Policy Briefing: A Strategic Analysis of the EU's Digital Omnibus Package

Position Paper of the FCCR on the „Digital Omnibus“

R. Koch/T. Weck (authors)*
A. Diefenhardt/M. Jager/J. Redenius-Hövermann

1. Introduction: A Critical Juncture for EU Digital Policy

The European Commission's introduction of the "Digital Omnibus" package on November 19, 2025, represents a pivotal ***moment for European digital policy***. While the stated objective of simplifying regulation and thereby strengthening the competitiveness of the European economy is to be welcomed, the current regulatory approach – including the gradual changes proposed in the omnibus package – is not sufficient to meet the challenges of the global digital landscape. ***Regulation*** in recent years has become a “jungle” that is ***no longer comprehensible to those affected***, thereby excessively restricting the scope for self-determined behavior. The EU regulatory framework therefore needs more than just minor adjustments; it requires a fundamental ***conceptual realignment.***

The EU should go beyond individual changes and develop a new, data-friendly regulatory philosophy that also strictly protects fundamental rights. This reorientation is necessary to manage the complex ***interplay between two key political objectives:*** the Commission's efforts to strengthen the competitiveness of businesses and the efforts of the EU and the German government to expand digital sovereignty. It is crucial to recognize that these two objectives are not equivalent. A sober critique of the existing framework is the necessary first step toward developing a more coherent and effective strategy.

2. The Design Flaws of Current EU Digital Regulation

In order to chart a new course, it is essential to first understand the ***fundamental shortcomings of the EU's current approach*** to digital regulation. These shortcomings are not isolated problems, but interconnected difficulties that create significant legal uncertainty, stifle innovation, and ultimately undermine competitiveness and sovereignty. The prevailing framework is characterized by four main shortcomings:

- **Ambiguous and Conflicting Objectives:** Major regulations like the General Data Protection Regulation (GDPR) and the AI Act blend public tasks (e.g., fundamental rights protection) with private economic interests (e.g., promoting the free movement of data or supporting innovation). This fusion of disparate goals leads to vague mandates and significant implementation challenges, as regulators and businesses struggle to navigate contradictory priorities.
- **Insufficient Private Enforcement Mechanisms:** The regulatory framework heavily relies on state-led, administrative enforcement. In contrast, the mechanisms for private entities to seek recourse through civil courts remain largely ignored and uncertain. Even where the rules create rights for those affected, the mechanisms

* Roland Koch, former Minister President, is Professor of Management Practice, and Thomas Weck is Associate Professor at the Frankfurt Competence Centre for German and Global Regulation (FCCR) at the Frankfurt School of Finance and Management. The authors declare that the FCCR is funded by companies that have been or are involved in regulatory proceedings on the topics discussed here at the EU and/or national level, although it is independent of its funding partners.

for asserting legal remedies before civil courts in the Member States are inconsistent, which weakens the entire protection structure.

- **Suppression of innovation:** The EU regulatory model has become fundamentally risk-averse, preventively depriving companies of important risk management decisions. This creates a climate of uncertainty that inhibits investment in new digital business models. The fact is, however, that leading European companies have often produced innovations despite – and not because of – the existing regulatory environment.
- **Lack of future-proofing:** The regulatory model is reactive and hardly able to keep pace with technological developments. The initial failure of AI law to foresee the rise of large language models is a prime example of this shortcoming. The very necessity of the Digital Omnibus Package – created to revise several important laws passed only in the last five years – is an admission that the current approach is neither agile nor forward-looking or sustainable.

These foundational problems necessitate a move away from the current approach and toward a new, more coherent conceptual model for digital regulation.

