Brussels, 17 June 2024

Orgalim key recommendations on digital policy

Policy proposals for the upcoming EU legislative period

Introduction

Orgalim represents Europe's technology industries, developing and manufacturing the products, systems and services that enable the digital transformation and a climate-neutral future for the European Union and its citizens. Europe's technology industries comprise 770,000 innovative companies spanning the mechanical engineering, electrical engineering and electronics, ICT and metal technology branches. Together they represent the EU's largest manufacturing sector, generating an annual turnover of €2,835 billion, manufacturing one third of all European exports and providing 11.7 million direct jobs.

As we enter the EU 2024-2029 legislative cycle, the priorities Orgalim puts forward in its policy agenda are designed to position Europe at the forefront of global technological innovation and sustainability, ensuring the EU remains a competitive force in the high-tech manufacturing sector. Here, we highlight six fundamental priorities:

- Decrease the regulatory burden
- Regain global leadership in research and innovation
- Recommit to the single market
- Make digital legislation work for manufacturing industries
- Remove trade barriers
- Ensure a competitive and secure energy supply

Recommendations

This paper addresses our specific recommendations for digital policies to give a strong boost to our industries' competitiveness in Europe:

1. Effective implementation of digital rules
2. Boost digital investment and capacity
3. Promote a strong and trusted industrial data ecosystem
4. Advance industrial artificial intelligence
5. Clarify overlaps and ensure efficient governance of cybersecurity rules
6. Initiate more international digital partnerships

A list of case studies of technology industries delivering digital solutions for the net-zero transformation is available on Orgalim's website.

1. Effective implementation of digital rules

- Over the past EU legislative term, we have seen an unprecedented amount of new digital legislation (AI Act[1], Data Act[2], Cyber Resilience Act[3], etc.) and sweeping revisions of existing rules (NIS 2[4], Product Liability Directive[5], etc). As technology manufacturers, including SMEs, start to implement all these changes they need enough **time and guidance** to be confident regarding their legal certainty and to ensure that the intended objectives are achieved in practice. This includes guidance on New Legislative Framework (NLF) concepts related to software (OS vs apps, placing on the market definition, app stores, etc.) to ensure legal certainty for economic operators.
- **Standardisation** is key for the implementation of digital policy and a fundamental element of workable and effective market access conditions. To enable efficient preparation, the development of standards should be transparent and participatory. Appropriate conditions and sufficient time are needed for standardisers to address the huge number of new requirements and for manufacturers to implement the new standards for processes and products before the entry into application of legislation[6].
- For the time being, **additional regulation in the digital area must be avoided**, giving companies and authorities time to implement the new requirements while supporting innovation. Regulation is not the only instrument available to EU legislators. If further regulation is considered indispensable, proposed new rules must be well targeted, **avoid overlaps** with other legislation and be backed up by thorough **impact assessments** covering the whole value chain. This means opting for innovation-friendly approaches such as the NLF and avoiding burdensome third party conformity assessments. Better regulation principles should be followed. In particular, new proposals must take into account sectoral specificities and the differences between business-to-business (B2B) and business-to-consumer (B2C) as well as the impact on SMEs. **Regulatory sandboxes** should be considered *before* proposing any new digital legislation and thorough consultation and involvement of industry must be allowed for.
- **Effective governance** of digital legislation must be ensured: one regulation, one interpretation. Interpretation of legal texts must be uniform across the EU and market surveillance authorities must have the resources to enforce new legislation. Verification, reporting and notification obligations should not be duplicated within the European single market and should be undertaken centrally wherever possible.

