework needs to be re-thought from start to finish:

- Programming classes must be part of school curricula from an early age.
- Higher education should encourage joint degrees between AI and data-related subjects and other areas of research and science.
- Lifelong learning, upskilling and retraining programmes need to be at the centre of the overall employment agenda.
- Policy-makers should support the development of public-private partnerships between schools and business, for example through placement schemes.

There is no AI without **research**, and no research without **funding**:

- EU policy-makers need to strengthen and reinforce investments in digital as part of the Multiannual Financial Framework (MFF).
- The funding programmes and existing research excellence centres should be improved through better coordination.
- Public-private partnerships can help steer AI development from inception to practical deployment use cases.
- Build out digital infrastructure (including high-performance and edge computing) to manage data analytics and realise AI's full potential.

Ecosystem of trust

We support the use of **clear definitions** of an AI system as proposed by the OECD and the AI HLEG, and a **risk-based approach:**

- New regulatory means should be narrowly targeted, focusing on specific use cases.
- Even within sectors, this requires differentiating based on the area of application, type of deployer and taking into account fundamental

changes between business-to-business and business-to-consumer contexts.

Ex ante conformity assessments could be challenging in practice and often not the most ideal solution:

- The focus should be on encouraging principle-based internal governance processes, industry standardisation, and clarifying the application of existing regulation.
- This should be coordinated and part of the established conformity assessment procedures already present in many sectors (for example the Medical Devices Regulation in the healthcare sector, or the Type-Approval process for vehicles).
- Sector regulators should continue to function as the best-placed enforcement agencies.

A voluntary labelling system may have value but seems premature at this phase. It would in any case require further reflection on how such a framework could accommodate the myriad of AI use cases and application areas.

As regards the **safety and liability framework**, we see little to no gaps:

- Well-established regulation such as the Product Liability Directive and General Product Safety Directive are technology-neutral and do not exclude AI systems.
- Existing rules could be reinforced through guidance and possible strict liability measures in specific high-risk cases.

Highlighting the use of AI in **facial recognition technologies** (FRT) or remote biometric identification systems, we find that existing rights and legislation already provide many safeguards in terms of transparency, accountability and fairness:

- This can be improved by better communication between the developer and deployer of the AI system on the capabilities and limitations of the system.
- We encourage a broad democratic debate on the deployment of FRT and remote biometric identifications systems in the public space by government agencies.

Regarding specific considerations for **vertical sectors**:

- The healthcare, manufacturing and transport sectors pose their own distinct challenges, for example on accuracy or safety, requiring a tailored approach.

- Many of these sectors have their own regulatory oversight agencies and mechanisms, often already featuring or having been adapted for AI and digital technologies.
- Established best practices, as well as sector-specific regulation and regulators should be reinforced, rather than upending these ecosystems with new or even conflicting obligations.

Table of Contents

Section 1: Ecosystem of excellence

Increasing AI uptake and development within SMEs

SMEs, start-ups and micro-enterprises are the backbone of the European economy. They are open to using digital technologies and recognise its benefits. But while many small businesses perceive artificial intelligence as a breakthrough technology and recognise its potential, they struggle with actual adoption and uptake, due to relatively high investment thresholds and long implementation timelines. Lack of technical know-how as well as a lack of business models specifically tailored for AI are major problems. SMEs also face challenges of accessing high-quality data and when they do, further curation efforts are needed so that it can be used. Moreover, they do not have sufficient access to capital, are under-resourced compared to other regions in the world, are often a more vulnerable part of the digital value chain and find it difficult to attract and retain talents.

SMEs therefore need to be supported in accessing, developing, and using AI. The EU can create an ecosystem of excellence for these companies through increased dedicated and strategic funding in the Digital Europe programme to stimulate the understanding and uptake of AI, for example by engaging SMEs in proof of concepts with experienced AI developers. Other actions, such as access to high-performance computing resources, high-value datasets and free software development kits should be implemented in parallel.

Creating an ecosystem of trust is highly important for SMEs to reduce uncertainty surrounding AI. Trust will be a key factor to stimulate SMEs to initiate their first AI projects. However, building trust will not be achieved by developing and implementing new additional AI regulations. SMEs already perceive compliance with European regulations as a burden, and EU policy-makers should understand and address this issue as part of any AI framework. Over-prescriptive rules will deter European SMEs from making any investments in AI, it could restrict use of innovative solutions and could also slow down the overall adoption of the technology in Europe. Instead, public sector should partner with SMEs to guide them through the development and deployment of new AI projects.

The role of the Digital Innovation Hubs (DIH) is well outlined in the White Paper, but it raises some considerations. The hubs play a central role in both the ecosystem of excellence and trust, by stimulating the uptake of AI for SMEs as well as guiding them through compliance. DIHs can help the uptake of AI by developing models of integration in organisations (e.g. also in sector actors, such as hospitals), addressing their services, organisational arrangements and workflows. DIHs can also help foster best practices on testing and reference

facilities, AI standards and partnership. However, in practice, SMEs may have difficulties finding their way towards these DIHs. We would suggest though not to go for building an AI one-stop-shop, but rather rely on existing organisations and mechanisms which have experience in working together with SMEs and divide the work and responsibilities between them. This would allow more SMEs to be reached and make sure they can fully benefit from trustworthy AI.

Improving digital skills, literacy and AI education

Digital skills are essential for everyone. Digital technologies like AI are key to make labour markets more efficient at a time where European countries are experiencing lower productivity, an aging workforce, and increased global competition. AI can speed up the digitalisation of virtually all sectors, while improving the quality and inclusiveness of education. Building trust in the technology is therefore critical to accelerate its use. All relevant stakeholders involved should widely understand AI's role and functions. It's equally important that the existing workforce and future talents develop the skills they need to leverage the job opportunities that AI will offer. This is fundamental since Europe's digital skills gap is widening, as new technologies emerge and develop.

The EU must act now to provide digital skills to Europeans of all ages, to narrow the existing digital divide and avoid losing competitiveness. Doing so requires strong investments to predict future skills needs – something which AI analysis may even help with – but also modernising Europe's education curricula, improving training systems including upskilling and reskilling, introducing lifelong learning during the entire working life and beyond it, and designing a robust social framework to safeguard people against potential negative impact from the most disruptive changes.