3. A Counter-Proposal: Rebalancing Data Regulation by Addressee and Function

A more effective regulatory framework must move beyond simplistic data categories, such as "personal" versus "non-personal," to a more nuanced model. This model should be structured around two key dimensions: the ***actors involved*** in a data interaction (the addressee) and the ***context and purpose of the relevant interaction*** (the function). This would allow for targeted, proportionate, and logically consistent regulation in various areas of the digital economy.

a) State Access to Data for Sovereign Purposes

When the state accesses personal data for sovereign purposes that interfere with fundamental rights – such as law enforcement or national security – the primary concern remains the ***protection of individual liberties*** against state power. For this domain, the GDPR and national data protection laws provide a suitable and proven regulatory framework. They strike a balance between enabling legitimate state tasks and protecting the rights of individuals. Existing rules should remain unaffected regarding state measures. Nevertheless, efficiency gains could be achieved if other public administration bodies were allowed to ***use existing data*** to fulfill their legal tasks. This should apply in any case where duplicate data collection can be avoided and no fundamental protection interests risk to be violated.

b) Data Use in Business-to-Consumer (B2C) Relationships

In business transactions between companies and consumers, the regulatory challenge is different. Here, consumers are not subject to state control, but exercise their freedom of contract. The core problem is the ***structural imbalance of bargaining power*** between the two parties. The current consent practice under the GDPR (Art. 6(1)(a)) is ineffective in this context; it does not take into account the considerable ***information deficit on the part of consumers*** and ultimately leads to legal responsibility being shifted onto them through mechanisms such as cookie banners. Centralized control of consent, e.g., via a web browser, is difficult to implement because consent is granted for specific purposes.

A more effective approach would be to move away from the consent model altogether and instead base consumer protection on solid contract and consumer law, such as ***standardized terms and conditions*** (civil law; cf. the current P2B Regulation). In addition, ***supervision*** of cross-border online services should be consolidated nationally ***in a single authority*** (such as the German Federal Network Agency) to ensure uniform enforcement. In addition, the development of model declaratory actions should be monitored in order to readjust ***civil law remedies*** for consumers if necessary.

c) Data Exchange in Business-to-Business (B2B) Relationships

The ***existing regulation*** of B2B data exchange ***remains inadequate.*** It does not address the key challenges of the market consistently enough, namely ensuring technical interoperability, overcoming information asymmetries, and striking a balance between data access and the legitimate protection of trade secrets. The European Health Data Space (EHDS) offers a ***more practical model*** than the Data Act, striking a better balance between data access and intellectual property protection.[1]

d) Data Use in Research and Development (R&D)

The ability to use and exchange data for research and development is a cornerstone of competitiveness. However, the current European landscape is too fragmented and restrictive. This leads to data remaining completely unused or to unnecessary multiple surveys (contrary to the once-only principle). A more efficient approach is needed to unlock innovation potential. The most important reforms should include:

- **Consolidating and simplifying** the multitude of data access rules that apply to public bodies under directives such as the Public Sector Information (PSI) Directive, INSPIRE, and others.
- **In Germany,** government agencies are permitted to use data within their remit in compliance with data protection laws. The scope of the upcoming Research Data Act will be expanded to allow access to data from all departmental research institutions.
- **At EU level,** concerted efforts are being made to reduce the fragmentation of data access standards and create a more coherent framework for researchers.

Further, the instruments of the ***Data Governance Act (DGA) are of limited use*** for R&D. The assumption that trust in data use arises primarily through the regulation of intermediaries falls short. What is more important is whether the data source is trustworthy and that data use is delimited in a legally secure fashion. In this regard, the ***"European Business Wallet"*** proposed in the Digital Omnibus ***appears more promising.*** However, this would require research institutions to be able to obtain a uniform identifier and the establishment of a freely accessible directory providing information on usage restrictions for EBW signatures.

e) Regulation of Artificial Intelligence (AI)

The fundamental approach of the AI Act is deeply flawed. The Act creates an ***additional layer of regulation*** on top of existing product safety and liability laws and establishes a

[1] The strict regulation in Sec. 393 of the German Social Code, Book V (SGB V) can be used as a supplement for questions regarding cloud use.

