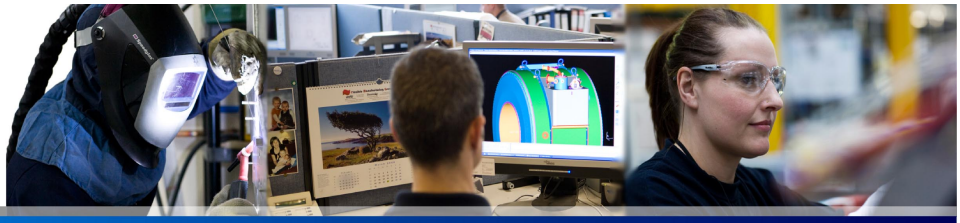
EUROPEAN FORUM for MANUFACTURING



EUROPE'S INDUSTRIAL AI MOMENT
Simplifying Data Rules for Advanced Manufacturing

Tuesday 10 November 2026

18h00 Cocktail - 18h30 Dinner Dialogue
European Parliament Members' Salon - Spinelli Building

Organised in partnership with Orgalim – Europe's Technology Industries





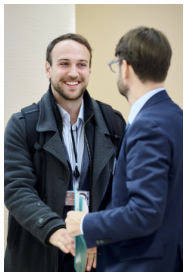












INTRODUCTION BY THE PARLIAMENTARY HOST

Maria GRAPINI MEP (S&D, Romania) Vice-Chair of the Internal Market and Consumer Protection Committee



Ladies and gentlemen, dear colleagues, representatives of the European Commission and European industry, it is a great pleasure to welcome you this evening and to host this European Forum for Manufacturing Dinner Dialogue.

I would like to begin by emphasising that I have always been a strong supporter of European industry. Having spent many years working in industry myself, I firmly believe that a strong manufacturing sector is essential to the strength of our Single Market and to Europe's competitiveness.

Europe needs a robust industrial base, and it is our responsibility as policymakers to ensure that businesses have the conditions they need to invest, innovate and compete.

As Vice-Chair of the European Parliament's Committee on the Internal Market and Consumer Protection (IMCO), I attach particular importance to maintaining an open and constructive dialogue with industry.

- A Timely Debate on Europe's Digital Framework
  Our discussion takes place at a particularly important moment.

  Earlier today, the IMCO Committee voted on its Opinion concerning the Digital Omnibus. Later this week, Artificial Intelligence will also feature in discussions at an informal meeting of the European Council convened by President António Costa. At the same time, the European Commission has identified advanced manufacturing as one of the priority sectors in which industrial AI can have a significant impact.

  These developments demonstrate the importance of ensuring that Europe's digital regulatory framework supports industrial innovation and competitiveness.

  We must also recognise the costs that complex legislation can impose on businesses. The Draghi report has highlighted the significant compliance costs associated with European regulation. Estimates concerning GDPR compliance suggest costs of up to €500,000 for small and medium-sized enterprises and up to €10 million for large organisations.

  For companies, particularly SMEs, these costs can represent a considerable burden.
  This is why the Digital Omnibus represents an important opportunity to simplify the rules and make them easier to implement.

- Simplification is essential.

  When legislation becomes too complex and bureaucratic, compliance costs increase and businesses face additional obstacles to their development. We need rules that are clear, practical and proportionate, while continuing to provide the necessary protections.

- Making Data Rules Work for Manufacturers
  Let me give a practical example.

  A connected industrial machine can generate valuable information about its performance and operation. At the same time, it may also collect information relating to the people who operate

it. Manufacturers therefore need clear rules governing how they can access and use these different categories of data. This is not always straightforward, particularly when new legislation is introduced.

The Commission is working towards simplification, but we must ensure that the implementation of these rules is equally practical and accessible for businesses operating within the Single Market. This is especially important in the context of international competition.

European manufacturers face increasing competitive pressure from other parts of the world. We must ensure that our regulatory framework does not place them at an unnecessary disadvantage. The ongoing debate on European industrial competitiveness, including discussions around the concept of 'Made in Europe' and European preference, is therefore particularly relevant. These discussions are far from concluded, and the views of industry are essential in helping us determine the right approach.

- From Legislation to Practical Implementation
  I hope our discussions on the Data Act and General Data Protection Regulation [GDPR] will help clarify what these rules mean for manufacturers in their everyday operations.

  It is one thing to develop legislation in theory. It is quite another to understand how that legislation works in practice. For me, this distinction is fundamental.

  We need to understand the real impact of European rules on industrial companies, their operations, their costs and their ability to innovate.

  Your contributions are particularly valuable because they provide the practical experience that policymakers need when considering future legislative proposals and recommendations. And this discussion comes at a time when several other important initiatives affecting European industry are being considered.

  We are looking at new measures concerning competitiveness, industrial development, access to markets and the implementation of European legislation. Each of these initiatives must be assessed not only in terms of its objectives but also in terms of its practical consequences for manufacturers.

  I therefore encourage you to share your experiences and concerns openly.
  Europe's industrial future depends on our ability to develop policies that respond to the realities faced by businesses.

Conclusion
I attach great importance to the outcomes of this dialogue and look forward to hearing the conclusions and recommendations arising from your discussions. Let me conclude by reiterating my strong commitment to European industry. A competitive and innovative manufacturing sector is essential for a strong Europe and a successful Single Market.

INDUSTRY OPENING REMARKS

Daniel Wennick, ORGALIM, Policy Director



Thank you, MEP Maria Grapini, for hosting us in the European Parliament, and thank you to the European Forum for Manufacturing for organising this event with Orgalim.

