

A European strategy for data

2020/2217(INI) - 02/03/2021 - Committee report tabled for plenary, single reading

The Committee on Industry, Research and Energy adopted the own-initiative report by Miapetra KUMPULA-NATRI (S&D, FI) on a European strategy for data.

Values and principles

Members stressed that the EU must strive for EU-wide data governance and a human-centric, data society and economy based on the Unions values of privacy, transparency and respect for fundamental rights and freedoms, empowering its citizens to take meaningful decisions over the data produced by or relating to them. The COVID-19 crisis has highlighted the role of and need for high-quality, real-time databases, information and data sharing, as well as shortcomings in the infrastructure and interoperability of solutions across Member States. Therefore, individuals should have full control of their data and be further assisted in enforcing their data protection and privacy rights regarding the data they generate. The right to data portability and the data subjects access, rectification and erasure rights provided for by the General Data Protection Regulation.

Data governance and spaces

The committee supports the creation of a data governance framework and common European data spaces, which should be subject to EU rules and cover transparency, interoperability, sharing, access, portability and security of data, with a view to enhancing the flow and reuse of non-personal data or personal data that is fully GDPR-compliant and securely anonymised in both industrial and public environments and across and within specific sectors.

Members called for the creation of a Commission-led expert group that would have the capacity to help and advise the Commission to set common, EU-wide guidelines on data governance in order to turn interoperability and data sharing into a reality in the EU. They encouraged the Commission to use common European data spaces to enhance trust, adopt common standards and regulations, and encourage the creation of well-formed application programming interfaces (APIs) along with robust authentication mechanisms, and to consider using pre-agreed, clearly specified and time-bound sandboxes to test innovations and new business models as well as new data management and processing tools, both in the public and private sector.

Inseparability of personal and non-personal data

The report recalled that personal and non-personal data, such as industrial data, is not always separable and can be difficult and costly to separate, with the result being that a large amount of data currently remains unused. Data sets in which different types of data are inextricably linked are always treated as personal data, including in cases where the personal data represents only a small part of the data set. Therefore, Members urged the Commission to:

- provide further guidance on the lawful processing of data and on practices on the utilisation of mixed data sets in industrial environments;
- consider establishing a legislative framework and a clear definition of horizontal and cross-cutting personal data spaces alongside other data spaces, and to further clarify the challenge of mixed data sets.

Data act, access and interoperability

Members urged the Commission to present a data act to encourage and enable a greater and fair B2B, B2G, government-to-business (G2B) and government-to-government (G2G) flow of data in all sectors. Collaborative approaches for sharing data and standardised data agreements should be encouraged to improve predictability and trustworthiness. There is a need for contracts to set clear obligations and liability for the accessing, processing, sharing and storing of data in order to limit the misuse of such data.

Infrastructure and cybersecurity

In relation to cloud service providers, Members called on the Commission to oblige in the future Cloud rulebook for service providers to show where they store data. Additionally, the report stated that cloud service providers should not have access to data stored on their servers, unless there is a separate agreement between parties. A more robust cybersecurity is a prerequisite for a stable data economy.

Global rules

Lastly, Members considered that global rules governing the use of data are inadequate. They invited the Commission to come forward with a comparative analysis of the regulatory environment for data in third countries. The report highlighted the need for international rules and standards to foster global cooperation aimed at strengthening data protection and establishing safe and appropriate data transfers, while fully respecting EU and Member States laws and standards.