ZUKUNFT GESTALTEN
Industriellenvereinigung

MAKING THE EU DIGITAL RULEBOOK WORK FOR INDUSTRY

POSITION PAPER OF THE FEDERATION OF AUSTRIAN INDUSTRY ON HARNESSING THE COMPETITIVE ADVANTAGE OF A SIMPLIFIED DIGITAL FRAMEWORK

OVERVIEW

Europe's economic strength and industrial competitiveness increasingly depend on secure and reliable digital foundations. Yet today, the **EU remains heavily reliant on technologies and infrastructures from abroad.** More than 80% of our digital tools, chips, and platforms are imported, mainly from the United States and China.[1] This dependence not only exposes European businesses to external political and legal pressures, such as foreign data access rules, but also weakens Europe's ability to act independently in strategic matters. For Austrian industry, which thrives on stability, innovation, and global integration, **this lack of digital sovereignty is becoming a critical concern.**

While Europe continues to excel in traditional manufacturing sectors, it lags behind global competitors in key future-oriented areas such as artificial intelligence, cloud computing, and advanced semiconductors. **Limited access to venture capital makes it difficult for promising deep-tech companies to grow.** The fact that a significant share of Europe's most innovative start-ups has relocated abroad underscores the **urgent need for better financing conditions, a more integrated market, and flexible rules** that encourage scaling within Europe.

The EU has already responded with an ambitious set of digital laws from artificial intelligence and data governance to cybersecurity and digital infrastructure - **the EU's 2030 Digital Agenda includes an astounding 116 pieces of legislation.** While these initiatives are designed to strengthen Europe's position, their sheer volume and overlapping requirements often create unnecessary hurdles for businesses. Companies face rising compliance costs that tie up resources better invested in research, product development, and innovation.

What the Federation of Austrian Industries is calling for is not less Europe, but better Europe: regulation that is coordinated, proportionate, and geared towards enabling innovation. Rules should be introduced only where genuine gaps exist, and their timelines and standards need to be harmonised so that businesses can plan investments with certainty. Reporting obligations should be streamlined, unnecessary duplication removed, and practical tools such as regulatory sandboxes made widely available to test new approaches in a safe and cost-effective way.

Each of the following chapters of this paper explores specific aspects of Europe's digital transformation that are critical for ensuring a competitive and innovation-friendly industrial landscape. The main takeaways include:

- **Digital Sovereignty:** Europe must strengthen its capacity to act autonomously in the digital sphere by investing strategically in AI, quantum computing, and cloud infrastructures, focusing on "derisking" rather than "decoupling" from global partners.
- **Artificial Intelligence:** The EU's AI Act should ensure trust and safety without stifling innovation. Implementation timelines must be realistic and overlapping obligations across regulatory frameworks need to be streamlined to foster an innovation-friendly AI ecosystem.
- **Data Protection:** A clearer and more coherent data protection system is needed. Harmonizing GDPR, the Data Governance Act, and the Data Act will reduce duplication, provide legal certainty, and balance privacy with innovation.
- **Data Economy:** To build a functioning data-driven economy, Europe must clarify key definitions, protect trade secrets, and align timelines between the Data Act and other regulations. A stable framework with practical guidance is essential for business confidence.
- **Cybersecurity:** The "once-only principle" should apply to incident reporting across overlapping frameworks (NIS2, CRA, GDPR, etc.), ensuring that resources are directed towards real defence rather than compliance duplication.

[1] Report „EuroStack – A European Alternative for Digital Sovereignty", Prof. Francesca Bria, Prof. Paul Timmers und Dr. Fausto Gernone, 2025, im Auftrag der Bertelsmann Stiftung

- **Infrastructure and Components:** Europe needs faster, more flexible funding and approval procedures to strengthen semiconductor production and digital infrastructure, alongside simplified telecom regulation to accelerate gigabit network rollout.
- **Digitalisation in the Workplace:** Instead of introducing new overlapping laws, the EU should align existing frameworks (AI Act, GDPR, and Platform Work Directive) and focus on upskilling and reskilling workers to ensure responsible and competitive AI use in workplaces.