Are We Ready To Use Our Industrial Data?
Let me begin with a simple question: Europe has world-class factories, machines and engineering know-how. We generate enormous quantities of industrial data every day.

But are we actually allowing European companies to use that data to build the next generation of industrial AI?

I will briefly do five things:

- Explain the opportunity
- Introduce Orgalim
- Describe the regulatory challenge
- Give concrete examples, and
- Set out what we believe Europe should do next.

- The Opportunity: Europe's Industrial AI Moment
  Industrial AI is not an abstract promise. It is already helping manufacturers optimise production and energy use, improve quality control, detect defects, anticipate maintenance and reduce costly downtime.

  Europe starts from a position of strength. We have a powerful industrial base and world-leading manufacturing know-how. Advanced manufacturing is one of the sectors where Europe has both high potential and large volumes of valuable data.

  The essential ingredient is clear: companies must be able to use data safely, confidently and at scale.

- Whom Orgalim Represents
  Orgalim represents Europe's technology industries: companies producing machinery, electrical equipment, electronics, automation and other technologies that underpin Europe's industrial economy.

  Our members are at the centre of the digital transformation. Their machines are connected. Software is embedded in products and production. Industrial data increasingly supports new services, better products and more efficient factories.

  For these companies, the debate is therefore not about whether data and AI matter. It is about whether Europe creates workable conditions for companies to **innovate here**.

- The Problem: Good Objectives, Growing Complexity
  Europe has built an extensive framework for the digital economy. The objectives are important: protecting personal data, strengthening cybersecurity, increasing access to data and supporting trust.
  But companies do not apply each law in isolation. They must manage the interaction between GDPR, the Data Act, cybersecurity rules and sector-specific requirements. The cumulative complexity creates uncertainty, cost and delay.

  And uncertainty has a very practical consequence: data that could support innovation, efficiency and new AI applications may simply remain unused.

- Two Real Problems For Manufacturers
  - First, consider GDPR.
    Data generated by a machine on a factory floor may appear non-personal. Yet it can sometimes be linked indirectly to an employee, for example by indicating who operated a robotic arm. A low-risk industrial dataset can then trigger the full complexity of personal-data rules. The intention is legitimate, but the result can be disproportionate.

    The compliance burden is significant. Estimates cited in the Draghi report reach up to €500,000 for SMEs and up to €10 million for large organisations.

  - Second, consider the Data Act.
    Its aim of increasing data sharing and interoperability is welcome. But manufacturers may have to renegotiate existing contracts, face obstacles to sharing industrial data with trusted research partners, and risk disclosing commercially sensitive information or trade secrets.

    If companies cannot protect the know-how behind their products, they will be less willing to share data, invest in connected services or develop industrial AI in Europe.

- Our Solution: Simpler, Proportionate And Trusted Rules
  This is why Orgalim supports ambitious simplification through the Digital Omnibus, and why the same practical ambition should extend to the wider digital and cybersecurity framework.

  Our position is not a call for deregulation.

  On GDPR, we do not want less privacy. We want rules that are proportionate to the actual risk, clearer to understand and easier to apply.

  On the Data Act, we do not want less data sharing. We want manufacturers to be able to use the data they already generate, work with trusted partners and protect the know-how that keeps them competitive.

  In short, simplification should do three things:
  - reduce unnecessary legal uncertainty,
  - protect privacy and commercially sensitive information, and
  - make responsible data use easier.

Conclusion: Turning Industrial Strength Into AI Leadership

The industrial data economy can only develop if people and companies trust it. Trust requires privacy, cybersecurity and proper protection of trade secrets. But trust also requires rules that companies can understand and implement in practice.

Europe already has the factories, the engineering expertise and the data. Our task now is to create a regulatory environment that allows those strengths to become industrial AI leadership.

That is the central question for tonight's discussion: how can we simplify the rules so that European companies can use data responsibly, innovate faster and remain competitive?

I am very pleased that we have representatives from the Parliament, the Commission and industry around the table to address that question together.

MEP VIEWS

Inese VAIDERE MEP (EPP, Latvia) Internal Market and Consumer Protection Committee, Industry, Research and Energy Committee



Data is a strategic resource. It can help businesses improve efficiency, develop new AI applications and create innovative products and services.

But to unlock this potential, companies must be able to access and use this data without facing unnecessary regulatory obstacles. This is precisely why the discussions on the Data Act and the Digital Omnibus are so important. Unfortunately, the Council - the Member States have pushed back against most of the proposed measures within the Omnibus but we in the European Parliament want to maintain a level of ambition.

As a Member of IMCO [Internal Market and Consumer Protection Committee] and ITRE [Industry and Research Committee], I see that finding the right balance between simplifying the rules, supporting innovation and safeguarding fundamental rights is not an easy task.

However, I believe that we should have concrete guiding principles:

- We Need To Make The Regulatory Framework Simpler.

  As we prepare for the ITRE vote in February, I see that most of us want to eliminate overlapping and unnecessary requirements, facilitate access to anonymised data for

European companies, encourage data sharing and make legislation easier to apply in practice, especially for the European SMEs. This is the right approach.

Let me give a practical example of where we need to make progress.

I welcome the proposal to establish a Single-Entry Point for reporting cybersecurity incidents and data breaches. It should make reporting simpler and reduce administrative burdens for businesses.

However, let us be frank: one portal alone will not solve the problem of excessive bureaucracy and uncertainty. We need to go further. We must better align reporting requirements and reduce unnecessary duplication. We should ask ourselves what information businesses really need to provide, how often and to whom.