burdensome, surveillance-like compliance system that is ***unsuitable for a fast-moving technology sector.***

The core problem with the law is that it focuses on the ***risks of AI outputs*** and their generation ***without providing legal certainty for the inputs*** that are crucial for AI development and innovation—in particular, the use of personal data, copyrighted content, and trade secrets for training models. This places innovators in a legal gray area. The AI Act thus ***sends*** an extremely ***negative signal to the market*** and directly hinders the EU's goals of strengthening competitiveness and digital sovereignty. The law must be fundamentally revised to strike a sustainable balance between risk management and innovation, or even repealed entirely.

4. Reclaiming Digital Sovereignty as a Core State Interest

"Digital sovereignty" has become a central objective of EU and German policy, but its meaning is often misunderstood. It is critical to draw a clear distinction: ***digital sovereignty is a state interest,*** concerned with maintaining control over critical digital infrastructure and state functions. ***Competitiveness is a corporate interest***, pursued by businesses within a given market framework. The German government's conflation of these two concepts is a fundamental error that leads to misguided policy.

From the perspective of digital sovereignty, complex regulations such as the ***Digital Markets Act*** (DMA) ***and the Digital Services Act*** (DSA) are not a sign of European resilience, but rather a ***symptom of long-standing political failure:*** For years, politicians failed to recognize or address the core problem of inadequate law enforcement in the areas of competition and platforms – proceedings against large US platforms sometimes took a decade. Additional behavioral obligations, such as those now included in the DMA and DSA, which in turn must be enforced, do not remedy the actual ***enforcement deficit.*** At the same time, these regulations are largely ***symbolic politics*** because they do not change anything about key structural challenges – in particular, business models based on personal data and the lack of effectiveness of GDPR consent. Instead, the DMA even adopts the flawed consent logic and thus falls short of effective consumer protection.

A ***genuine strategy*** for digital sovereignty must be proactive and structural. It requires a focus on four key measures:

1. **Decentralize Critical Digital Infrastructure:** Reduce dependency on single providers by promoting decentralized architectures, especially for government services and essential economic sectors like finance and energy.
2. **Promote Open Protocols and Standards:** Foster the use of open-source technologies and interoperable standards to break down walled gardens and reduce vendor lock-in.
3. **Strengthen Effective Legal Enforcement:** Prioritize simple, clear rules that can be enforced quickly and effectively. This requires a well-resourced judicial system and a clear focus on neutralizing violations rather than merely imposing fines.
4. **Increase Political Momentum:** Transparently disclose the ongoing costs and strategic risks arising from dependencies on foreign digital services and infrastructures (e.g., due to license restrictions).

This strategic reorientation provides the foundation for the specific policy recommendations that follow.

5. Analysis and Recommendations for the Digital Omnibus Package

This section offers a targeted critique of the specific legislative proposals on data and AI within the Digital Omnibus Package. While some of the proposed changes are beneficial, many either reinforce the flawed regulatory philosophy outlined above or create new problems that will further complicate the legal landscape.

a) Proposed Amendments to the Data Act

The amendments to the Data Act present a ***mixed picture:*** they combine sensible consolidation with the preservation of failed concepts.

- **Positive:** Consolidating various related legal acts (such as the regulation on the free flow of non-personal data, the Data Governance Act, and the Data Act) into a single instrument is a sensible step toward simplification. Similarly, the introduction of measures to protect public data from uncontrolled access by third countries is a welcome step towards strengthening resilience.
- **Negative:** The decision to adopt the failed DGA rules on data intermediaries and data altruism is a serious mistake. These provisions have proven ineffective and alien to the market and should be deleted, not integrated. Furthermore, the new rules on the protection of trade secrets are impractical, and the creation of multiple, overlapping definitions for small and medium-sized enterprises leads to excessive complexity.

b) Proposed amendments to the GDPR and the ePrivacy Directive

The proposed amendments to the GDPR risk creating ***more uncertainty*** than they eliminate.