In light of such considerations, the Commission should:

- **Ensure trust in AI through awareness, inclusion and development of digital skills and AI knowledge.** It is crucial to incorporate new ways of AI learning and ICTs in primary and higher education curricula, and provide EU-wide free AI courses for people of all ages.

  There is also a need for an inclusive, lifelong learning-based and innovation-driven approach to AI education and training. The Commission should provide the necessary tools to increase social inclusion, gender balance and multi-ethnicity in the labour force to prevent potential bias when using data in AI algorithms.

  Overall, AI technology needs to be developed in unbiased and inclusive ways to ensure that it reflects the society as a whole. A more diverse and demographically representative participation of programmers, AI experts

and designers, as well as multi-disciplinary teams, will help achieve this goal. It will also help to unleash the potential of AI for personalised education.

- **Promote basic digital skills,** which have now become a fundamental tool of active citizenship. Using and creating effective AI-embedded solutions requires educational and training programmes that **support the development of medium- and advanced-level digital skills** and encourage lifelong learning. The gains from investing in new technologies can be achieved only if there are enough people with the right skills to make the best use of it.

  The European Social Fund+, the European Regional Development Fund and the Digital Europe Programme represent the most significant funding opportunities to bridge the digital skills gap in the 2021-2027 multiannual financial framework (MFF). The EU rules applicable to funds and programmes need to reflect market realities, encouraging also advanced ICT training and taking into account the high real market cost of training related to ICT.[2]

  Building a talent pool for AI means developing competences in technologies indispensable to sustain AI analytics and machine learning. Without specialists in foundational technologies like big data, cloud computing, networking and infrastructure, Europe will not be able to make full use of AI's potential.

- **Create a Europe-wide platform for digital higher education and enhance cooperation between schools, universities, research centres and AI-focused businesses**. Erasmus+ should be used to increase cooperation through school partnerships and pupil mobility.

  The EU should also encourage cooperation and coordination between public and private sector to guarantee better technology training and re-skilling of the existing workforce. Primary examples of public-private cooperation are those defining competence-based curricula and placement schemes that promote dual degrees or trainings/education on AI and data analytics in sectors like electrical engineering and manufacturing. The European Universities initiative is a very good step in this direction. For example, in a sensitive sector such as healthcare, university curricula should include teaching on data sciences and AI.

[2] More on the cost of training in ICT in the paper here (pages 5-6): https://www.digitaleurope.org/wp/wp-content/uploads/2018/11/DIGITALEUROPEs-Position-on-EU-funding-for-digital-skills_fin.pdf

- **Ensure that AI qualifications, competences and skills can be easily identified, validated, recognised and understood.** It is absolutely crucial to embed them into well-established classifications and frameworks at European level – such as the European Qualification Framework (EQF) and the European classification of Skills, Competences, Qualifications and Occupations (ESCO) – and industry-led certifications. These schemes are up-to-date with job market needs and reflect industry skills recognition, which make them immediately transferable across the EU and beyond.

- **Make online training for digital skills a priority in the European Pact for Skills.** The European Commission should build a digital skills training catalogue valid for all workers, including MOOCs and coding classes.

- **Enhance skills intelligence in Europe through regular analysis of skills supply, demand, mismatches and development.** The European Centre for the Development of Vocational Training (CEDEFOP) should play a central role on that. It already used complex big data analysis techniques and ESCO[3] labour market intelligence to extract information from online job vacancies[4] and inform training providers on the labour market relevance of their programmes.

- **Support measures to upskill current workforce.** The EU must promote the creation and adoption of AI training, boost EU investments and scale innovation training programs across Europe. Training materials should be made available to employees, for instance through popular MOOCs and technology platforms, which offer instant access and certification.

  Lifelong learning will also become key in a dynamic AI environment. The Commission should guarantee workforce reskilling to make sure individuals remain employable in the labour market, even if the nature of their job changes. Companies should provide training opportunities and foster lifelong employability of people through continuous learning.

  This should be coupled with business measures. To this extent, companies should invest more in human capital and make skills development a key aspect of their corporate strategy.

---

[3] ESCO (European Skills, Competences, Qualifications and Occupations) is the European multilingual classification of Skills, Competences, Qualifications and Occupations.

[4] More information can be found on the European Centre for the Development of Vocational Training's website: https://www.cedefop.europa.eu/en/events-and-projects/projects/skills-online-job-vacancies

Boosting the EU's research, innovation and investment agenda

None of the EU's ambitions on AI would come to fruition if they are not paired with an equally strong research, innovation and investment agenda. DIGITALEUROPE therefore warmly welcomes the 'ecosystem of excellence' chapter and proposed measures in the Commission White Paper. Here, we offer additional points of focus and prioritisation:

- **Industry-led AI R&I superclusters** should be established to generate global leading innovations, enabling European AI talents and relevant stakeholders to join forces rather than dispersing efforts. A strong collaboration between industry and academia will allow the development of practicable AI solutions within those superclusters, so that supply and demand will be intertwined.

  Member States should also consider how **to incentivise commercialisation of AI knowledge from universities and public research organisations** across the EU, for example through grants, tax incentives, and local university-business collaboration schemes.

- **A coordinated network among the many existing AI research excellence centres** should be prioritised over creating a new one. This network needs to create a leadership structure to ensure coordination and coherent operation; agree on a vision regarding the focus and priorities beyond national borders; and provide continuous financial investment at the necessary level.

  Europe needs to invest in test labs, where industry and universities can jointly develop innovative AI applications and test them in real-life environments, under clear liability and data protection rules (including encryption, pseudonymisation and anonymisation) to foster confidence and trust.

  Public funding is needed to encourage SMEs to participate and provide innovative use scenarios to these test centres.

- R&D&I activities on AI should have a prominent place throughout the **Horizon Europe and the Digital Europe programme**, by funding core AI research, including work on AI components in research projects, while using specialised Digital Innovation Hubs as places where SMEs are enabled to test their use cases.

- As the **MFF** entails various funding programmes, **the synergies between these programmes should be strengthened** for the next 2021-2027 programming period to better support AI specific projects across Europe.

The EU funding framework should be based on agile and fast processes, including mechanisms to shorten the application-to-granting timeline for EU R&D funding.

Furthermore, we support more public funding directed at the usage of controlled training data pools with an open-source approach.