- We Must Look At Simplification As A Matter Of Europe's Economic And Technological Sovereignty.

  As a member of the International Trade Committee, I also look at this proposal through the lens of geopolitics.

  We must be able to develop artificial intelligence and other digital services here in Europe, with European companies leading the way and bringing innovations, at least in key sectors. Being able to train AI models in Europe is essential. If European manufacturers cannot make effective use of the data they generate, they will struggle to compete with companies in the United States and China.

  Reliable data and trustworthy artificial intelligence models are not only essential for economic growth; they are also crucial for Europe's economic security and the safety of our citizens in this increasingly volatile world.

- The Third Issue I Want To Emphasise Is Legal Certainty.

  Commission proposals sometimes, despite good intentions, are lacking in clarity and so can create more problems than they solve.

  Protecting people's personal data and or trade secrets remains essential. Most of my colleagues agree on this, although we may have different opinions on how best to achieve it. In my view, the problem is not the protection of private and business data, but the unclear, overlapping and unnecessarily burdensome way in which some rules are applied.

  To conclude, our objective must be real simplification – not simply changing the wording of laws or moving obligations from one place to another. Less paperwork, lower administrative costs and more time and resources for European businesses to innovate, grow and compete globally.

Lukas MANDL MEP (EPP, Austria) Legal Affairs and Civil Liberties Committee, Justice and Home Affairs Committee
(*points noted from the presentation*)



I believe we are now working in a more favourable political environment for European industry and competitiveness than in previous parliamentary mandates. However, we must accelerate our efforts to ensure that this change translates into tangible economic benefits.

Let me begin with the Omnibus packages. I deliberately use the term deregulation rather than simply simplification, because I believe Europe needs to go further than reducing administrative complexity. We must remove unnecessary regulatory burdens, reduce bureaucracy and give businesses greater freedom to operate, invest and innovate.

Having participated in negotiations on several Omnibus initiatives, particularly Omnibus IV, I see this as an important step towards restoring Europe's competitiveness. However, deregulation alone is not enough. It removes obstacles, but we must also create the conditions for economic growth and investment.

Artificial intelligence is a particularly relevant example. The European Union was among the first jurisdictions to establish a comprehensive regulatory framework for AI. This was an important achievement, and I recognise that appropriate rules are necessary. We must continue to develop and adapt this framework as technology evolves.

But regulation alone will not make Europe competitive in artificial intelligence.

We have outstanding talent, researchers, developers and innovative companies. We are capable of developing new technologies and creating successful businesses. Yet too often, when these companies reach the stage where they need to scale up, they leave Europe.

Europe must not only be a place where innovation begins. It must also be a place where innovation can grow, attract investment and generate prosperity.

To achieve this, we need a better business environment, stronger capital markets, less unnecessary regulation and more favourable conditions for companies to expand.

Investment is therefore essential. I strongly support the European Commission's Savings and Investments Union initiative, which can help channel European savings into productive investment, supporting businesses, innovation and economic development.

The proposed 28th regime for companies could also contribute to a more favourable environment by reducing legal and administrative fragmentation and making it easier for European businesses to operate and grow across the Single Market.

Ultimately, we need both deregulation and stronger investment if we are to restore Europe's competitiveness.

Our objective must be to create a Europe where innovative companies can develop, scale up and compete globally, supported by a regulatory environment that encourages

entrepreneurship and technological progress rather than placing unnecessary obstacles in their way.

We have the talent and the technological capabilities. We must now ensure that Europe provides the conditions for them to succeed.

DATA ACT

EUROPEAN COMMISSION KEYNOTE SPEECH



Bjoern Juretzki, EUROPEAN COMMISSION, DG CNECT, Head of Unit Data Policy and Innovation

First of all, I would like to thank the European Forum for Manufacturing and Orgalim for organising this event and bringing us together for this important discussion. I would also like to thank the Members of the European Parliament for their contributions and introductory remarks.

I would like to focus on the Data Act, our broader European data strategy, and how we see the landscape evolving over the coming months and years, particularly with regard to artificial intelligence in Europe.

- Europe's Industrial Strength as a Competitive Advantage
  Europe has considerable industrial strengths. We have world-class engineering expertise, advanced manufacturing capabilities, leading machinery producers, sophisticated robotics and highly developed production processes.

  All these activities generate enormous volumes of data that could potentially be used to develop and deploy artificial intelligence.

  We therefore possess an extraordinary resource. Increasingly, it is becoming clear that access to unique, high-quality datasets will be a key competitive differentiator in AI. Europe's industrial data could provide us with a significant advantage in this global competition.

  The challenge is how to unlock this valuable data, which often remains confined within proprietary systems and isolated silos, and make it available for innovation.

  A first essential step is to ensure that our regulatory framework is simpler, more coherent and easier to apply. This is precisely what we are seeking to achieve through the Digital Omnibus.

- The Digital Omnibus: Simplification and Legal Certainty
  Let me briefly outline where we stand.

  The European Commission put forward its proposal on 19 November 2025, with the objective of reducing complexity, fragmentation and compliance costs, while providing greater legal certainty and maintaining essential safeguards.

  The Council agreed on its negotiating mandate in October, and I would like to highlight some elements of particular relevance to the manufacturing sector.

We fully recognise the importance of protecting trade secrets. This concern was already reflected in the Commission's original proposal, which sought to make it easier to invoke the trade-secret safeguards provided under the Data Act.