POLICY RECOMMENDATION AT A GLANCE:

The rapid expansion of digital regulation, introduced without sufficient coordination, impact assessment, or clarity on entry-into-force timelines, has led to unnecessary complexity and friction. The Federation of Austrian Industries therefore calls for a reduction of disproportionate burdens and a shift towards a more coherent and agile framework that treats digital not as a stand-alone sector, but as a horizontal driver of resilience, innovation, and growth.

To ease the regulatory load, cut red tape, and unlock Europe's competitiveness by fully leveraging digital transformation, we recommend three overarching steps:

- **Streamline reporting obligations:** Many digital acts impose extensive and overlapping reporting requirements. These should be simplified and harmonised to free up resources for research, innovation, and the rollout of new business models.
- **Withdraw or consolidate outdated or redundant legislation:** Where new frameworks provide clear, harmonised, and enforceable rules, older or overlapping legislative schemes should be removed or consolidated to reduce duplication and administrative burdens for businesses.
- **Align timelines and standards:** The EU has adopted a wide range of interdependent digital regulations, yet their implementation schedules and the availability of harmonised standards are not synchronised. The Commission should coordinate timeframes and introduce flexibility, such as a "stop-the-clock" mechanism, so that obligations apply no earlier than 36 months after the necessary standards are available.

DIGITAL SOVEREIGNTY:

The recent semiconductor shortages, debates over secure 5G suppliers, and the search for GDPR-compliant cloud services have made one fact clear: **Europe cannot afford to remain dependent on external providers for critical digital technologies.** Ensuring digital sovereignty has therefore become a central priority. For Austria, it is not about striving for complete self-sufficiency, but about the ability to use and assess third-party technologies in a secure, transparent, and controllable way.[2] **In practice, this means giving companies, institutions, and individuals the tools and competences to act independently and self-determinedly in the digital world.**

Digital sovereignty should be understood in a broad sense: it is not only a question for governments, but also for businesses and society as a whole. Companies need to be able to design and produce key digital products and services within Europe, evaluate the risks of foreign technologies, and integrate trusted external solutions responsibly. This balanced approach – **more about "derisking" than "decoupling"** – recognizes that global cooperation will remain essential, but also that Europe must strengthen its own capacity to innovate and compete.

Experts estimate that building a sovereign digital ecosystem will require at least €300 billion in investment and a long-term effort of ten years or more.[3] **Priority areas include artificial intelligence, quantum computing, and cloud infrastructures.** Far from being a burden, these investments should be seen as an opportunity: they allow Europe to foster innovation that reflects its own values and to create credible alternatives to dominant providers from the U.S. and China.

> "Europe's cloud computing market was worth around €87 billion in 2022 and is estimated to reach €200 billion by 2028. The three US-based cloud 'Hyperscalers' account for 65% of the whole cloud computing market."
>
> - CEPA, 2025

For Austrian industry, digital sovereignty is both a necessity and a chance. A resilient and independent European digital ecosystem strengthens competitiveness, reduces vulnerabilities in times of geopolitical tension, and secures long-term prosperity. At the same time, there is a risk that misguided policies could result in protectionism or fragmentation. **It is therefore vital to pursue sovereignty without closing Europe off from global innovation and value chains.**

The path forward requires close cooperation between policymakers, businesses, and research institutions. Only through a joint effort can Europe secure the skills, technologies, and frameworks needed for digital independence.
Europe must remain open and globally connected, while at the same time building the capacity to act autonomously, safeguard critical infrastructures, and ensure that no one is left behind in the digital transformation.

ARTIFICIAL INTELLIGENCE:

Artificial intelligence (AI) is a decisive technology for Europe's competitiveness and for Austria's industrial strength. A strong and innovation-friendly AI ecosystem will help companies adapt to global challenges, strengthen resilience, and secure long-term growth. Yet many Austrian firms see current regulatory developments as a major investment hurdle. While the United States is lowering barriers to encourage AI deployment, the EU risks burdening its businesses with excessive bureaucracy. **If regulation becomes too rigid, companies will be forced to spend resources on compliance rather than on innovation, slowing down Europe's ability to compete globally.**

THE AI ACT:

The AI Act, as the EU's flagship regulation, must strike the right balance. Its goal of ensuring trust, transparency, and safety is shared by industry. However, the current approach risks overregulation. For instance, products already covered by detailed EU safety frameworks (such as medical devices or machinery) should not be subjected to overlapping AI obligations. **Sectoral rules are the right place to address sector-specific risks, rather than duplicating requirements in the AI Act.**

[2] Definition used by the Austrian government: digital sovereignty is understood as 'the sum of all abilities and possibilities of individuals and institutions to be able to fulfil their role(s) in the digital world independently, self-determinedly and securely'. Accordingly, digital sovereignty enables the 'ability to act in the (digital) world in a self-determined manner and to resist the will of other actors.'
[3] Report „EuroStack – A European Alternative for Digital Sovereignty", Prof. Francesca Bria, Prof. Paul Timmers und Dr. Fausto Gernone, 2025, im Auftrag der Bertelsmann Stiftung

Another pressing concern is the timeline for implementation. The guidelines for high-risk AI systems are expected in early 2026, with obligations applying only months later. This leaves companies with little time to adapt. Standards for high-risk requirements are also delayed, creating legal uncertainty. Without adequate standards in place, firms are likely to hold back investments. **To ensure a workable transition, Austrian industry calls for at least a 24-month extension of the implementation deadlines** for the high-risk requirements in Annex I and Annex III, as well as a **"stop-the-clock" mechanism** until the necessary standards are available.

Products listed in Annex I present some of the lowest fundamental rights risks amongst systems covered by the AI Act. Yet they face some of the most extensive compliance obligations. This mismatch cuts against the risk-based foundation on which the AI Act is built. **For general-purpose AI (GPAI), clear rules and a grace period for the new Code of Practice are also essential.**

Consistency across Europe's legal framework is equally critical. Currently, overlapping requirements in the AI Act, the GDPR, and the Data Act risk creating contradictions. A coherent approach that aligns data protection, transparency, and data-sharing obligations would provide legal certainty and reduce unnecessary costs. **Clear guidance from supervisory authorities, particularly on AI use in sensitive areas such as human resources, would further support practical implementation.**

Finally, documentation obligations for high-risk AI systems need to be proportionate. As currently drafted, Annex IV demands extensive technical files (texts, system documentation, hardware requirements, possibly images of hardware components, design specification) that risk overwhelming companies. **Providing standardized templates and simplifying documentation where no personal data is involved would help companies comply without stifling innovation.**

For Austrian industry, the message is clear: **AI must be regulated in a way that protects fundamental rights while enabling innovation.** A business-friendly, coherent, and realistic framework is the only way for Europe to build a sovereign AI ecosystem that can compete globally and deliver tangible benefits to citizens and companies alike.

DATA PROTECTION:

Effective and practicable data protection is a cornerstone of Europe's digital economy. **For Austrian industry, strong rules that protect the rights of individuals while at the same time enabling innovation and data-driven business models are essential.** Yet the current regulatory environment is complex, fragmented, and often burdensome. Companies face overlapping obligations under the GDPR, the Data Governance Act (DGA), and the Data Act – a situation that creates legal uncertainty, raises costs, and risks slowing down digital transformation.

CALL FOR CLEAR LEGAL DEFINITIONS:

One of the biggest challenges is the unclear distinction between personal, mixed, and non-personal data. Today, businesses must comply with two parallel regimes (one for personal and mixed data sets, and one for all other data), with different rules for personal and non-personal data. On top of that, the obligation to assess whether foreign government data requests comply with EU or national law places a heavy responsibility on companies and risks leading to de facto data localisation. **Austrian industry therefore calls for a clearer and simpler system: Articles 31 DGA and Article 32 of the Data Act should be deleted, and countries deemed adequate under the GDPR should automatically be considered secure for non-personal data transfers as well.**

Legal clarity on anonymization is another urgent need. The GDPR provides no binding definition of what counts as "anonymized data," and interpretations differ widely between authorities. This uncertainty discourages the use of anonymized data sets, which are critical for research, innovation, and industrial applications. **Practical guidelines and harmonized standards are necessary to reduce bureaucracy and give companies confidence that their anonymization processes are compliant.**

"PRIVACY BY DESIGN" VERSUS "ACCESS BY DESIGN"

Equally important is addressing the interplay between the GDPR and the Data Act. While the GDPR is based on "privacy by design," the Data Act promotes "access by design." These principles can conflict when product or service data contains personal information. **In practice, companies are unsure about who qualifies as a controller, who must inform users, and who bears liability if datasets are misclassified.** To resolve these issues, the Data Act should provide a clear legal basis for data sharing under Article 6(1)(c) GDPR, and Recital 7 – which denies such a basis – should be removed. Standardized technical tools for automated data classification, along with certification schemes, could help businesses manage compliance effectively.