- **Europe needs to develop focused investments in industrial AI**, based on a combination of a wide range of technologies, including Machine Learning, semantics, Natural Language Processing (NLP), and vision.

  This needs to be combined with domain know-how, in those domains where Europe plays a leading role, such as combining hardware solutions, automation, semantics, high-performance and edge computing, (data) analytics, explainable and data scarce AI.

  Investments, such as through the Digital Europe programme, should be targeted at increasing the efficiency of industrial infrastructures (factories, power, transportation, etc.).

- **The planned AI public-private partnership needs sufficient support and budget**. Based on their best practices during the current MFF, the two associations Big Data Value Association (BDVA) and European Robotics Association (euRobotics) are committed to jointly shaping, developing and operating this new AI PPP.

  This AI partnership (AI PPP) will foster adoption across a wide range of sectors by enabling the leveraging of the combined resources of its members and their expertise in innovation, markets and technology.

  By leveraging the impacts and success of the Big Data Value and Robotics PPPs, the AI PPP will increase competitiveness in industrial and business sectors that are critically important for the European Union (e.g. healthcare, manufacturing, logistics, agri-food, etc.), and will accelerate transformation across sectors of economic and societal relevance for European business and citizens.

Section 2: Ecosystem of trust

Definition and scope of 'high-risk' AI

The Commission White Paper rightly identifies the need for a well-defined risk-based approach to AI regulation in order to have an effective, functional and targeted legislative framework that works with the multitude of different AI applications. Such an approach should target the right use cases, provide legal certainty, and not discourage the development and diffusion of AI.

The Commission's risk-based approach consequently proposes a tiered and incremental regulatory framework that focuses on 'high-risk' AI, looking at sectors where the AI system is used in a manner that significant risks are likely to arise. For these high-risk use cases, specific regulatory measures may be required (see below). For more general AI use cases, the existing legislative framework will suffice, possibly complemented by a voluntary labelling scheme.

DIGITALEUROPE largely agrees with the proposed risk-based and incremental approach, but finds that more effort is required to really qualify and quantify what use cases should be seen and treated as 'high-risk', if this regulatory proposal is to be applicable in practice.

Before addressing what is 'high' or 'significant' risk of AI, DIGITALEUROPE wants to comment on how to formulate a meaningful definition of an 'AI system'. Given the diversity of technologies and approaches that have been put under the term 'artificial intelligence' over the past decades, this is not an easy or straightforward task.

Ideally the definition applied by EU policy-makers originates in wide stakeholder discussion, and where possible in alignment with global partners. This would aid maximum understanding of the scope with all organisations developing and deploying AI, in and outside of Europe.

In that sense, we can refer to the definition developed by the OECD[5]:

> *An AI system is a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. AI systems are designed to operate with varying levels of autonomy.*

[5] https://www.oecd.ai/ai-principles

Of course, as a member of the Commission's High-Level Expert Group on AI, we also highlight and support the definition provided in the Ethics Guidelines[6]:

> *Artificial intelligence (AI) systems are software (and possibly also hardware) systems designed by humans that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge, or processing the information, derived from this data and deciding the best action(s) to take to achieve the given goal. AI systems can either use symbolic rules or learn a numeric model, and they can also adapt their behaviour by analysing how the environment is affected by their previous actions.*

Neither definition is likely to be perfect – especially as the technologies evolve over time, so too will what we consider to be AI change.

Regarding the risk-based approach and the White Paper proposal of what should be seen as 'high-risk' AI, DIGITALEUROPE finds that this framework and related methodology should:

- **Emphasise the need for proportionality.** Risk assessments must reflect the probability and likelihood of harm and not just the possible severity of the harm. It should also take account of the wider operational context when assessing risk, since the same AI application used for the same purpose will pose different risks depending on the way and depth of its integration into operations (e.g. task given to AI to perform, extent of human oversight, additional safeguards such as monitoring or professional training).

  For that reason, we believe that a risk assessment carried by both developers and deployers of AI systems is the best way to ensure than any obligation is tailored around the specific risks emerging from the infinite scenarios in which AI can be deployed.[7]

- **Place the use case at the centre of the assessment of risk.** While the sector criterion should be maintained, it should also not lead to any and all AI usage within that field to automatically be considered high-risk. Because even within a sector, there will be many different types of use

[6] https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines#Top

[7] We note that the cumulative criteria leads to a circular definition, because it says "should be considered high-risk where it meets [….] the AI application in the sector in question is, in addition, used in such a manner that significant risks are likely to arise." In other words, what should be considered high-risk is where "significant risks are likely to arise". The core concept is thus the risk assessment.

cases. Building out use cases and use scenarios will over time help to better understand how requirements and mitigation strategies best address similar risks (within as well as outside of the sector in which the deployment occurs).

- **Ensure consistency with existing (sector-specific) legislation.** A future proposal for AI regulation should consider the existence of several pieces of regulation in place which already cover in their scope software with AI application and ensure their consistency and coherence (e.g. the GDPR). The most effective approach would be to classify and assess the risk of the AI applications under their respective sector-specific regulatory framework, when available (e.g. risk-classification in healthcare[8]).

  Considerations must also be given to the risk classification defined in existing legislation versus a potential different risk classification in a new AI framework and the respective regulatory requirements.

- **Tailor the obligations for 'high-risk' to the actual risks and context.** Even the same general AI system can raise very different issues based on the context it is used in, and will necessitate a different approach and remedy.

  The use of AI in a consumer-facing context will raise different challenges and require different solutions than within a business-to-business situation. It would be problematic to have a list of required of countermeasures that must be used for all 'high-risk' cases, regardless of whether the measures are relevant to that AI use case.

  For instance, for concerns related to a qualified high-risk AI system trained on an insufficiently diverse training data set, leading to a racially disparate impact, any legislative requirements should address here this specific discrimination risk (e.g. by setting acceptable accuracy thresholds for performance across different ethnic and demographic backgrounds on training as well as testing datasets).

  In contrast, an AI application involving Machine Learning on a production line to determine potential collisions and disruptions would need a different approach to guarantee safety. Consequently, a principle-based approach here would give flexibility to best adapt the mitigation measure to the risk.

[8] For example, the Medical Devices and In-Vitro Diagnostics Regulations provide already a clear framework for the risk classification of healthcare application of software classified as medical device. New EU legislation on an AI framework should reference to existing legislation on healthcare products in order to avoid overlapping provisions or duplication of work as well as legislative uncertainty to which provisions apply as opposed to the new AI regulation.

