ministry of
digital affairs

The Danish Government's response to the consultation of the Commission on a European Data Union Strategy

18 July 2025

1. A refreshed European approach to data

The time is right for a refreshed and enabling European approach to data. It is in this spirit that Denmark welcomes the Commission's efforts toward a new European Data Union Strategy (EDUS). The Danish government calls for a strong focus on streamlining and simplifying the current regulatory framework to unleash the full potential of data, also in view of the upcoming Digital Package.

The availability of large quantities of high-quality data is critical for the development of artificial intelligence (AI), which is a key enabler for enhancing Europe's global competitiveness. Data sharing across the public and private sector is important for European companies to be able to develop data-driven solutions.

The current regulatory framework for data hinders the full potential of data sharing. It is also imposing significant administrative barriers and cost-related burdens for companies and authorities, ultimately stifling data-driven innovation.

From a Danish point of view, priority should be given to revise existing regulation in, with a focus on reducing burdens, and improving the balance between protection and innovation. This starting first and foremost with the General Data Protection Regulation (GDPR), as well as it's interaction with the ePrivacy Directive. Moreover, also horizontally across data regulations to ensure simplification, consistency and legal clarity.

Furthermore, at a horizontal level, new and existing legislation should be digital ready from the get-go through a screening of the acquis and by ensuring that structured and standardised data formats are set for businesses reporting requirements.

Finally, automating digital business reporting - by standardizing and streamlining cross-border data interoperability – is crucial to reduce administrative and unlocking the many opportunities of a more connected and streamlined EU data economy.

Against this background, the following response elaborates on our key points to be aware of in the forthcoming EDUS:

- Making more room for innovation while maintaining a strong framework for data-protection
- A clear and consistent regulatory framework for data sharing
- Ensuring the availability of high-quality data for the uptake of AI-solutions
- Encouraging the use of data-driven solutions to burden reduction and enabling data sharing between businesses

2. Making more room for innovation while maintaining a strong framework for data-protection

While the protection of personal data is a fundamental right, which in its core shall be respected, the GDPR in its current form is creating barriers to the development and use

of data-driven solutions such as AI that benefit European companies, citizens and public authorities. Where better data use could support the development of solutions that benefit European companies and citizens, the current regime risks stalling technological and societal innovation and limit Europe's chances to compete in the AI race.

A recent study finds that compliance with GDPR (and associated national legislation) costs Danish companies close to EUR 2 billion every year. There is an urgent need to address the negative effects of GDPR, which constitute a drag on European competitiveness.

Many initiatives in the private and public sector are being paused or abandoned due to concerns over compliance, stemming from GDPR rules that can be complex, unclear, and challenging to navigate without specialised legal expertise.

Danish companies point to burdensome documentation requirements and mapping of dataflows and the broad scope of the rights granted to the data subjects. In particular, small companies and non-profit organizations find the GDPR burdensome to comply with. The impact is also felt by citizens — who find it more cumbersome to participate in community and volunteer organisations. From a Danish perspective it is very important to safeguard the continued functioning and prosperity of the civil society and local associations.

Thus, Denmark advocates for an upcoming revision of the GDPR that ensures that public authorities, businesses and individuals can benefit from data-driven solutions. Rather than hindering innovation, the revised framework should unlock improved access to data for the training of AI models.

There is no doubt that we need data protection in the EU. Nonetheless, we need to do it smarter and more flexible. Specifically, Denmark encourages an even more risk-based approach, where regulatory requirements are proportionate to the actual risks involved in data processing. Denmark sees a need to recalibrate the balance between, on one hand, ensuring an adequate level of protection of personal data, and on the other, ensuring the right scope of action for companies, so they can continue to thrive.

Additionally, in the spirit of ensuring that companies are not stifled by excessive regulatory burdens, the interaction between GDPR and the ePrivacy Directive should be particularly considered. The costs related to implementing and maintaining a cookiebanner for companies are substantial vis-à-vis the often harmless – from a privacy perspective – simple tracking purposes involved in maintaining a website. Users are also becoming increasingly desensitized to cookie consent banners. Instead of fostering trust, this risk leading to "cookies fatigue" — where rules overwhelm users, rather than empowering them.

From Danish side, it is suggested that only companies collecting data for purposes of marketing or sharing of data with third parties should be required to maintain a cookiebanners. This would massively reduce burdens to European companies and avoid overwhelming users, while not compromising with the protection of personal data. Thus, it could be appropriate to make an exemption in the GDPR, whitelisting the processing and storage of personal communications data for technical purposes and for simple statistics.

In this vein, Denmark recommends:

- Revise and simplify the data protection regime to reduce burdens for businesses and make it more innovation friendly.
- Consider a more risk-based approach to data protection.

- Abolish the cookie-banner for non-harmful purposes.

3. A clear and consistent regulatory framework for data sharing

Efforts to achieve a single market for data are currently hindered by the absence of a clear, simple and consistent regulatory framework for data sharing and reuse (see examples in Chapter 6. Appendix, Figure 1.).

The upcoming EDUS and Digital Package is an opportunity to review the EU data regulation to addresses these inconsistencies, in view of simplifying burdens for companies and enable data sharing for businesses, citizens and authorities. Against this background, the Danish Government strongly recommends specifically:

- The horizontal digital regulation should be aligned in order to provide a clear and consistent legal framework for data sharing and reuse. This includes the General Data Protection Regulation (GDPR), Data Governance Act (DGA), Data Act (DA), AI Act (AIA), Interoperable Europe Act (IEA), Open Data Directive (ODD), Free Flow of Data Regulation (FFDR).