The Council has gone further by strengthening these safeguards, particularly regarding the risk of unlawful disclosure of commercially sensitive information. It has also introduced an additional refusal mechanism where there are specific, substantiated risks of unlawful acquisition, use or disclosure of protected information.

While we would naturally have preferred the Commission's original proposal, the Council's approach is one we can work with. In the European Parliament, discussions are also progressing. The relevant committees are examining the proposal, with particular attention to the data provisions, as well as the GDPR and privacy-related aspects.

The tentative timetable is for Parliament to establish its negotiating mandate during the first quarter of next year, allowing trilogue negotiations to begin shortly afterwards.

Overall, we are making encouraging progress.

However, regulatory simplification is only one part of the picture. Equally important is ensuring that the rules we already have work effectively in practice.

- Making the Data Act Work in Practice
  This brings me to the implementation of the Data Act.

  The Data Act has been applicable since September 2025. It gives users new rights to access and use data generated by connected products, including industrial machinery.

  The underlying principle is straightforward: if you own, rent or lease a connected device, you should have a say in how the data it generates is used.

  Users should also be able to decide whether that data is shared with third parties, including providers of innovative services. This can unlock substantial opportunities, particularly for independent maintenance services, industrial optimisation and the development of new data-driven business models.

  To support implementation, the Commission has undertaken a range of activities:
  - We have organised numerous workshops with industry representatives, including many participants around the tables today, to explain the legislation and address practical questions.
  - We have also published comprehensive FAQs and, more recently, model contractual terms designed to make it easier for businesses, particularly SMEs, to establish data-sharing agreements.
  - In addition, we have established a dedicated legal helpdesk for the Data Act, which receives questions on a regular basis.

  Further guidance is being prepared, notably on definitions and compensation.
  These initiatives reflect our commitment to ensuring that the Data Act delivers tangible benefits rather than simply establishing legal obligations.

- A Dedicated Dialogue with the Automotive Industry
  In the automotive sector, we are taking this approach one step further.

We are establishing a dedicated industrial dialogue bringing together vehicle manufacturers, suppliers and aftermarket service providers. The first meeting is imminent.

The objective is to go beyond the standard implementation measures and identify additional practical obstacles that may prevent the full potential of the Data Act in this specific domain from being realised.

For example, we are exploring whether it might be possible to agree on a common, cross-brand dataset that vehicle manufacturers could make available.

This would go beyond existing legal obligations, but it could represent an important step towards facilitating innovation and competition, particularly in the automotive aftermarket. We are also considering whether this model of structured industrial dialogues could be extended to other sectors.

- Physical AI: Europe's Next Major Opportunity
  Looking further ahead, physical AI represents one of the next major opportunities for Europe.

  This is an area where our industrial strengths place us in a particularly favourable position. Europe has a substantial installed base of connected machinery, industrial equipment and sophisticated production systems. These assets generate precisely the kinds of data that will be essential for developing AI applications interacting with the physical world.

  We already have many of the foundations required to succeed. The challenge is to make it significantly easier to access and use the data generated by these industrial assets.

  And this brings us to another important dimension of our strategy: the infrastructure needed to enable effective data sharing.

- Common European Data Spaces: Turning Access into Innovation
  The Data Act establishes legal rights regarding access to and use of data.

  But legal rights alone are not sufficient. We also need practical mechanisms through which companies can exercise those rights and share data securely and efficiently.

  Over recent years, the Commission has developed and financially supported the concept of common European data spaces. We are now seeing approximately 240 data-space initiatives across the European Union. The principle is to combine technical infrastructure, such as cloud-based solutions, with clear governance arrangements defining who can access data and under what conditions.

  I want to address one concern that is sometimes raised. Participating in a data space does not mean that companies surrender control over their data. On the contrary, companies retain control over how their data is shared and used. They can establish access conditions and, where appropriate, monetise their data. This is an essential feature of the model.

  The Commission is supporting the development of data spaces in individual sectors, while also providing horizontal assistance through the Data Spaces Support Centre. The Centre has developed practical resources, including blueprints and guidance, to facilitate the establishment and operation of data spaces.

  We are already seeing promising results. In March next year, the Data Spaces Symposium will take place here in Belgium, bringing together the wider European data-space community.

It will provide an opportunity to discover successful initiatives and exchange experiences.

One interesting example is a Belgian data-space initiative that enables farmers to derive economic value from their data. It has already demonstrated encouraging results and received recognition for its work. This example shows that the concept can deliver real benefits.

Looking ahead, however, we would like to see greater private-sector investment.
Public funding is necessarily limited, and as data-space initiatives mature and move closer to the market, private investment will become increasingly important for their long-term development and sustainability.

- From Rules to Results
  Let me conclude.

  All the initiatives I have described:
  - implementation of the Data Act
  - Digital Omnibus
  - development of common European data spaces
  - our broader data strategy

  ultimately serve the same objective: enabling Europe to make better use of its industrial data to support innovation and competitiveness.

  This is a clear priority for the European Commission, and we are making a substantial effort to translate that ambition into practice. Through the Digital Omnibus, we are working towards simpler rules, reduced complexity and lower compliance costs. Through the Data Act, we are making more industrial data accessible. And through common European data spaces, we are building the mechanisms that allow this data to reach the companies and innovators capable of putting it to productive use.

  Physical AI represents a particularly important opportunity for Europe, and I believe the Data Act can make a significant contribution to realising that potential. We are starting from a position of strength. We have an outstanding industrial base, advanced machinery, engineering expertise and considerable technological capabilities. We also believe that we have the foundations of an appropriate regulatory framework, particularly once the simplification measures have been completed.