- **Ensure legal certainty.** The cumulative risk-based criteria is, broadly, a workable approach. That said, while using sector as an initial criterion may help focus the scope of potential regulatory requirements on high-risk AI, this in itself cannot be the main factor. Given that use cases within a sector will vary significantly, it would be more practicable to emphasise the criterion of the actual use case (and associated likelihood of harm).

  Furthermore, the 'exceptional instances' clause that goes beyond the cumulative criteria (including AI applications that affect consumer rights) should be carefully examined and should not be open-ended to avoid legal uncertainty.

  The processes to establish and periodically review the 'exceptional instances' as well as a possible exhaustive list of high-risk AI use cases should be clear, transparent, based on evidence and take place in consultation with involved stakeholders. Changes and additions to any such list should be followed by a transition period to ensure AI developers can review, prepare and implement new procedures.

- **Remove the concept of 'immaterial damages' from scope of risk definition.** This is a wide legal concept that can mean anything from economic or data loss or emotional distress. Because it requires a complex, always ad-hoc and subjective analysis, it could lead to legal uncertainty, discouraging investment and innovation.

- **Be reasonable about the performance standards imposed on high-risk AI.** There is a concern that innovative uses of AI could be precluded by demanding regulatory standards for AI systems far exceeding that required of non-AI approaches.

  While it is important to seek to minimise mistakes, no system, whether human or AI powered, will ever be perfect, and in some situations a lower level of accuracy may be acceptable. A sensible regulatory standard would be to require developers/deployers of high-risk AI systems to determine, as part of their risk assessment, reasonable levels of accuracy needed to ensure safe outcomes. It could also include requiring certain skillsets and competences of professional users in high-risk applications, where professional education and certification may be important tools.

- **Factor in the benefits of using AI and the opportunity cost of not using AI.** Any risk assessment should take a holistic view, reflecting not only potential harms but also potential benefits to citizens, businesses and societal opportunities.

The benefits may outweigh the risks, especially if these can be mitigated in a thoughtful way with appropriate safeguards. Regulation must not discourage use in such cases.

We also remind here that many actions can be done by either using AI or other technologies. Technology-specific regulation may have a counter-productive effect, if it leads to other inferior technical solutions being applied just because they're easier regulation-wise, or to the same work being done without AI yet with continued or more risks (e.g. bias from human error).

- **Be technology neutral where possible.** AI is constantly evolving and improving and should be treated equally with other technologies. The so-called 'technology neutrality' principle has already been recognised and applied at European level in recent key legislations such as in the GDPR and the NIS Directive.

  Therefore, we strongly recommend the application of the technology neutrality principle when assessing the need for regulatory intervention on AI. This ensures that policy framework remains dynamic, adapting to the evolution of the technology.

Governance framework

Continuing from the risk-based approach, the White Paper envisions a framework in which high-risk AI applications would be subject to a mandatory pre-marketing conformity assessment. These assessments should test and certify specific AI products or deployments against five key requirements.[9] These obligations will be imposed on the actors that are best placed to address any potential risk across the AI value chain, including on developers, deployers and other end-users.

Consequently, for this to be effective and to work in practice, it will be essential to clearly define what is and is not a high-risk AI application. Any enforcement mechanism should then also as much as possible be specified under existing sectorial legislation (where available) and rely there on the expertise of the

[9] Paraphrased from the Commission White Paper (p.18 and further):

"(1) the quality and relevance of the AI's training data, including to ensure that the data does not result in prohibited discriminatory outcomes; (2) the ability to provide accurate documentation on the datasets and programming techniques used to build, test, and validate the AI; (3) transparency requirements—namely, that developers disclose the capabilities and limitations of their AI offerings, and deployers notify those who interact with an AI system; (4) on the system's robustness and accuracy; and (5) for various types of human oversight would tested and certified by a designated body."

established regulatory authorities. On the proposed regulatory framework, DIGITALEUROPE therefore recommends that this should:

- **Build on existing laws and governance mechanisms**, to develop a framework which incentivises developers of AI to establish a governance and accountability structure through risk-based, verifiable and operational practices. This enables more flexible and tailored processes, formats and tools and rather than imposing specific rigid or strict requirements.
- **Support research efforts aimed at clarifying how existing laws should be interpreted and applied** vis-à-vis AI systems with the aim to provide for baseline structures, requirements, tools, and remedies in the protection of fundamental rights.
- **Ensure that any conformity assessment clearly distinguishes risks to safety and value-based risks**, and that existing rules on market surveillance or conformity assessments are not duplicated. Beyond duplication, it would also be recommended to integrate any requirements imposed on AI into existing conformity assessment processes, rather than building a new stand-alone horizontal process for AI.
- **Compliance assessment of an AI framework should factor in existing provisions** in other pieces of legislation which require certain classifications and risk assessment. Therefore, such compliance provisions should be structured to refer to existing requirements in order to contribute to enhanced legislative clarity and to avoid any inconsistencies, through the development of sector specific guidance documents issued by the respective regulatory authorities.
- **Encourage innovative, risk-based and collaborative regulatory oversight**.

Requirements on 'high-risk' AI systems

DIGITALEUROPE believes that, to effectively mitigate any risk arising from the deployment of AI systems, measures should be adequate and proportionate to the risks. The best way to achieve this is to tailor any obligation (e.g. re-training the system or keeping records) to the outcomes and conclusions of the risk assessment and identify the best and most efficient tools to match the AI system with the overall principles, norms and requirements.

Requirements that are intrusive and burdensome would simply stifle innovation, limit the openness of the market for smaller players and make it unnecessarily difficult for organisations to deliver innovations to customers. Cost is also a consideration: conformity assessment requiring excessive compliance burden will

be prohibitive for smaller companies that might not have the resources to cover expensive, and repeated, assessments.

Governance[10]

Consequently, rather than focusing on or mandating specific requirements and as an alternative to potentially burdensome ex-ante conformity assessments, we find that governance and accountability (systems, controls, and processes), within organisations, can be a better way to achieve for trustworthiness and will contribute to actually operationalise principles through risk-based, verifiable practices. Indeed, governance of organisations must play a role in laying out the principles by which they will use or develop artificial intelligence.