2. Boost digital investment and capacity

- **Encourage private investment:** incentives for private investment in digital technologies must be created, particularly in startups and SMEs focusing on Europe's current strengths such as advanced manufacturing (AI, cybersecurity, and data management, etc.). The aim must be to create stable conditions and establish a clear and predictable regulatory framework, with uniform interpretations of regulations, that encourages private investors

[1] Artificial Intelligence Act (AI Act) as adopted by the European Parliament on 13 March 2024.
[2] Data Act Regulation (EU) 2023/2854
[3] Cyber Resilience Act (CRA) as adopted by the European Parliament on 12 March 2024.
[4] NIS 2 Directive (EU) 2022/2555
[5] Product Liability Directive as adopted by the European Parliament on 12 March 2024.
[6] See Orgalim Position Paper on Enhancing EU manufacturing competitiveness with a future-proof approach to placing products on the Single Market, June 2023

to feel confident and also take risks in their investments in these areas. EU programmes must be designed in a manner that incentivises and leverages private investment, including through public-private partnerships (PPPs) such as Made in Europe and the Smart Networks and Services Joint Undertaking. National specific requirements that hamper the development of the single market must also be scrutinised.

- **Foster R&D in key technologies, such as semiconductors, photonics, AI and quantum technologies:** the continuation of the Chips for Europe programme must be ensured under the next Multiannual Financial Framework. The strategic goals should focus on long-term supply security for the European economy and achieving a competitive edge. Innovations such as leading-edge semiconductors for AI and quantum computing are key to gaining a knowledge advantage. Investments should also be geared towards power electronics, microcontrollers, safety components, and innovative Application-Specific Integrated Circuits (ASICs) to meet the growing innovation needs of machinery and equipment. Partnerships between businesses, research institutions, and the public sector should be encouraged.
- **Strengthen the electronics ecosystem:** the EU aims to increase Europe's current share of global semiconductor production from less than 10% to 20% by 2030. To achieve this and encourage private investments in the European semiconductor industry it is necessary to optimise the framework conditions; for example by increasing access to skills, accelerating the granting of permits, and decreasing the regulatory burden. In addition to semiconductors, advanced packaging[7], printed circuit boards (PCBs) and electronics manufacturing services (EMS) should be recognised as indispensable parts of the electronics ecosystem. In this context, machine manufacturers and packaging companies should also be supported to strengthen the EU's advanced assembly capabilities and reduce its dependence on international suppliers.
- **Support Next generation network deployment** by fast-tracking and simplifying the rollout of 5G and leading in 6G technology development, ensuring that European industries benefit from cutting-edge communication technologies for increased productivity and efficiency. Uniform European frequency allocations and timeframes are key for making the European market attractive and supportive for the development of these capabilities in Europe.
- **Digital skills** are a crucial asset and a precondition for cutting-edge research as well as for the uptake of advanced manufacturing, industrial AI, cloud and edge computing and management of industrial data and cybersecurity. Increased access to digital skills, upskilling and reskilling is needed throughout Europe. Initiatives such as the European Union Cybersecurity Competence Centre (EUCCC) are moving in the right direction and should be further supported.
- **Foster the development of and participation in European Digital Innovation Hubs (EDIHs):** these hubs cover areas, businesses and use cases that are relevant to technology industries (industrial AI, industrial data and data spaces, cybersecurity, semiconductor ecosystem etc. as mentioned in this paper).

[7] Covering inter alia chiplet-based design, heterogeneous integration, multi-chip modules or system-in-package. These innovative packaging technologies require production efficiency in terms of capabilities, capacities and economics.