- The proposal to introduce a new ***"subjective" definition*** of personal data based on whether a specific body can identify a person establishes a situation-dependent standard that is unsuitable for the protection of fundamental rights. It would create legal uncertainty and immense difficulties in proving cases in legal disputes.
- The idea of a ***"three-tier model"*** that applies different rules depending on the size of the company is to be rejected. The risk arises from the nature of the processing activity, not from the size of the company carrying it out. The principle must be: "Same risk, same regulation."
- The new provisions clarifying the use of personal data in ***AI training*** are insufficient. They do not offer innovators the necessary legal certainty and potentially weaken the protection of fundamental rights without strengthening the position of data subjects accordingly.

c) Regulation of digital identities ("European Omnibus Wallet")

The introduction of a digital corporate identity is to be welcomed. The proposed regulation presented in the "Digital Omnibus" package is limited to what is necessary and involves little bureaucratic burden. However, it would be desirable for ***identifiers developed by international organizations*** to also be recognized as "uniform identifiers" throughout the EU. In addition, steps should be taken to ensure that ***research institutions*** can also obtain a uniform identifier under EU law and that a ***freely accessible directory*** is set up to provide information ***on restrictions on the use of EBW signatures.***

At the ***national level***, there are initiatives – such as the establishment of a basic register for company data at the Federal Statistical Office – that should also be taken into account in the design of new EU legislation in the interest of more comprehensive and consistent regulation of digital identities.

d) Proposed amendments to the AI Act

The "Digital Omnibus on AI" offers only ***superficial solutions*** that do not remedy the fundamental design flaws of the AI Act.

The fact that the Commission has announced the need for ***13 additional guidelines*** to clarify the law is a tacit ***admission of a failed regulatory approach.*** These guidelines will only increase the compliance burden on businesses.

The creation of ***special privileges*** for different categories of small businesses is ***further evidence*** that the ***regulation is too burdensome for everyone.*** Instead of creating complex exemptions, the basic rules should be proportionate and practical.

The proposals do not address the ***many core problems of the AI Act:*** duplicate liability rules, significant legal uncertainty regarding training data, and the chilling effect on innovation. While ***delaying the application*** of the law is a ***welcome tactical move,*** it does not replace the necessary strategic overhaul.

6. Conclusion: Key recommendations for a revised regulatory framework

The European Union is at a ***crossroads.*** To secure its digital future, it must shift from its current complex, risk-averse, and burdensome regulatory policy to a clear, principle-based framework that enables innovation, promotes competition, and effectively protects citizens. The Digital Omnibus package offers an opportunity to initiate this change, but only if it is accompanied by a more profound paradigm shift.

The following ***overarching recommendations*** summarize the key measures required for a successful regulatory realignment:

- **The GDPR should be refocused on its core purpose:** protecting fundamental rights in interactions between the state and citizens. In commercial transactions, specific, targeted consumer and contract laws should be used to eliminate power imbalances.
- **Promote B2B data exchange** by abolishing failed DGA models for data transfer and instead focusing on practice-oriented, industry-led standards for interoperability and the effective protection of trade secrets.
- **Data use in research and development should be significantly simplified and harmonized.** In Germany, state institutions should be given greater scope to use existing data within the framework of their legal mandate, and the scope of the planned Research Data Act should be extended to all departmental research institutions. At the EU level, coordinated initiatives are needed to reduce existing fragmentation and provide researchers with coherent, reliable access to data.
- **The AI Act should be fundamentally revised** to eliminate regulatory duplication with existing liability laws, create clear legal certainty for the use of training data, and align compliance burdens with demonstrable systemic risks, not arbitrary parameters such as company size.

- **Pursue digital sovereignty as a national strategy** by focusing on concrete, structural measures—such as promoting decentralized infrastructure, open standards, and the rapid enforcement of existing laws – rather than creating new layers of complex and often symbolic regulation.

* * *