To this aim, the framework should incentivise that AI considerations are integrated into the governance of organisations and ensure compliance with EU rules, including the rules protecting fundamental rights and consumers' rights, in particular for AI systems operated in the EU that pose a high risk and including measures to address those risks, and possibly to redress undesired effects.[11]

At the same time, given how varied internal approaches to AI development and its applications are, any specific mandated set of governance requirements run the risk of being very limiting. AI developers and deployers must be given the space to develop governance framework that suit their activities and allow them to innovate in that space.

Any internal governance framework for high-risk AI use cases could additionally be strengthened through a voluntary process-based certification scheme instead of individual product or algorithm-based certifications in order to avoid 'repeated assessments over the lifetime of AI systems' as suggested in the White Paper. It could focus on the effectiveness of the company or system wide processes that are applied to the ethical development, deployment and operation of AI systems.

With process certification, one can provide the required insights into best practises applied to the development and deployment activities that each AI system undergoes. Therefore, it would enable new product versions without the need to re-assess AI systems throughout their lifetime each time. This will require

[10] In the White Paper, 'governance' is used as meaning regulatory oversight. We suggest replacing 'governance' by 'regulatory oversight', to not create confusion with governance of organisations.

[11] Elements of possible governance mechanisms might include the following: implementing a robust risk assessment to identify and mitigate risks early on; internal standards to guide the responsible deployment and operation of all AI-embedded products and services, ensuring proper oversight; reviewing potential benefits and risks, defining mitigation strategies, contingency plans and metrics, and adopting procedures to continuously review and improve; appointing and training dedicated staff with responsibility for ensuring the adherence to the commitments.

defining the criteria and a methodology for evaluation. Following this approach, a process certification scheme could serve as the baseline across industries that will provide a transparent and effective processes to develop and deploy trustworthy AI systems.

Robustness & Safety

Compliance of products with safety legislation in Europe has historically been enforced through voluntary or mandatory assessment, national standards, or codes of practice. The current framework for products safety in Europe is composed by the General Product Safety Directive (GPSD) and other sectorial legislations.[12] The GPSD introduced general safety requirements for products placed on the market. Compliance is determined through a conformity and safety assessment procedure, conducted by the company itself or with a certified body, depending on the requirement of the legislation.

Potential new or additional AI-related conformity and safety assessments should therefore be based on self-assessment and limited only to the most high-risk scenarios, where significant harm to health and safety is a serious risk. Any such conformity assessments need to be aligned to existing rules which already provide an adequate framework to address health, safety and protection of consumers and of the environment. Market surveillance authorities should have powers to make reasonable requests to all actors involved if they believe requirements have been breached so a reasonable request for documentation can be made. Sectorial legislation and enforcement mechanisms, often already covering AI, should be retained.[13]

Standards

DIGITALEUROPE argues that the international and European standardisation should play a central role in supporting compliance with the conformity assessments. While different options for compliance could be warranted in some cases, implementation of industry standards can offer an efficient and common way to do so, for instance as it is done with presumption of conformity under the New Legislative Framework (NLF). Open standards can complement this and boost innovation, create trust and accelerate scaling interoperable solutions.

Specification through international and European standards provide technical and organisational means that organisations can use in support of their

[12] Including the Machinery Directive, the Medical Devices Regulation (MDR), the Radio Equipment Directive (RED), and Vehicle Type-Approval Directive.

[13] For more detail, see the final chapter of this paper with highlights on the existing safety and conformity assessment frameworks in the area of Healthcare, Manufacturing and Automotive.

compliance to regulatory requirements.[14] Industry standards can therefore be a way to make terms such as explainability and transparency more concrete and operational in a specific context.

The drive for standardisation should were possible be bottom-up, giving space for AI developers to develop standards that support flexible demonstration of data quality, robustness and accuracy for example, tailored to specific sectors and applications.

DIGITALEUROPE encourages the EU therefore to have a greater coordinative role to shape the development of international standards for trustworthy AI in cooperation with for example International Organisation for Standardisation (ISO) and International Electrotechnical Commission (IEC) to harmonise the technical requirements of AI. This will ensure a level playing field globally and open AI markets for European industry worldwide.

Voluntary labelling

Even for low risk applications of AI, the value of a voluntary labelling scheme is not clear from a regulatory perspective. Since providers are responsible for the assignment of quality labels, such a scheme is not suitable to address liability or accountability issues. However, if seen as a means for providers of AI-based products and services to provide information on their quality, voluntary labelling could be beneficial for customers in order to compare them.

The Commission's AI White Paper itself provided very little information what such a system could look like, who it would be for (i.e. even within 'low risk' AI, there are great discrepancies between the B2C or B2B context), and what it would entail in practice for companies to apply and manage such a label. Consequently, any such voluntary labelling framework can only be achieved through a unified approach, hence we urge the need to incentivise the use of standards in this space. This should be industry-driven, sector-relevant as needed, supervised by the European Commission and endorsed by all EU Member States in order to serve as a valued benchmark within Europe and across the globe.

Regulatory oversight

DIGITALEUROPE believes that it is also important to identify the best possible authority that should oversee the compliance with these rules, as well as rely on

[14] For example, concerning also the earlier point on governance, we can refer to the work done in IEEE, CEN-CENELEC and especially the ISO/IEC JTC 1/SC 42 on AI standardisation, including also on Management Systems Standards: https://blog.iec.ch/2019/11/international-standards-committee-on-ai-ecosystem-achieves-milestone-and-launches-new-areas-of-study/

existing sector regulatory bodies and their European coordination structures.[15] While we believe national authorities might need to play a role to enforce the rules locally and in its specific sectors, it is also mandatory to ensure the coordination of enforcement across Europe given the global nature of AI technology development.

Reviewing the safety & liability framework

In addition to the White Paper, the Commission published a report on liability and new technologies, seeking views of stakeholders on whether liability rules should be reviewed and expanded in anticipation of the increasing use of AI, to which it attributes specific characteristics such as complexity, opacity, and autonomy. Several reflections should be made in that respect.

As noted before in the discussion on scope and definition, AI as a technology cannot be clearly and unambiguously defined. It is a general term under which various subcategories are summarised. Each of these is characterised by special technical features, which can be weighted differently given that in each case, AI systems are designed for a special field of application. The diversity of emerging digital technologies (and the diversity of use and application) leads to a wide array of risks, which makes it very difficult to come up with simple solutions.