  Nevertheless, important challenges remain.

  Data is still too fragmented, too difficult to access and too often underexploited. As a result, we are not yet making full use of the enormous potential of Europe's industrial assets.

  With the Data Act and the Data Union Strategy, our ambition is to overcome these barriers and move from rules to results.

  That is ultimately what matters: ensuring that Europe's industrial strengths translate into innovation, new business opportunities and greater competitiveness.

INDUSTRY VIEWS



My Bergdahl, TEKNIKFÖRETAGEN, Director for Standardisation and Chair of Orgalim's Digital Transformation WG

Imagine standing outside a concert hall. Listening. One note tells you little. Hear every note, and you can reconstruct the entire score.

Industrial data works in much the same way. One sensor reading may seem harmless. Thousands can reveal how a machine works – and years of research and investment.

This is the perspective I bring tonight on behalf of Orgalim and 770,000 technology companies across Europe. We support the Data Omnibus. Europe needs simpler, more coherent digital rules that support industrial innovation and investment. But simplification must be real.

Let me highlight four priorities:

- We Must Protect Europe's Industrial Know-How
  Trade secrets reflect years of investment. Once disclosed, that knowledge cannot be taken back.
  - Please support amendments preventing disclosure without the trade secret holder's consent.
  - Please reject requirements to prove serious economic damage before a leak has happened. Data sharing depends on trust.

- Safety And Cybersecurity Must Come First
  Manufacturers must not be required to share data where this would undermine product safety or cybersecurity.

  Please make clear that European safety and cybersecurity requirements take precedence where obligations conflict. Complying with the Data Act must not mean breaking the Cyber Resilience Act or the Machinery Regulation.

- Let Manufacturers Use Data To Innovate
  Using product data to improve products can require a separate agreement with the customer – even when manufacturers already hold that data.

  Please give manufacturers, as data holders, a clear right to use non-personal product data and share it with development partners, while fully protecting personal data.

- One Incident Should Mean One Report.
  Please defend a single European reporting entry point, including reporting under the Cyber Resilience Act.

  A common website is not enough if definitions, thresholds and deadlines still differ. The test is simple: must a company submit the same information more than once?

Let me finish where I began. Europe must share the music without giving away the entire score.

Parliament can make the Data Omnibus deliver real simplification: protect know-how, put safety first, enable innovation and remove duplicate reporting. That is what Europe's technology industries are asking for.

Emir Demircan, SIEMENS AG, Senior Director



Tonight's question is simple: are we really simplifying data rules for manufacturers and supporting Europe's Industrial AI ambitions?

Many industrial companies would say no. For instance, the Data Act was meant to support data sharing in Europe. Instead, it has made it more complicated.

But we can still fix the Data Act's main flaws with the Digital Omnibus package.
I will describe three main problems of the Data Act and propose a simple fix for each:

- Trade Secrets
  The Data Act requires manufacturers to disclose trade secrets. It assumes that organizational and technical measures taken by third parties will protect the manufacturer's trade secrets. But in practices security standards vary widely, so a manufacturer with strong security is as safe as the weakest company it shares data with.

  And the proposed handbrake mechanism is fundamentally flawed. A manufacturer would have to prove future economic harm. But how does one assess a competitive advantage that only materializes in market share gains years later? What portion of lost revenue can be causally attributed to the trade secret?

  In practice, it is effectively impossible to determine whether and which trade secrets are used in competitors' product development or disclosed further along the supply chain globally. Also, trade secrets of a European manufacturer must also be fully protected within the European Union, not only in third countries.

  In medical, industrial and railway sectors, among others, industry is already sharing data but also protecting its trade secrets.

  In this regard, the EU Trade Secrets Directive sets clear rules. Information counts as a trade secret only if it is not generally known, it is properly protected, and it has value because it is secret. The Data Act should follow these rules, not weaken them.

  Trade secrets can only be protected by not disclosing them. Once a trade secret is disclosed, its value is lost. The resulting harm is irreversible. Simply put, a disclosed trade secret is a lost trade secret

  - Simple fix: exclude trade secrets and data from which trade secrets can be derived from the mandatory data transfer rules of the Data Act.

- Industrial AI
  The Data Act hinders the scale-up of Industrial AI in Europe. It has made unclear whether manufacturers can use data from the machines they built to train AI models or build new digital services.
  - Simple fix: manufacturers should keep access to the data generated by the machines they build.

- Cloud Switching

Data Act's cloud switching rules are damaging Industrial Software- and Platform-as-Service (SaaS and PaaS). Industrial SaaS and PaaS depend on domain-specific data, customer-specific configurations, and many other processes.
Imposing short-term switching rules undermines this technical architecture and commercial viability. It eliminates business planning certainty and hinders innovation, as providers cannot guarantee return on investment.

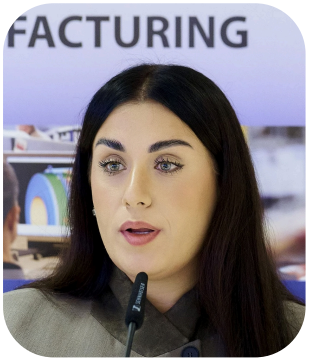
- Simple fix: exclude industrial SaaS and PaaS from Data Act's cloud switching rules.

Where do we stand?
The Council has agreed its position, but multiple Member States did not support it. The Digital Omnibus is now being discussed in the European Parliament.

Industry will keep defending trade secrets, access to machine data for industrial AI, and investment in industrial software and platforms.