EXTENSION OF REPORTING DEADLINES:

Another important issue are the short reporting deadlines in the GDPR. In accordance with Article 33, data breaches are to be reported within 72 hours. **This deadline is often inadequate in practice, as it fails to account for weekends, public holidays or internal organisational processes.** In this regard, the principles of EU Regulation 1182/71, which stipulates the rules applicable to periods, dates and time limits, should be taken into consideration: the regulation stipulates that legal deadlines must account for a minimum of one full working day and are to be extended if they fall on non-working days. Consequently, the Federation of Austrian Industries proposes an extension to the reporting deadline to 120 hours, on the basis that this reflects the maximum duration of an extended holiday period (e.g. Christmas). The purpose of this extension is to facilitate a comprehensive internal evaluation and a coordinated response.

For Austrian industry, the objective is not to weaken data protection, but to align it with Europe's broader digital agenda. A coherent and risk-based approach, supported by clear guidance from the European Commission and the European Data Protection Board (EDPB), is needed to balance privacy, innovation, and competitiveness. By reducing duplication, clarifying responsibilities, and streamlining data sharing rules, Europe can strengthen trust in digital technologies while ensuring that its industries remain globally competitive.

DATA ECONOMY:

A thriving data economy is key to Europe's competitiveness and resilience. **For Austrian industry, access to and use of data along value chains is central to innovation, efficiency, and new business models.** To achieve this, Europe needs coherent and accessible structures that make data sharing practical and secure. Today, however, companies face a patchwork of overlapping rules and unclear definitions that create legal uncertainty and unnecessary costs.

The Data Act, as the cornerstone of the EU's data strategy, introduces new rules on data sharing, access, and contractual practices. While its ambition to create a European single market for data is welcome, its one-size-fits-all approach risks slowing down rather than enabling innovation. Unclear definitions of basic terms such as "data holder" or "user," and contradictions with existing frameworks such as the GDPR, the Trade Secrets Directive, or competition law, leave companies unsure of their rights and obligations. **This uncertainty is particularly problematic for Austrian firms - many of them mid-sized, export-oriented manufacturers - that depend on legal clarity to plan investments.** The concern is that companies may be incentivized to design their products in a more data-efficient manner, thereby undermining the very objectives the Data Act aims to achieve.

PROTECTION OF TRADE SECRETS

A central concern is the protection of trade secrets and intellectual property. As currently designed, the Data Act could force businesses to share sensitive information with competitors, potentially undermining security and innovation. Safeguards must go beyond governance processes and provide real protection, including recognition of cybersecurity risks. Exemptions for trade secrets should be clear, proportionate, and enforceable.

Equally important is the issue of timelines and overlaps. The Data Act is applicable as of September 2025, but manufacturers will also need to comply with the Cyber Resilience Act from 2027 and with NIS2 obligations. These overlapping regimes create conflicting requirements, particularly when data sharing obligations interact with product security rules. **Austrian industry therefore calls for realistic implementation schedules, including grace periods and, where necessary, a "stop-the-clock" mechanism until guidance and standards are available.**

To make the European data economy workable in practice, the following steps are needed:

- Establish a central glossary and harmonized definitions across EU digital laws.
- Ensure that safety and security rules prevail over data sharing obligations in case of conflict.
- Give data holders a clear right to use and share data for purposes such as quality control, diagnostics, or R&D, rather than placing all power with users.
- Delete or revise unnecessary provisions regarding unfair contractual terms in B2B-data contracts, which restrict contractual freedom (Articles 13(4) and (5)).
- Extend the transition period of the Data Act by at least two years or reassess the regulation 18 months after its entry into force to address practical problems.