In addition, some of the characteristics ascribed to AI are equally applicable to other technologies, for example with regard to complexity. While many innovative products, such as smart devices or robots, involve multiple producers (e.g. separate hardware and software producers), this is also true for many tangible products today (e.g. cars have many hundreds of suppliers) that are effectively regulated by the EU's existing liability regime. Moreover, some of the special issues generally associated with AI, such as the lack of transparency or the unpredictability of concrete individual results, do not apply to all forms of AI but to the more data-driven, probabilistic AI solutions where causality can be more difficult to identify.

Finally, autonomy is neither a characteristic feature of AI in general nor of Machine Learning in particular. Although artificial intelligence can be used in autonomous systems, both are not the same. In fact, it is perfectly viable for autonomous systems to exist without AI technology: the essential feature of autonomous systems is self-control without human intervention in the system process. AI is often used in assistance systems that support a human decision, but does not replace it.

[15] For example the Medical Devices Coordination Group or the European Medicines Agency.

All these points highlight that the concept of artificial intelligence is a difficult starting point for a technology-neutral regulation.

Consequently, we need to be thoughtful about how new rules will fit within the broader existing EU regulatory framework – that has largely proven to be fit for purpose – and how the AI White Paper's envisaged regulatory changes, for instance with regard to responsible AI (e.g. on data quality, transparency, certification, etc.) or safety are likely to take away some of the concerns with AI. This could significantly reduce the need for new liability rules such as changing the burden of proof.

At the same time, these envisaged changes will not simplify the uptake of the technology. A difficult balance has to be found to avoid that more rules – including on liability – would take away incentives for developers to innovate responsibly if they are exposed to a wide array of risk. Innovators need clear and workable rules and should only be held responsible for circumstances which they can really influence. Otherwise, companies will substantially slow the rate of innovation for fear of triggering unforeseeable consequences that could lead to significant liabilities. The remarkable innovations we have seen over the last twenty or more years only exist because the legal environment for them is favourable and balanced. Changing the current regime requires further empirical evidence and compilation of 'real-world' case studies where the existing rules have proved inadequate as a first step.

AI in the context of the wider liability framework

The Product Liability Directive (PLD) sets out clear, well understood and time-tested rules which are technology neutral in relation to products and consumers. That the PLD has been in force for over 30 years is a sign of its strength, not a weakness – it has functioned very well even in the last decades accommodating many technological changes, uptake of digital technologies and development of new innovative products. The burden of liability risks is on the producer but without demanding anything impossible or unreasonable, leaving room for innovation.

Noting the work of the Commission expert groups and advisory bodies on a potential review of the PLD, we could agree that some clarification could be useful on certain definitions to enhance legal certainty. For instance, it would be beneficial to clarify that when a producer has embedded software in a product, this is considered part of this product. Case law and jurisprudence has largely already taken this approach.

Outside of the PLD, it is crucial to keep private autonomy for companies to – within a framework – freely negotiate their contractual relationships or

partnerships. Technology providers should not be held responsible or liable to a use or application of technology that was not agreed or explicitly excluded by way of contract. In many sectors, contractual liability or other compensation regimes will usefully apply alongside or instead of tortious liability.

These considerations are of particular importance given that AI applications can evolve, which complicates the division of legal responsibility between operator and manufacturer of an AI system. In Machine Learning, for instance, it depends not least on whether the system continues its learning activity in productive operation or whether the learning function is switched off when the system is delivered. In the case of continuous learning activity, incorrect output results of the system may not be the sole responsibility of the manufacturer but may be due to the data supplied by the operator. Special care must be put on situations, where services are delivered via the cloud or an API, where the services provider does not maintain control over the use and purposes of the technology.

As an additional note, a pan-European framework would be preferable to further fragmentation or divergence of different national liability rules. An EU-wide framework would help prevent local 'AI safe harbours'. For similar reasons, it would be important to find common ground not only within Europe, but also internationally as much as possible.

Burden of proof

As suggested in the liability report, a reversed burden of proof is a very sharp tool with major consequences for existing legal systems and court procedures. As a general rule, a claimant should rather continue to be required to prove the fault and defect, harm and causal link. A reversed burden of proof should only be considered in high risk cases and be context specific. In cases where it would be indeed an unreasonable hurdle for the claimant to prove the liability conditions, due to the specifics of the technology and concrete circumstances, the defendant (here: the producer) could be required to demonstrate that they complied with the applicable safety and responsible AI conditions. Any other approach risks to impose a disproportionate and possibly unbearable burden of proof on the producer, by requiring them to prove that the harm is not caused by their fault (without for example knowing how the product was used by the claimant).

Strict liability in exceptional cases

Strict liability for AI applications should only be considered in very exceptional cases and clearly defined, limited to those situations concerning harm to life or limb and in the public space. Any other definition would risk to water down the definition of high risk. The public space criterion is critical in this context: a strict liability regime only seems to be justified if the significant damage occurs in

public, where there is no direct link or contractual relationship between the involved parties.

Wider and less defined approaches would be particularly problematic for AI developers and would dis-incentivise innovation by making it very difficult for developers to control their liability risk. For strict liability to be applied properly it is crucial to understand who has the economic or social benefit from applying a system or using the technology and for what use the technology was foreseen.

As noted above, legal certainty is another crucial constraint. If an AI application area would to be formally listed or classified as high-risk, then operators and actors in the value chain (including for example insurance providers) should be given transition time to correspond to different and the more stringent requirements paired with strict liability.

Even in those cases of strict liability, the injured party should at least have to plausibly demonstrate and, if necessary, prove the amount of his loss and the fact that the loss was caused by a system of the operator. Mere allegations must not lead to compensation. In any case, operators of high-risk AI systems must be exempted from liability if they can prove that the operation of their system did not effectively cause the damage (e.g. because such damage was due to the negligent acts or omissions of the harmed person or any third party).

Product compliance and standalone software

The existing product safety framework, specified through EU Harmonisation Legislation, remains the most proportionate way to deal with products placed on European markets where AI plays a role to the functioning of that product. This framework focuses on a specific set of products that raise specific safety concerns, defines requirements and an established process to demonstrate. As underlined by the Commission report on product safety and liability accompanying the AI White Paper, this body of rules already covers embedded software and, more broadly, requires producers to consider the product's use throughout its lifestyle.