3. Promote a strong and trusted industrial data ecosystem

- **Support industry-driven data spaces for manufacturing (such as Manufacturing-X and others)** to enhance data usage and value creation, while ensuring interoperability, trust and security. Data spaces must be inclusive and internationally oriented, and their development should be driven by the actual business value they can provide to their participants, including SMEs. Sector-specific solutions must remain possible. Interoperability should be ensured both within and between data spaces for manufacturing, so as not to create silos. The development and networking of data spaces must be encouraged. In the case of regulatory projects, it must be ensured that technical solutions are approved or are based on technical standards (such as OPC UA[8], AAS[9] and others) which are already developed in the respective sectors and can be connected to the corresponding data spaces. Examples of Industry 4.0 include, among others, the Digital Product Passport 4.0 (DPP4.0) or the Manufacturing-X initiative, which can be used to combine compliance with regulatory requirements and new data-driven business models. Data spaces will play a key role in the net-zero transformation of Europe's manufacturing base and they are also expected to be pivotal for the emergence of new AI models and applications in industrial contexts.
- **Promote the Digital Product Passports (DPPs)** as a key element for a strong and trusted product data ecosystem[10]. DPPs should be interoperable and flexible and their data architecture should be designed in a way that protects intellectual property rights (IPR) and trade secrets and supports uptake by European industries. This can be achieved by starting small and focusing on mandatory requirements, while maintaining the possibility for companies that wish to move faster and make more data available through DPPs on a voluntary basis. By doing so, companies and their customers, rather than the regulation alone, could drive DPP development.
- **Foster the industrial metaverse, digital twins and XR development:** promote the development, uptake and interoperability of virtual and augmented reality technologies for industrial applications through soft law instruments and incentives, including by supporting interoperability and the deployment of low-latency cloud and edge infrastructure. Together with the proliferation of new human-machine interactions, by leveraging these technologies manufacturers can enhance productivity, optimise energy and resource usage, reduce waste and minimise environmental impact.
- **Support implementation of the Data Act:** The European Commission should provide clear guidance on the implementation of the Data Act and carefully monitor its impact on the intellectual property (IP) and trade secrets of technology industries. Interplay with other regulations, such as the Data Governance Act, the General Data Protection Regulation (GDPR)[11] and cybersecurity requirements (e.g. the Cyber Resilience Act (CRA)) must be clarified to avoid legal uncertainty and even more litigation. According to the EU Industrial Forum, concerns and challenges around data (e.g. overregulation, IP and cybersecurity) are among the main reasons for the current underusage of advanced manufacturing solutions in Europe. Uniform interpretation and development of balanced market practices should lead the way, learning from the challenges presented by the implementation of the GDPR.
- **Reassess the approach to personal data protection:** the merits of the current European protection regime for personal data should be reassessed, particularly vis-à-vis the growing need to reinvigorate Europe's industrial

[8] Open Platform Communication Unified Architecture (OPC UA). More info.
[9] Asset Administration Shell for digital twins. More info.
[10] See Orgalim's recommendations on the Digital Product Passport in Orgalim's key recommendations on the circular economy, section "*Data requirements must work for both circularity and competitiveness*", 21 May 2024.
[11] General Data Protection Regulation (EU) 2016/679

base and the EU's ties with its allies. Preventing diverging interpretations and enforcement across Member States and a more standardised approach to privacy-preserving technologies would result in significant progress. The European Data Protection Board (EDPB) should prioritise practical guidance to strengthen harmonisation, and to reduce the compliance burden whenever the GDPR text allows. Consideration should be given to adopting a more flexible and risk-based approach to the processing of data (e.g. by simplifying data protection impact assessments) and cross-border data transfers. As regards enforcement and procedural rules, it should be ensured that the one-stop shop mechanism is preserved, and that the due process rights of defendants are guaranteed in the issuance of Adequacy Decisions.