Finally, the European Commission must work closely with industry to provide clear guidance on implementation and strengthen the European Data Innovation Board (EDIB) to ensure harmonisation across Member States. Only with a stable, predictable, and business-friendly framework can the EU's data strategy succeed in creating common European data spaces while supporting industrial competitiveness.
The Federation of Austrian Industries' priority is to build a European data economy that fosters innovation and collaboration, while protecting sensitive know-how and keeping compliance costs manageable.

CYBERSECURITY:

For Austrian and European industry alike, cybersecurity has become a matter of strategic survival. **Nearly half of all businesses in Europe suffered at least one successful cyberattack in 2024,** ranging from ransomware to data theft and industrial espionage. At the same time, companies are faced with a fragmented regulatory environment, in which overlapping rules and reporting obligations threaten to drain resources away from actual defence and resilience.

The EU has adopted several important legislative initiatives - NIS2, the Cyber Resilience Act (CRA), the CER Directive, GDPR, and DORA - each with their own reporting requirements. **In practice, one incident can trigger multiple parallel obligations.**

Example:

If a physical intrusion in an energy facility (CER) compromises data integrity (NIS2) due to a known product vulnerability (CRA) and involves personal data (GDPR), the operator must report separately under all four frameworks. Timelines further complicate the picture: NIS2 requires notification within 24 hours and more detailed reports within 72 hours; GDPR sets a 72-hour deadline for personal data breaches; the CRA requires manufacturers to report vulnerabilities and severe incidents within 24 and 72 hours, followed by a final report within 14 days. Each regime has its own addressees, formats, and thresholds, making compliance complex and costly.

To ensure that scarce cybersecurity resources are used for prevention and mitigation rather than paperwork, Austrian industry calls for the implementation of the "once-only principle". A single incident report - submitted to one competent authority - should suffice to meet obligations across all relevant frameworks. Interim reports "upon request" should only be required if the competent authority can demonstrably act upon the information to support mitigation.

The coexistence of the Cybersecurity Act (CSA), which introduced voluntary certification schemes, with NIS2 and CRA creates further uncertainty. Businesses face the risk of redundant audits and inconsistent requirements. **Austrian industry therefore urges that CSA certifications, where voluntarily obtained, be recognised as evidence of compliance with overlapping legal requirements.** At the same time, the principle of proportionality must be upheld: low-risk products should remain subject to self-assessment modules, while high-risk categories can require stricter conformity procedures. Future delegated acts under CRA must avoid unnecessary expansion of certification requirements.

Equally problematic is the treatment of affiliated companies under NIS2. Article 22(5) currently treats subsidiaries within a corporate group as independent entities, requiring them to meet the same obligations as external actors. For Austrian industrial groups with centralized IT and cybersecurity functions, this creates unnecessary duplication. Companies serving only affiliates should be exempt from Article 22(5), with group-wide management and harmonized documentation accepted as compliant practice.

While the CRA is a major step forward in securing products with digital elements, its implementation raises several practical issues for industry:

- **Transition period:** The CRA relies on harmonized European standards as the legal basis for compliance. These standards need time to be developed with industry input. A minimum of 36 months between publication of standards and the end of the transition period is necessary for companies to adapt.
- **Support period obligations:** CRA requires manufacturers to provide free security updates throughout the entire lifetime of a product. However, industrial products often last decades, while their digital components follow much shorter innovation cycles. Austrian industry calls for a clear distinction between physical lifetime and digital lifetime, allowing manufacturers to define a reasonable support period for digital elements.
- **Reporting obligations:** Article 14 requires manufacturers to issue an early warning notification of an actively exploited vulnerability within 24 hours of becoming aware of it, a detailed vulnerability notification within 72 hours, and a final report no later than 14 days after a corrective or mitigating measure is available. In addition, a manufacturer must notify any severe incident having an impact on the security of the product with digital elements (cf. Article 14 (3 and 4)). This duplicates NIS2 and GDPR obligations. A streamlined model with two reports only (initial within 48 hours, final within 14 days) would be more workable. Reporting should ideally be consolidated through ENISA's platform.
- **Everlasting monitoring obligations:** Article 69.3 requires monitoring and reporting obligations indefinitely, even for legacy products launched before CRA. This is disproportionate. Obligations should expire five to ten years after the end of the declared support period, providing predictability without undermining resilience.