Given the very broad scope of AI powered software products and services, any extension of product compliance requirements to standalone software must be very careful considered in terms of proportionality and impact on innovation. Unlike physical products, software more generally can be very easy to distribute. They can be developed under short timelines and can be rapidly updated. Imposing burdensome testing and product safety compliance requirements on software before it is placed on the market could therefore seriously slow the development of innovative, low risk AI-powered solutions. Any consideration linked to the specific characteristics of AI should be managed within the

established framework of existing EU product safety legislation (i.e. self-learning medical diagnostics software within the scope of the Medical Devices Regulation), and any requirements on software falling outside of the scope should be strictly focused on high-risk applications of AI.

Highlight on Facial Recognition Technologies and Remote Biometric Identification Systems

AI technologies that process personal information for remote identification purposes are generally used to reduce the time spent to identify people in pictures and video. Finding missing children, expediting the authentication process to enter into a building, finding and removing illegal imagery posted online and preventing and fighting against criminal offences are all use cases for which AI can improve manual processes to become more accurate and efficient. However, these technologies may indeed have the potential to impact on fundamental rights, especially if misused. As outlined by the Commission in the White Paper, such impact can vary considerably depending on the purpose, context and scope of the use.

In the White Paper, the Commission classified 'remote biometric identification' and 'invasive surveillance techniques' as high-risk AI use cases. The Commission also recognised that the General Data Protection Regulation (GDPR) and the Charter of Fundamental Rights of the EU (EU Charter) already apply to these use cases. Before moving forward with new regulation, it's important to understand the scope of these existing protections and to clearly identify any gaps.

Both the EU Charter and the GDPR are 'technology-neutral'. They already fully apply to remote biometric identification systems based on AI not only by framing the use of such technologies but also by providing strong enforcement mechanisms to prevent potential misuses likely to impact rights and freedom of individuals. The GDPR often requires deployers of AI involving the management of European citizens' data to perform Data Protection Impact Assessment, looking at risks and benefits of such processing and to consider purpose limitation and data minimisation. The existing EU legal framework also covers specific uses of remote biometric identification such as for law enforcement purposes where it is strictly necessary and subject to appropriate safeguards.

In this context, deployers of remote biometric identification are in the better position to make sensible decisions about whether a particular AI system is appropriate for a given use case and to implement processes to mitigate any risks or shortcomings of the AI system. AI developers can nevertheless play a role in helping to ensure that remote biometric identification systems are

developed and deployed in ways that do not undermine fundamental rights. Steps that developers can take to promote the quality, safety and appropriate use of these tools include being transparent about the capabilities and limits of the AI systems they provide, and taking steps when developing and training those systems to mitigate risks of unfair bias, discriminatory outcomes and other harms to fundamental rights. These and similar types of processes and procedures designed to mitigate risk and protect rights are particularly relevant given that AI development takes place around the globe, and AI developers in some cases may not be directly subject to EU law (such as the GDPR) in the same way that deployers may be.

Especially where a remote biometric identification system is used in a law enforcement situation, the complexity of the use case at stake combined with potential social concerns that facial recognition can raise could require AI developers to take further steps in order to help deployers to mitigate against possible misuse and abuse (through aforementioned information on the AI system's capabilities and limitations). Developers should also be able to take steps to help ensure that the law enforcement body using the technologies deploys them in ways that protect EU fundamental rights of the person targeted.

Any decision likely to impact the rights and freedom of a person, for instance starting a criminal investigation, should be taken by a duly trained person, based on their analysis of the identification evidence provided by the AI system. More generally, anyone having access to the remote biometric identification system on a need-to-know basis should receive specific training on the AI system in order to be able to use the system appropriately and interpret the results accurately.

Ultimately, the use of such technology for surveillance purposes should be under oversight of a competent body to avoid any uncontrolled use. Additional measures may also be appropriate. For example, to help identify and address problems of bias in remote biometric identification technologies used in high-risk scenarios, encouraging developers and deployers to support the development of appropriate testing and other methods that help mitigate bias.

Sector-specific considerations

AI & Healthcare

In the EU Single Market, there are strong risk-assessment processes in place for AI-based health solutions intended for medical purposes such as diagnosis, prevention or treatment of diseases, which fall under the scope of the Medical Device Regulation (MDR) 2017/745 and In Vitro Diagnostic Regulation (IVDR) 2017/746. These regulations contain well-defined risk classifications based on the potential risk of harm posed by the device.[16]

Manufacturers of AI-embedded medical devices and AI/software regarded as a medical device must then meet very strict requirements and establish a robust Quality Management System which can rely on well-detailed European harmonised standards[17]. They must also submit to the notified body's review extensive technical documentation that must include data summaries and conclusions of software verification and validation against reference datasets, as well as the manufacturer's plan to guarantee post-market surveillance of the medical device.

Additionally, there is extensive guidance on how to conduct the assessment and meet those requirements, particularly as laid out by the Medical Devices Coordination Group's Guidance Document on the Qualification and Classification of Software in the MDR/IVDR (MDCG 2019-11). Nevertheless, there are areas where more guidance would be helpful to support authorities' assessment and harmonising requirements for manufacturers (for example for self-learning systems), which could build upon the strong basis provided by the Guidance Document (MDCG 2020-3) about significant changes where it clarifies how to approach changes to a device that should be considered a "significant change in design or a significant change in the intended purpose".

The sectoral regulatory authorities and bodies (i.e. Medical Devices Coordination Group and Notified Bodies) should define the guidance and ensure enforcement of MDR/IVDR on AI systems under the scope of these regulations as they are

[16] Specifically, according to Rule 11 in the Annex VIII of the MDR, software will be classified from high (Class III) to low (Class I) risk depending on the purpose and potential harm. This is based on factors such as if the software provides information for decision-making or diagnosis, which can then be split up between medium or high risk (IIa, IIb or III) if it can cause serious deterioration, or irreversible deterioration or death respectively. The same goes for software intended to monitor physiological processes, and if these can result in immediate danger to the patient.

[17] Such as EN ISO 13485:2016 and EN ISO 14971:2012, respectively covering quality management and risk management.

best positioned to assess risk and potential management strategies, based on their expertise in healthcare applications.

As regards safety, the MDR contains its own general safety and performance requirements for medical devices, as well as liability provisions. The Product Liability Directive also applies to medical devices.