We ask the European Parliament to deliver a Digital Omnibus that strengthens our industrial base and make Europe more competitive.

Laura Fiumara, CECE, Policy Manager



This evening, I would like to share CECE's perspective on the implications of the EU Data Act for the construction equipment industry, building on our work throughout the legislative process, our exchanges with the European Commission, and our cooperation with Orgalim.

CECE stands for the Committee for European Construction Equipment, representing the interests of European construction machinery manufacturers. With approximately 1,200 companies, our industry employs around 300,000 people and generates an annual turnover of €60 billion.

The EU Data Act has the potential to reshape how manufacturers access, use and share data, and how they interact with customers and business partners. Since the proposal was first introduced, CECE have invested significant effort in understanding its implications and translating its requirements into practical guidance for the industry.

However, beyond compliance, the key question is "what does the Data Act mean in practice for sectors that design, manufacture and maintain connected machinery?

I would like to focus on one fundamental aspect: the importance of access to machine generated data for manufacturers and why data is so important for construction machinery.

Construction equipment manufacturers are increasingly moving beyond the traditional model of designing, manufacturing and selling machines. They are becoming providers of connected intelligent and data-enabled solutions.

Since modern machines generate significant amounts of operational data through sensors, telematics and connected services, this data has become a strategic asset because it provides valuable insights into machine performance, operating conditions, maintenance needs and productivity.

Effective access to relevant machine-generated data enables manufacturers to improve product quality and reliability, identify technical issues, develop predictive maintenance solutions, deliver software improvements and support research, development and industrial AI applications.

Original Equipment Manufacturers [OEM] typically use machine data and advanced analytics, increasingly combined with AI, to anticipate failures and improve operations reliability - full access to historical and operational machine data is therefore essential to identify patterns and improve accuracy of predictive models.

This is particularly important because manufacturers cannot realistically test every operating condition before a machine enters the market. Actual operating data provides valuable feedback on how equipment performs over time and in different environments.

Access to relevant machine-generated data is therefore not simply about compliance with the Data Act. It is fundamentally about enabling manufacturers to innovate, improve their products and remain globally competitive.

At the same time, access alone is not sufficient. Manufacturers must also be able to use, reuse and, where appropriate, share data within the wider industrial ecosystem.

This is where the specific characteristics of our sector become particularly relevant.
Construction equipment operates within a complex B2B environment involving manufacturers, dealers, rental companies, service providers, maintenance operators, component suppliers, and software developers. All these actors can have legitimate reasons to access and use machine-generated data.

A practical challenge arises because manufacturers do not always maintain a direct relationship with the actual user of a machine. Equipment is often sold through independent dealers or operated by rental customers, meaning manufacturers may not have a direct contractual relationship with the final user.

Against this background, the implementation of Article 4 of the Data Act raises important practical questions. The contractual basis required for the use of non-personal data, together with restrictions on sharing data with third parties, can create difficulties for collaborations across the machinery value chain.

In practice, manufacturers may need multiple contractual arrangements with different business customers in order to access, use and share relevant data for legitimate industrial purposes. Given the number and diversity of actors involved, this can become burdensome and create legal uncertainty.

Let me be clear: this is not a call for unrestricted access to customer information. Any access, reuse and sharing of data must fully respect users' rights, data protection requirements, trade secrets and industrial know-how.

The challenge is therefore not only to understand the legal text, but also to apply it effectively across complex commercial relationships.

For CECE, the guiding principle is straightforward:

- data sharing in business-to-business relationships must be workable, proportionate and supported by contractual freedom.

The Data Act offers significant opportunities for our sector, but those opportunities will only be realised if implementation follows a clear, predictable and practical approach.

GENERAL DATA PROTECTION REGULATION

EUROPEAN COMMISSION KEYNOTE SPEECH



Karolina Mojzesowicz, EUROPEAN COMMISSION, DG JUST, Acting Head of Unit, Data Protection

Over the years, stakeholders from across the spectrum – businesses, researchers, civil society and privacy professionals – have pointed to areas where EU data protection rules are not sufficiently clear, where divergent interpretations create costs, and where legal uncertainty can become an obstacle to investment and innovation.

It is against this background that, last November, the Commission proposed targeted amendments to the GDPR as part of the Digital Omnibus.

Let me be clear from the outset:

- The Digital Omnibus is not about deregulation. And it is certainly not about lowering the level of protection of personal data in Europe.

  We have not touched the core principles of the GDPR. We remain fully committed to ensuring a high level of protection of personal data and safeguarding fundamental rights. What we are seeking is greater clarity about how the rules apply in practice.

And today, I would like to focus on one particular element of our proposal, which I consider especially important:

- The clarification of the definition of personal data.

  This may sound like a technical legal question. But it is much more than that. The definition of personal data determines the scope of application of the GDPR. It determines when its obligations apply and when they do not.

  And in an increasingly data-driven economy, this distinction has profound implications for European businesses, also European manufacturing industry.

  Let me illustrate this with an example from European manufacturing.

  Today, industrial machines generate enormous volumes of data: information about their performance, energy consumption, operating conditions, maintenance requirements and patterns of use.

  This data is essential for improving productivity, developing predictive maintenance and, increasingly, training and deploying industrial AI systems.

  But when is this data personal data?

  Imagine a machine generating information about its operating cycles, the time it is used or its performance. In some circumstances, that information may be linked to an identifiable machine operator. In others, it may be purely technical information, with no realistic means of identifying an individual.