As a directive, NIS2 is implemented differently across the 27 Member States. Some classify entities in one tier, others in three; some extend scope, others stick to the minimum. This leads to companies facing different compliance requirements across jurisdictions. A uniform EU-wide approach is urgently needed.

Incident reporting under Article 23 of NIS2 is also excessive. In case of a significant cyber security incident, **companies must currently submit up to five reports per incident—initial, detailed, interim, progress, and final.**[4] Austrian industry proposes a simplified structure:

- Early warning within 48 hours, limited to essential information;
- One interim report upon request of the competent authority, including relevant status updates;
- Final report one month after resolution, detailing root cause, impact, and mitigation and, where applicable, the cross-border impact of the incident.

Such simplification would reduce administrative costs and allow cyber teams to focus on real defense. Standardized templates and unambiguous definitions would further support compliance.

Cybersecurity is a cornerstone of Europe's digital sovereignty, but today's regulatory complexity threatens to undermine resilience rather than enhance it. **For Austrian companies, the priority is clear: reduce duplication, harmonize definitions and timelines, and allow resources to flow into protection and innovation rather than into fragmented compliance.** A coherent, simplified framework—based on the once-only principle, proportionality, and harmonization—will strengthen both Europe's cyber resilience and the global competitiveness of its industry.

INFRASTRUCTURE AND COMPONENTS:

Robust digital infrastructures form the backbone of modern industry. Data centres, semiconductors, submarine cables, and high-speed networks are indispensable for production, innovation, and competitiveness. Yet Europe remains highly dependent on non-European providers. U.S. cloud providers dominate the market, only 11% of global semiconductor output is produced in Europe, and control over submarine cables largely rests outside EU hands. Combined with extraterritorial rules such as the U.S. CLOUD Act or Chinese data regulations, these dependencies expose European companies to legal uncertainty, supply bottlenecks, and geopolitical pressure. **For Austrian industry, this translates into real risks for operational continuity and long-term competitiveness.** To secure digital sovereignty, the EU must build up strategic capacities in critical hardware components. Semiconductor shortages in recent years have shown how vulnerable Europe is in sectors ranging from automotive to machine building.

> 60% of the world's semiconductors and more than 90% of the most advanced semiconductors are still produced in Taiwan.
>
> - Cigref, 2025

Despite the €43 billion package of measures under the European Chip Act, European companies are not playing a significant role in the development of high-performance computing (HPC) and AI chips. Specialised chips are essential for technologies such as AI, quantum computing, and edge applications, all of which are vital for Austria's export-oriented industries. **While initiatives such as the European Chips Act and IPCEIs are steps in the right direction, the current approval and funding procedures are far too slow and bureaucratic.** In a sector with rapid innovation cycles, waiting two years for a grant decision means losing ground to global competitors. Funding processes must therefore become faster, more flexible, and better aligned with industrial realities. At the same time, nurturing talent and investing in semiconductor R&D are crucial for strengthening Europe's role in high-value segments such as quantum chips and AI hardware.

Connectivity is another decisive pillar. Without gigabit networks, Austrian companies cannot deploy next-generation digital solutions at scale. The Gigabit Infrastructure Act (GIA), entering into force in November 2025, aims to speed up broadband rollout, yet in

> 90% of EU data is stored on Non-European infrastructure..
>
> - Cigref, 2025

[4] In case of a significant cyber security incident, companies must fulfil three to five reporting obligations. The first report must be submitted within 24 hours after becoming aware of the incident and the second must follow within 72 hours after becoming aware of the incident. Upon request of a CSIRT or, where appropriate, the competent authority, can request an interim report on relevant status updates. Moreover, companies have to submit a final report no later than one month after the submission of the notification of the incident. In case of an ongoing security incident at the time of submission of the final report, the organisation concerned must submit a progress report at that time and a final report within one month of the handling of the security incident.

practice it risks creating new red tape, for example through additional notification obligations. What is needed instead are fully digital approval procedures and binding tacit approval rules to drastically shorten timelines. Equally important is the Digital Networks Act (DNA), which must reduce outdated regulatory burdens in the telecom sector and create conditions for sustained investment. **Only if Europe's communications infrastructure is modern, resilient, and profitable will industry have reliable access to the digital services it needs.**

For Austria, an integrated industrial and digital policy approach is essential: **strengthening semiconductor production, supporting critical infrastructure investments, and ensuring predictable, business-friendly rules for network operators.** A simplified, well-coordinated European framework will not only enhance connectivity and resilience but also attract private investment and safeguard Europe's competitiveness in the global race for digital leadership.