4. Advance industrial artificial intelligence

- **Innovation-friendly and predictable implementation of the AI Act:** we call for the development of harmonised standards, timely publication of Commission guidelines with full support from the industry, involvement of industrial stakeholders and uniform interpretation across the EU as keys to the success of this landmark regulation. The primary target of the Commission should be to foster a predictable, investment and innovation-friendly environment to develop European Industrial AI models and practices. Not implementing these goals in the right way may stifle European innovation in strategic technology. Guidelines, delegated acts and implementing acts should consider sector-specific needs, the reduction of bureaucratic hurdles and clarify definitions in the AI Act and the interplay with other product legislation (e.g. Machinery Regulation). They should also be consistent with the multilateral AI governance initiatives in which the EU is participating (e.g. G7 Code of Conduct). To reduce the compliance risk, we recommend the temporary suspension of fines until guidelines and standards are in place.
- Member States should swiftly set up **AI regulatory sandboxes** as mandated by the AI Act, including specific measures for uptake and innovation by SMEs. The Commission should deliver timely guidance for the setup of sandboxes across Member States. The contribution and recognition of sandboxes in the development stage must be done in a harmonised way to avoid differences in their impact across the single market. Administrative authorities should also be ready to support real-world testing. The analysis and validity of the test plans prepared by companies must be carried out in due time for the measure to be truly effective.
- **Invest in AI Research, skills and uptake:** funds should be allocated to AI research with industrial applications and support education and training initiatives to prepare for AI-powered industries. We advocate for the development of domain-specific AI-models and the exploration of possibilities for open language models and joint European computing resources for SMEs to support them in their AI R&D efforts. According to the Commission, AI is likely to have an overall economic impact on manufacturing and the Industrial Internet of Things (IIoT) in Europe of up to €200 billion by 2030[12].
- **Avoid overregulating industrial AI liability:** in light of the new AI Act and the revised Product Liability Directive (PLD), we call on EU legislators to thoroughly assess the real need for an AI Liability Directive[13] as proposed by the Commission in 2022. The strict liability requirements of AI are already fully covered by the new PLD and some national legal frameworks provide additional layers of liability. Overregulation would stifle innovation and

[12] Industrial applications of artificial intelligence and big data - European Commission (europa.eu)
[13] AI Liability Directive as proposed by the European Commission in 2022.

prevent uptake, which is urgently needed considering that the EU is very far from meeting its own AI uptake target of 75% by 2030, as reported in the Commission's 2023 Digital Decade report[14].

5. Clarify overlaps and ensure efficient governance of cybersecurity rules

- **Consider a one-stop shop for cybersecurity incident reporting:** reporting obligations for significant cybersecurity incidents under the Cyber Resilience Act (CRA) and NIS 2 directive are overlapping to a certain extent. Under GDPR, when such cybersecurity incidents also involve personal data, the reporting obligation is doubled and the same incident must be reported to a different public authority (data protection authority) using a different process and creating an even greater administrative burden for the business, which should rather be focusing its resources on resolving the incident. Going forward, as new cybersecurity rules are implemented, it is essential that enforcement is rationalised and incident reporting simplified, such as by the establishment of a one-stop shop mechanism.
- **Efficient implementation of CRA and NIS2 to avoid burdensome overlap in product-related risk management**: apart from the need to align reporting in both pieces of legislation, Member States should take care not to create further overlap by adding requirements to their adoption of the NIS2 and on products once the CRA is applicable. A possible approach would be the recognition of CE marking under the CRA for products which are part of an entity under the NIS2 in terms of acquisition and installation of products in connection with communication networks and computer systems. For example: IoT products in an assembly line that have the CE marking but have not been substantially modified by this entity (e.g. for integration on the assembly line) could be deemed to be in accordance with NIS2.
- **Repeal the Radio Equipment Directive (RED) Delegated Act (DA)[15] on cybersecurity** when the CRA becomes applicable, particularly for products that fall under the scope of both the CRA and the RED DA. The CRA provides a more comprehensive and neutral approach to cybersecurity, making it more suitable for addressing cybersecurity requirements horizontally. A double regulation would serve no purpose and would only create legal uncertainty without added value for product security. In addition, Orgalim calls for a transitional provision before repealing RED DA. According to industry's experience, regulatory changes without a transition phase are the most challenging as the development of the product, compliance testing and placing on the market have to be taken into account. Therefore, the RED DA should be amended in such a way that compliance with CRA provides RED DA compliance. This would avoid double regulation during the transition from one regulation to another.
- **Maintain the voluntary and technical nature of cybersecurity certification schemes** and, prior to making any such schemes mandatory, ensure that such a policy decision is supported by thorough assessments of the impact on the market of their target products and the wider product ecosystem. As part of the Union Rolling Work Programme for cybersecurity certification[16], schemes related to the critical products listed in Annex IV Cyber Resilience Act should be prioritised. This should then be followed by an assessment as to whether a scheme for Industrial Automation and Control Systems (IACS) would still have added value.