- So, when does data about the use of a machine become personal data, subject to the GDPR? And when does it remain non-personal industrial data?

  This is precisely the kind of question on which companies need clear and predictable answers. And it is particularly important today, as Europe seeks to develop its industrial AI capabilities.

  European manufacturers need to be able to use the data generated by their machines to improve production processes, develop new applications and collaborate with technology providers. But if they cannot determine with sufficient certainty whether that data falls within the scope of the GDPR, they may hesitate to use it or share it, even where doing so would be perfectly lawful.

- We cannot expect European industry to lead in industrial AI if companies are uncertain about the legal status of the data on which that AI depends.

  This is why the Commission has proposed to clarify the definition of personal data, drawing on the case law of the Court of Justice.

  A central issue here is the assessment of identifiability.

  The question is not simply whether information could theoretically be linked to an individual by someone, somewhere. What matters is whether the individual is identifiable, taking account of the means reasonably likely to be used by a concrete entity and the circumstances in which the data is processed.

  This is particularly relevant for pseudonymised data, which may constitute personal data for one actor but not necessarily for another.

  And this brings me to a second issue, which is equally important for European industry.

- What happens when data that is not personal data for one company is transmitted to another company that has additional means to identify an individual?

  Consider a manufacturer holding machine-use data from which it cannot reasonably identify an individual. It shares that data with a technology provider or an AI developer. The recipient may have additional information enabling it to link the data to a particular person. If this is the case for that receiving entity, it would of course be subject to the GDPR.

  But what about the entity which transmitted that data?

  Does the mere fact of transmitting the data to such a recipient automatically mean that the sending company must treat that data as personal data and becomes subject to the GDPR? Or should the legal position of the sender and that of the recipient be assessed separately, taking account of the relevant circumstances and the means of identification reasonably likely to be used?

- This distinction is fundamental.

  The fact that one company possesses the means to identify an individual should not, by itself and irrespective of the circumstances, automatically determine the legal position of every other company handling the same information.

  Of course, the circumstances of the transmission matter, including what the sender knows about the recipient's ability to identify individuals. But we need clarity on precisely how these factors should be assessed.

  This is particularly important in industrial ecosystems, where data is increasingly shared between manufacturers, equipment suppliers, technology providers and AI developers. Legal uncertainty about the status of that data can discourage precisely the cooperation that Europe needs to develop industrial AI.

  In this context, I would also draw attention to the recent Opinion of the Advocate General in Case C-654/25. The Advocate General makes some very interesting points about the assessment of identifiability, the means available to different actors and the relevance of the recipient's ability to identify individuals when assessing a data transmission. The Opinion is not binding on the Court, but it demonstrates both the complexity and the practical importance of these questions. And it reinforces the need for a clear and predictable legal framework.

And I want to stress one point in particular:

- Clarifying the definition of personal data is not about reducing the protection of personal data.

  It is not about creating loopholes or excluding information from the GDPR where individuals can be identified. On the contrary, it is about ensuring that the GDPR applies where its protection is required, while avoiding unnecessary uncertainty about information that does not constitute personal data.

- A clear boundary around the scope of the GDPR does not weaken its protection. It makes that protection more predictable and effective.

  For European manufacturing, this is not a marginal legal adjustment. It is a matter of competitiveness.

Europe has a strong manufacturing base, world-class engineering capabilities and significant industrial expertise. Industrial AI offers an opportunity to build on these strengths. But to seize that opportunity, companies need legal certainty about the data they generate, use and share. They need to know when the GDPR applies. And they need to know when it does not.

Beyond the definition of personal data, the Digital Omnibus also includes provisions aimed at providing greater legal certainty for the development and operation of AI systems, while maintaining a high level of protection for individuals.

The negotiations on the Digital Omnibus are progressing. The Commission will continue to support the co-legislators in reaching a balanced agreement.

Svetlana Stoilova, BUSINESS EUROPE, Senior Adviser



This discussion is very timely. With the Digital Omnibus votes passed in IMCO and JURI, the ongoing work in the main committees ITRE and LIBE, and the upcoming discussion at EUCO level on AI application, it all goes to show that the stakes for the European economy are high.

In this light, together with 16 other associations, we have published a list of 9 fixes that can be made now in the Digital Omnibus, which will propel European enterprises forward.

It is a rare moment when so many associations have such a long list of common objectives. This has to be underlined, because this is not yet another statement; it is a call from enterprises that want to put Europe's future in Europe's hands.

Behind this statement are millions of companies of every size, represented by those associations. BusinessEurope alone represents, via our member federations, more than twenty million enterprises from thirty-six countries in the EU, European Economic Area and EU's neighbourhood.

Different countries. Different industries. But one shared belief: Trust is the foundation of a strong economy. Hence, data protection and economic growth are not competing goals.

European businesses have embraced the GDPR. They have invested in it and helped make Europe a global reference point for data protection. We should be proud of that.

But we must also be honest about the challenges. Individually defensible rules can create a collectively unworkable regulatory system.

When regulation becomes so complex that only larger companies can easily manage it, smaller businesses are put at a disadvantage. Even when we speak about industrial data, this is not always just about machines. Machine data can sometimes be linked to the employees operating them. This means that even when the purpose is purely industrial (improving efficiency, safety or sustainability), personal data protection rules may apply.

And businesses need legal certainty about where that boundary lies.

And if the legal uncertainty is too great, a company may simply decide not to innovate, even though it has the engineers. It has the ambition. It has the technology. But it does not have an army of lawyers.