DIGITALISATION IN THE WORKPLACE:

The digital transformation of the workplace offers enormous opportunities for Austrian industry, from productivity gains to improved working conditions. Artificial intelligence (AI) and algorithmic tools are already shaping processes such as task allocation, resource planning, and skills matching. **However, the regulatory landscape governing their use has become increasingly fragmented.**

Currently, three overlapping legal regimes apply: the AI Act, the General Data Protection Regulation (GDPR), and the Platform Work Directive (PWD). Each addresses similar issues (safety, fairness, and data privacy) but from different perspectives. As a result, companies face multiple and sometimes conflicting obligations, such as parallel impact assessments, transparency reporting, and documentation requirements. This creates legal uncertainty and discourages innovation.

The problem is aggravated by the fact that the PWD will be transposed differently across 27 Member States, leading to divergent obligations on the use of algorithms. Moreover, many of its provisions duplicate or even contradict existing GDPR rules, for example in the areas of data portability, transparency, or bans on biometric checks. The result is regulatory complexity rather than clarity.

ADDING EVEN MORE REGULATION:

On top of this, the European Parliament is discussing adding a new directive on "AI at Work". **For Austrian industry, what is needed is not another directive but a streamlined and coherent framework that avoids duplication and ensures predictability.** The EU already has robust safeguards in place through the AI Act, GDPR, and existing labour and safety laws. Rather than adding layers of regulation, policymakers should focus on better coordination and practical implementation. This would also be consistent with the EU's political commitment to reduce reporting obligations for businesses.

To make regulation more workable, we propose:

- Cross-referencing and alignment between the AI Act, GDPR, and PWD, applying the "once-only principle."
- A unified risk assessment framework acceptable under all three instruments.
- Explicit alignment of PWD provisions (e.g., Articles 7–11) with corresponding GDPR rights and timelines.
- Joint guidance from supervisory bodies (EDPB, AI Office, Labour Inspectorates) to provide practical clarity.
- A stronger focus on up- and reskilling, ensuring workers and businesses can fully benefit from AI in the workplace.

The European Union already has a robust framework of legislation that governs the use of AI and protects workers' rights, including the AI Act, the General Data Protection Regulation (GDPR), the Platform Work Directive and other existing and occupational safety laws. These frameworks provide clear obligations for transparency, accountability, and non-discrimination, ensuring that AI systems used in the workplace are deployed responsibly. **Overlaying this with a new, specific directive risks creating legal uncertainty, duplicating requirements, and increasing compliance burdens without adding meaningful protections.** In a global context where the EU is already striving to close the innovation gap with other major economies, placing extra regulatory hurdles on AI deployment in the workplace could further weaken Europe's position.

CONCLUSION:

For Austrian and European industry, a simplified and coherent digital rulebook is essential to strengthen competitiveness while safeguarding openness and global cooperation. **Europe must position itself as a leader in emerging technologies** such as quantum, AI, and semiconductors, aligning digital ambitions with competition policy to advance open strategic autonomy, **without slipping into protectionism that would deter innovation, talent, and investment.**

Future regulation should be evidence-based, risk-oriented, and proportionate, introduced only where genuine gaps exist. Rules must be clear, technology-neutral, and consistent with existing frameworks, supported by thorough impact assessments to ensure predictability for businesses.

At the same time, Europe's digital transition can only succeed if it is underpinned by a strong skills agenda. Addressing shortages in digital talent, expanding education and training pathways, and fostering digital literacy for all citizens will ensure no one is left behind. Austria, as an innovation-driven economy, has a particular interest in attracting skilled workers and enabling its workforce to seize the opportunities of the digital age.

Policymakers, businesses, and researchers must therefore work hand in hand to build a stable and sovereign digital ecosystem. One that empowers industry, drives innovation, and secures Europe's competitiveness on the global stage.