[14] In the Commission's 2023 Report on the Digital Decade, the target of 75% of EU businesses taking up AI by 2030 was only 11% achieved in 2022 2023 Report on the state of the Digital Decade | Shaping Europe's digital future (europa.eu)
[15] Commission Delegated Regulation (EU) 2022/30
[16] Union Rolling Work Programme for European cybersecurity certification | Shaping Europe's digital future (europa.eu)

- **Cooperation in cyber governance:** there should be increased collaboration between Member States and the private sector to address threats and vulnerabilities, with reliable bidirectional information-sharing between public and private parties to avoid fighting cyberattacks in silos and for developing best practices between different industries.
- **Support industry solutions for quantum-safe encryption**: this should include post-quantum cryptography (PQC algorithms), while allowing hybrid usage of classical and quantum-safe encryption methods.

6. Initiate more international digital partnerships

- **Strengthen transatlantic and global partnerships:** the EU should enhance collaboration with the United States and other strategic partners in technology and areas such as semiconductors, AI, data governance and cybersecurity to address common challenges and ensure a level playing field. The EU-US Trade and Technology Council is a good example of how to build further partnerships in this regard.
- **Modernise the digital trade chapters in free trade agreements:** this would enable the free flow of data (personal and non-personal) and avoid forced localisation requirements while ensuring research data security in an open world[17]. Existing trade agreements without relevant provisions on digital trade should be complemented by digital partnerships or digital trade agreements (such as EU-South Korea). The recent digital trade addendum to the EU-Japan Economic Partnership Agreement provides a solid blueprint for this approach, demonstrating an important shared commitment to avoid digital protectionism and arbitrary restrictions on data flows.
- **Support multilateral efforts to facilitate digital trade**: we suggest the inclusion of the G7 Data Free Flow with Trust Initiative and the consideration of further cooperation within the OECD to achieve a workable and predictable framework for international industrial data flows, which will be essential for the net-zero transition of industries as well as compliance (CBAM[18], CS3D[19], CSRD[20], Digital Product Passport, etc.).

[17] For more information, cf. Orgalim's position paper on the new EU research framework programme (FP10), April 2024.
[18] Regulation (EU) 2023/956 establishing a Carbon Border Adjustment Mechanism (CBAM)
[19] Corporate Sustainability Due Diligence Directive, as adopted by the European Parliament on 24 April 2024.
[20] Directive (EU) 2022/2464 on corporate sustainability reporting.

Links to Orgalim publications

Orgalim Policy Agenda and key recommendations for the upcoming EU legislative period 2024-2029

- Orgalim Policy Agenda for a European high-tech manufacturing base for the 2024-2029 legislative cycle
- Orgalim key recommendations on the single market for the 2024-2029 legislative cycle
- Orgalim key recommendations on the circular economy for the 2024-2029 legislative cycle
- Other Orgalim key recommendations for the 2024-2029 legislative cycle will soon be available on the Orgalim website.

Orgalim publications on the digital and green transitions

- Orgalim's Technology at Heart and Technology in Action series present stories showcasing how the technology industries we represent are shaping a future that's good for Europe's environment, economy and society.

Orgalim aisbl
BluePoint Brussels
Boulevard A Reyers 80
B1030 | Brussels | Belgium

+32 2 206 68 83
secretariat@orgalim.eu
www.orgalim.eu
VAT BE 0414 341 438