There are numbers telling us something important. According to the OECD report 'Time For Regulatory Reset?', from December 2025, 3.9% of EU employment is devoted to regulatory compliance tasks. By comparison, just 1.7% is dedicated to research and development. And this raises a bigger question.

The cost of regulation is not just the money businesses spend on compliance. The engineers who spend time together with lawyers navigating regulatory uncertainty are engineers who could otherwise be developing new technologies, improving production and creating new products.

The opportunity cost of bureaucracy is not paperwork. It is innovation that never happens.

That is why the Digital Omnibus matters. We believe it should focus on three priorities:

- Legal certainty.
  We need a clear, practical approach that considers whether a particular organisation can reasonably identify an individual, reflecting the Court of Justice's jurisprudence as it has evolved over the years.

  This makes the rules clearer and more proportionate.

- Protect industrial know-how and support AI.
  Companies must be able to use industrial data without putting their trade secrets at risk.

  We also need legal clarity on using legitimate interest for AI development, training and testing, and confirmation of the broad understanding of research, which can also advance commercial interests.

  If we want European AI, we must enable European companies to develop it.

- Make compliance proportionate to risk.
  Human oversight should focus where people's rights and safety are at stake.

  For broad, routine or low-risk processes, we should assess whether human oversight is proportionate, and consider what kind of tasks some requirements create for workers. Human oversight must be meaningful, make good use of people's skills, rather than simply creating repetitive procedural work.

  Our rules should account for that perspective too. This is about the kind of European economy we want to have.

When we think of the Digital Omnibus now, we should not think of the current industrial players only. The economy is not static. Our next industrial champions may today be a small factory, a regional engineering firm or an entrepreneur with a new idea. The responsibility of this legislative initiative is to make sure they can succeed in Europe and beyond.

The Digital Omnibus is the legislation that paves the path for Europe's technological leadership. We must not forget this opportunity.

Salome Peters, VDMA, Legal Counsel



Introduction
Europe's industrial AI moment depends on one thing above all: data. And in industry, our ability to use data is often limited not by technology, but by the way the GDPR is applied.

My message tonight is: The GDPR should protect people where there is a real risk, and it should not burden machines, production lines and manufacturer, especially SMEs, where there is none.

- The core problem: one size fits all

  The GDPR applies the same obligations to every processing activity, regardless of the risk to the data subject. This approach is appropriate for companies which business models rely on the processing of large volumes of personal data. In such cases data privacy should be thought and practiced in a comprehensive way to ensure that natural persons and their personal data are protected.

But in industrial settings, personal data is often a mere by-product. Take a staff number stored on a machine that is operated by that person. If it is not processed any further, the risk is minimal, if not non-existent. Yet the full set of GDPR obligations applies. For SMEs, this means a heavy organisational burden.

VDMA therefore welcomed the Commission's Digital Omnibus proposal of November 2025, in particular the clarification of the definition of "personal data".

- Let me give you two examples of why this matters:
    - Example 1: Industrial Data And The Data Economy

      Under the current approach, any data that can be linked, however indirectly, to a natural person is personal data. In a factory, that includes timestamps, production metrics, localisation data and maintenance records, because in theory they could reveal something about the machine operator.

      In practice, only the data controller can identify individuals from such data. Still, every recipient must comply with the GDPR: find a legal basis, fulfil information duties, conduct data protection impact assessments and delete data on request.

      The EU Data Act obliges manufacturers to share industrial machine-data , yet this data is often still considered personal. As a result, companies face huge organisational effort. A clearer definition of personal data, as initially proposed, would reduce unnecessary bureaucracy and support an effective, innovation-driven data economy.

- Example 2: Data Spaces

  The success of European Data Spaces depends on companies sharing data efficiently.

  Recipients, however, typically receive pseudonymised technical data and cannot identify anyone. Under the current approach, they face the same obligations as the controller.

  Full anonymisation is not a realistic alternative. It is technically complex, there is no harmonised guidance, and it often fails the strict GDPR standard. Clarifying that pseudonymised data does not always constitute personal data for every data recipient is still an essential requirement. It would allow Data Spaces to operate as intended and unlock their full economic potential.

- Our Three Recommendations:
    - Adopt a clarified definition of personal data.
      Pseudonymised data should not be personal data for recipients who cannot reasonably identify individuals. This is essential for Data Spaces.

    - Introduce a genuinely risk-based approach.
      For processing with little or no risk, such as by-product data in machines, we need exemptions from certain GDPR obligations, such as extensive information obligations or records of processing activities.

    - Focus on SMEs.

  Compliance must be manageable for small and medium enterprises especially. That is how we win wider acceptance of data protection, as a prerequisite for secure data processing and data sharing.

Concluding Remarks

Simplification is not deregulation. It means protecting people where it matters and enabling industry to use data where it is safe to do so.

CLOSING REMARKS



Antony Fell, EUROPEAN FORUM FOR MANUFACTURING, Secretary General

This has been an interesting discussion and I would like to thank our Parliamentary host Maria Grapini MEP.

We welcomed the contributions from the two Commission Directorates General, Bjoern Juretzki from DG CNECT and Karolina Mojzesowicz from DG JUST.

The MEPs interventions by Professor Inese Vaidere and Lukas Mandl provided a valuable extra dimension. The input from manufacturers' sectors highlighted the opportunities and challenges of this dossier.

Our thanks to Orgalim for its role in acting as a partner for this EFM dinner debate.

Finally, I would like to thank the EFM team, Chloé Matagne and Janice MacCormack for all their support and now formally close this European Forum for Manufacturing event.

****