Complementing further our overall comments on skills and education for AI, DIGITALEUROPE especially encourages the EU to involve all relevant stakeholders in educational and training programmes to reap AI benefits in health. Regulators need to fully grasp the technology's inner workings when they are to make decisions on the certification of sophisticated AI devices in highly regulated environments. Healthcare practitioners must have data science skills to integrate technology in their daily work and need to have the necessary healthy level of scepticism and critical thinking when embedding AI outputs into decision workflows. They also need to be in the position to accurately explain AI's benefits, limitations and risks to patients, who should also have digital acumen if we are to build trust in the technology. Finally, it is absolutely crucial to modernise school and university curricula to prepare tomorrow's AI talent.

Building on our recommendations regarding research and investment, we reiterate that the establishment of world-reference testing facilities and supporting AI research excellence centres which focus on healthcare will help advance knowledge in this domain and attract and retain the best talent. As said before, these centres should partner with healthcare actors to test AI solutions in real operational environments.

AI & Manufacturing

When it comes to AI in the manufacturing and industrial Internet of Things context, we see that AI-embedded manufacturing solutions such as connected devices, machinery and other equipment are covered by EU product legislation such as the Machinery Directive as well as legislation under the New Legislative Framework (NLF). The existing framework should continue to cover them.

Before placing an AI-embedded product in the market, the manufacturer must ensure that the product satisfies the relevant essential health and safety requirements. This is generally based on international standards and self-assessment, covering a wide range of detailed requirements on specific aspects. For machinery, this includes general principles, control systems, protection against mechanical hazards, characteristics of guards and protective devices, risks due to other hazards, and maintenance.

There is also a compulsory risk assessment process that manufacturers must conduct before the machine is even designed. It is an iterative process and includes the definition of the intended use and, importantly, any reasonably foreseeable misuse, the identification of hazards that can be generated by the machinery and the associated hazardous situations, as well as an estimation of possible risks of injury or damage to health and their likelihood to occur.

As said, this is an iterative process of risk assessment and risk reduction. Should the manufacturer identify any potential risk stemming from AI, it would remove it in this process. The process is supported by harmonised standards.[18] Consequently, AI safety is already covered in this existing conformity assessment regulatory framework.

AI & Transport

In terms of the use of AI for autonomous driving and intelligence transport systems, it is crucial to recall that road vehicles fall under the New Legislative Framework and are regulated at the EU-level. There is legislation for specific conformity assessment as part of Regulation 2018/858 for passenger cars and commercial vehicles, and other sectorial Regulation for two and three-wheelers. These procedures, called Type-Approval, are rather strict.

Under EU law, motor vehicles are tested following a list of requirements (part of aforementioned Regulation 2018/858) put forward by a testing laboratory acting on behalf of the Government Agency (the so-called Type-Approval Authority). The Type-Approval Authority is ultimately in charge of deciding whether to grant a certificate to allow the manufacturer to sell vehicles in any Member State.

There is only a very limited list of systems which can be assessed in-house. All other vehicles need to go through mandatory third-party assessment. The Type-Approval certificate is also in principle not limited in time, but once 7 years are passed the Authority evaluates if it has to be renewed (new rule valid from 2020).

This Type-Approval conformity assessment procedure therefore is well established in Europe. Therefore, there should not be any new or separate process specifically for AI systems. Any regulatory approval related to AI or digital should be done within the framework of the existing Type-Approval rules.

The same is true for aspects related to safety: this area is primarily covered by Type-Approval already. The automotive industry also widely uses design and

[18] For example, EN ISO 12100 on risk assessment and risk reduction is harmonised under the Machinery Directive. It provides a robust methodology for achieving safety in the design of machinery.

performance standards overseen by major standardisation bodies that define the state of the art in engineering. Of course, the safety framework is complemented by tailored provisions on liability, here specifically through the Motor Insurance Directive. The sector is assessing to what extent guidance or amendments could be useful to apply these rules fluently to automated vehicles.

OR MORE INFORMATION, PLEASE CONTACT:

Jochen Mistiaen

Senior Policy Manager

Jochen.mistiaen@digitaleurope.org / +32 496 20 54 11

About DIGITALEUROPE

DIGITALEUROPE represents the digital technology industry in Europe. Our members include some of the world's largest IT, telecoms and consumer electronics companies and national associations from every part of Europe. DIGITALEUROPE wants European businesses and citizens to benefit fully from digital technologies and for Europe to grow, attract and sustain the world's best digital technology companies. DIGITALEUROPE ensures industry participation in the development and implementation of EU policies.

DIGITALEUROPE Membership

Corporate Members

Accenture, Airbus, Amazon, AMD, Apple, Arçelik, Bayer, Bosch, Bose, Bristol-Myers Squibb, Brother, Canon, Cisco, DATEV, Dell, Dropbox, Eli Lilly & Company, Epson, Ericsson, Facebook, Fujitsu, Google, Graphcore, Hewlett Packard Enterprise, Hitachi, HP Inc., HSBC, Huawei, Intel, Johnson & Johnson, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, MasterCard, METRO, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe Inc., NEC, Nokia, Nvidia Ltd., Océ, Oki, Oracle, Palo Alto Networks, Panasonic Europe, Philips, Qualcomm, Red Hat, Roche, Rockwell Automation, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Siemens Healthineers, Sony, Swatch Group, Tata Consultancy Services, Technicolor, Texas Instruments, Toshiba, TP Vision, UnitedHealth Group, Visa, VMware, Xerox.

National Trade Associations

Austria: IOÖ
Belarus: INFOPARK
Belgium: AGORIA
Croatia: Croatian Chamber of Economy
Cyprus: CITEA
Denmark: DI Digital, IT BRANCHEN, Dansk Erhverv
Estonia: ITL
Finland: TIF
France: AFNUM, Syntec Numérique, Tech in France
Germany: BITKOM, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: Technology Ireland
Italy: Anitec-Assinform
Lithuania: INFOBALT
Luxembourg: APSI
Netherlands: NLdigital, FIAR
Norway: Abelia
Poland: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Romania: ANIS, APDETIC
Slovakia: ITAS
Slovenia: GZS
Spain: AMETIC
Sweden: Teknikföretagen, IT&Telekomföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
Ukraine: IT UKRAINE
United Kingdom: techUK