bitkom

On track for the Data Union

Addendum to the EU Data Union Strategy Public Consultation

July 2025

Content

1 Data Availability

Data Space initiatives need scaling

While many data space initiatives have created a running demonstrator or even built an enterprise-ready system to discover and share data between organisations in a trusted manner, scaling certain initiatives to a level of users/traffic that allows them to **operate sustainably** has sometimes proven **more difficult than initially expected**.

Against this background, there is a **high amount of potential to scale national data space initiatives to other member states, connect them with Common European Data Spaces**, and **collaborate with actors in third countries** to significantly lower the transaction cost for sharing data.

On an organisational level, while the DSSC has proven very useful as a point of contact and collaborates well with entities such as Eclipse Foundation, Gaia-X, FIWARE, IDSA, BDVA, to name a few, the number of working groups and resources needed if a company wants to actively shape best practises or standards remains very or too high for many. In addition, there is a need to further **enhance coordination between EU and member state level when it comes to creating dataspace-friendly conditions** and support in scaling them, for which a **continuous dialogue, or a new modified working group under the EDIB**, could be promising.

On a technical level, the extent to which SIMPL will be of value to specific data spaces by bridging interoperability gaps depends on its broad adoption (-> network effects) which in turn largely depends on its **cost-effectiveness for data spaces**. **Connectivity with SIMPL must be easy** to achieve both in terms of time and resources and yield to higher value than cost.

Standardisation needs better communication

There is a need to increase **trust in the legal validity of emerging Privacy Enhancing Technologies**. This could drive acceptance and thus uptake. A viable approach could be to **greenlight specific approaches** via legislation, enforcement or at last using soft law guidance.

Furthermore, there is room to further **improve communication of upcoming and ongoing standardization activities on the European level**, which links to the ongoing review of (EU) 2012/1025 (Standardisation Regulation) to **encourage more SMEs** to join these discussions in due course.

2 Simplification

The recent data law acquis has brought new opportunities by increasing trust in data sharing, reducing data localisation and clarifying data access rights and obligations. Nevertheless, this also came with significant hurdles for businesses.

Applying several laws simultaneously creates aggregate complexity beyond the complexity of the individual laws. We have already noted the need for a simplification law ahead of the EU elections.[1]

Some substantial changes are required

In detail, while **Data Act, Data Governance Act, Open Data Directive, Free Flow of Non-Personal Data Regulation, GDPR, e-Privacy Directive** all have their merits, some more some less, their parallel application and overlaps render them difficult to understand and implement. Ironically, if two laws counteract each other, legislative intention can remain unfulfilled while implementation causes high effort.

For the development of innovative technologies – and thus the competitiveness of European companies – legally reliable access to relevant data is essential. This requires an urgent reform of data protection and ePrivacy regulations, including targeted legal adjustments and, in particular, addressing the highly one-sided and unbalanced interpretations of the law by data protection authorities.

In terms of substance, we have already outlined areas for **harmonisation between horizontal digital laws, both more generally[2] and in detail[3].**

In addition, we are open and are committed to certain harmonisations and clarifications to the substance of the Data Act, already this year. This includes the necessary **guidance on international data transfers** mentioned in Article 32 (3) last sentence should be published without delay (see also chapter 3).

Institutional governance needs a reform

In terms of governance, there is room for improvement regarding the **EU Data Innovation Board**. Its capacity should be heightened by allocating more staff and **increasing the frequency of meetings**. Ideally it should be institutionalised and be brought on par with the EDPB. There is a need to **increase the transparency of its nomination procedure** and **its work results**. Decisions by EDIB (and EDPS) should be **made reviewable by EGC/ECJ**.

[1] The Digital Policy Priorities for the European Elections in 2024 by Bitkom are available here: https://www.bitkom.org/EN/List-and-detailpages/Publications/On-Digital-Policy-Priorities-for-the-European-Elections-in-2024.
[2] Legislative focus areas that would merit more consistency identified by Bitkom are available here: https://www.bitkom.org/EN/Bitkom/Publications/Toward-Coherent-EU-Tech-Framework.
[3] Concrete suggestions where and how to harmonise the EU digital acquis are available here: https://www.bitkom.org/EN/Bitkom/Publication/Patchwork-to-Blueprint-Toward-Coherent-EU-Tech-Framework.

In terms of regulatory cooperation and harmonised enforcement of digital laws, including DGA and DA, the relevant supervisory authorities should profit immensely from a **common case management system**. This would enable a faster and more precise view on individual enforcement decisions, could help to prevent a **race to the bottom/forum shopping** and establish further **evidence on the proportionality of the data law** acquis in particular.