- The horizontal digital regulation should be coordinated with sectoral regulation such as Intelligent Transport Systems Directive (ITS), Payment Services Directive (PSD), Infrastructure for Spatial Information in the European Community Directive (INSPIRE), European Health Data Space Regulation (EHDS) and others in order to provide an easier overview and reduce redundancy or the risk of inconsistency.

- Focus on the value added of existing regulation, without prejudice to any piece of legislation. This may involve integration of some of the regulation, e.g. the ODD and chapter II the DGA, in order to collect related regulation in single acts to provide an easier overview and reduce redundancy or the risk of inconsistency. This could furthermore involve repealing the DGA whilst placing its governance structure elsewhere, namely the European Data Innovation Board (EDIB). Alternatively, the Commission should consider reviewing the conditions for data intermediation services provider (DISP) listed in article 12 of the DGA with a view to stimulating innovation in the data market that is yet to develop.

- The rules regarding AI training on personal data or other protected data should be clarified with deference to the protections provided by the GDPR, the DA and other relevant regulations.

4. Ensuring the availability of high-quality data for the uptake of AI-solutions

The availability of large quantities of data of high quality are an essential component in the development of AI-solutions.

The EDUS should continue and build on ongoing efforts to make more data reusable for AI training and other purposes. This should encompass both ODD and DGA related data sharing by public sector organizations and data sharing of companies in data spaces.

Further efforts regarding data quality would increase usability for AI. This includes clear definitions of data quality, increased use of standardized data, standards for documentation and processes for data quality assurance and trusted data transactions. Moreover, greater legal certainty regarding intellectual property rights (IPR) and personal data rights in relation to AI training and models is needed to support Europe as an AI continent.

A renewed effort to highlight the value of data sharing through data spaces and other mechanisms is also important. In order to support efficient supply chains, the flow of data within the EU need to be as open and smooth as possible. Open data in particular should remain open to maximize value creation and avoid introducing administrative burdens. The strategy should also support improved sustainability of European data spaces. This includes both the common European data spaces and other initiatives. Data valuation and pricing seems to be a particular challenge as well as definition of sustainable business models for the data spaces. Engagement of private businesses is also hampered by uncertainty about security of business secrets, unclear business models and this should therefore be addressed in the EDUS.

5. Encouraging the use of data-driven solutions to burden reduction and enabling data sharing between businesses

Data-driven solutions have a significant potential to simplify data sharing and reporting, facilitating compliance and reducing the administrative burdens faced by businesses. To this end, we encourage the use of digital tools, such as the European Digital Identity Wallet under eIDAS2 Regulation, and the forthcoming Business Wallet.

Furthermore, while acknowledging the need to simplify existing data regulation, a similar long-lasting effort must be taken to encourage digitisation, standardisation and automation of data collection, handling and sharing needed for businesses reporting obligation.

Increasing businesses digital capabilities, streamlining and harmonising digital reporting requirements and provide common open and decentralized EU data infrastructures, has the potential to dramatically reduce the current burdens stemming from manually business-to-business data gathering, processing and sharing across fragmented systems available on the market.

Thus, the EDUS should promote digital ready legislation to existing and new reporting requirements making sure that they follow structured and harmonised data formats that can be easily shared across interoperable IT systems in open business data exchange infrastructure.

Furthermore, efforts should be targeted to make EU digital tools and businesses digital systems interoperable, portable and to handle standardised data by exploring common minimum requirements and technical functionalities as well as methodology on data sources and methodology in digital business systems to make digitised and automated reporting comparable. This could be realised through the establishment of a long-term open business data infrastructure build on standards and interoperability in collaboration between the Commission, Member States and private actors.

Here a clear governance model should be explored in terms of combining and creating interoperability between existing EU building blocks as well as defining a common EU architecture for business data distribution and by ensuring the necessary links to other efforts such as the EU data spaces. The infrastructure should look to existing best practices in Member States, existing Union wide data infrastructures, such as the Open Peppol network, and ongoing efforts to build new infrastructures, such as the digital

product passport system. It is key to secure an open and interoperable infrastructure that all European businesses can use without risking vendor lock-in and keep cost down.

6. Appendix

Figure 1.: For example, while GDPR establishes the principle of privacy by design (Regulation (EU) 2016/679, article 25), the Data Act (DA) demands access by default. Similarly, while the Cyber Resilience Act (CRA) requires that manufacturers of digital products address vulnerabilities through security updates (COM (2022) 454 final, article 1(3)(k)), the Ecodesign for Sustainable Productions Regulation (ESPR) stipulates that "no change shall occur as a result of rejecting [software and firmware] updates" (Regulation (EU) 2024/1781, article 40(5)).

Additionally, definitions lack of consistency as well, such as "data processing service" in the DA and "cloud computing service" in NIS2, as well as "data centre service" in NIS2. In addition to this, the term "data holder" is defined differently in the DA and the Data Governance Act (DGA).

At the same time, contradictions and inconsistencies regarding reporting and auditing requirements also exist across EU legislation. One example is the lack of harmonization on the requirements related to market surveillance systems (e.g. the NIS 2 Directive, CRA, Cybersecurity Act, and AI Act), leading companies to submit the same or similar information multiple times.