Similarly, in terms of procedure, to ensure effective implementation of Article 35 of the Data Act, the development of standards for technical portability and interoperability must **be transparent, inclusive, and based on continuous stakeholder input**. The ongoing development of the methodological framework for the standards repository should be subject to **public consultation and include continuous mechanisms for feedback and participation** to reflect the complexity and broad relevance of data processing services.

3 International Data Flows

Supply chains & sovereignty are complex issues

Data transfers cannot be considered in isolation from supply chains and business processes. Especially for companies that manufacture physical products, there is often a physical value chain behind a data transfer. It is important to take this into consideration when discussing any potential restriction of data transfers.

Irrespective of any particular definition, the concept of **data sovereignty should always be analysed in conjunction with the necessary hardware and software for the storage, transfer and processing of data**.[4] In other words, measuring or strengthening data sovereignty will not be implementable in practise as long as Europe lacks the required **public and private investments in hardware and software** to store, transfer or process data within the EU Single Market to a greater extent.[5]

Apart from investments, this fundamentally depends on a Digital Single Market Policy that creates an **innovation friendly level playing field and refrains from (protectionist) barriers to trade**.

Even more, the **concept of sovereignty must also be applied to such hardware and software if one does not want to merely *replace* a low level of sovereignty in one area for another area**.

[4] The 2025 results of Bitkom Research on digital sovereignty (in German) are available here: https://www.doi.org/10.64022/2025-digitale-souveraenitaet.
[5] The response to the Cloud & AI Development Act Consultation by Bitkom offers greater detail with respect to this matter and is available here: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14628-AI-Continent-new-cloud-and-AI-development-act/F3571510_en.

For some use cases, for instance cybersecurity services, data sovereignty may not even be desirable, as the most effective cyber defence relies on world-wide data sources and globally distributed infrastructures.

Against this background, the **long-term goal of the EU should be to diversify the origins and destinations of data transfers more broadly without being neither dependent nor autarch from a particular third country**. In other words, supply chain risks, be it due to geopolitical shocks, trade barriers or other events, must be continuously managed between many third countries in parallel. Being able to do this in practise requires

1. **Public and private investment in hardware and software mentioned above (i.e. long-term building the resources to change to),**
2. **a multitude of effective Free Trade Agreements (i.e. trusted trading partners),**
3. **continuous deep-level risk assessments conducted by the respective (national) authorities, which ideally do not contradict each other.**

The above framework applies to public and private entities as well as on an EU macro level. Thus, businesses must also be enabled to voluntarily:

1. **increase transparency of their supply chain risk to be able to then**
2. **manage them individually and**
3. **obtain support – or as the case may be, instructions – by the relevant authorities.**

Trust is created in collaboration

Generally, data protection, data use and information security must be conceptualised and balanced in an integrated manner to be effective. **Data protection by design, be it for personal data, trade secrets or IP-protected data, can be much more effective than a legal prohibition *per se* or at least be an important complement.** For example, while there a difference in terms of applicable jurisdiction and legal consequences, it does not necessarily matter too much to a company if its trade secrets are stolen from a German or a Korean data centre. The same holds for malicious attacks to gather personal data or breaches of copyright.

There **is a need for an international forum that brings together authorities for the protection of data, those for the use of data and those for information security**.

Furthermore, there is a **need for guidance regarding technical and organisational measures between Data Act, DGA, ODD, GDPR, Trade Secrets Directive**[6]. It can be difficult to apply different TOMs according to which law(s) the data is subject to: It can happen that significant volumes of data are treated as personal data even if not all of it necessarily is – to be on the safe side with respect to GDPR. While rights and obligations between personal and non-personal data will change e.g. with Data Act, TOMs should be as uniform as possible.

[6] Per se there is no explicit focus on international data transfers in the Trade Secrets Directive but it is de-facto related with respect to technical and organisational requirements for protection of data from unlawful access.

Bitkom represents more than 2,200 companies from the digital economy. They generate an annual turnover of 200 billion euros in Germany and employ more than 2 million people. Among the members are 1,000 small and medium-sized businesses, over 500 start-ups and almost all global players. These companies provide services in software, IT, telecommunications or the internet, produce hardware and consumer electronics, work in digital media, create content, operate platforms or are in other ways affiliated with the digital economy. 82 percent of the members' headquarters are in Germany, 8 percent in the rest of the EU and 7 percent in the US. 3 percent are from other regions of the world. Bitkom promotes and drives the digital transformation of the German economy and advocates for citizens to participate in and benefit from digitalisation. At the heart of Bitkom's concerns are ensuring a strong European digital policy and a fully integrated digital single market, as well as making Germany a key driver of digital change in Europe and the world.

Published by
Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin
Germany

Contact person
David Schönwerth | Head of Data Economy
P +49 30 27576-179 | d.schoenwerth@bitkom.org

Responsible Bitkom Committee
WG Data Policy & Data Spaces