Neapolis University Pafos, Cyprus
AI-Z-TRACE-CRIME
Jean Monnet Center of Excellence
Co-funded by the European Union

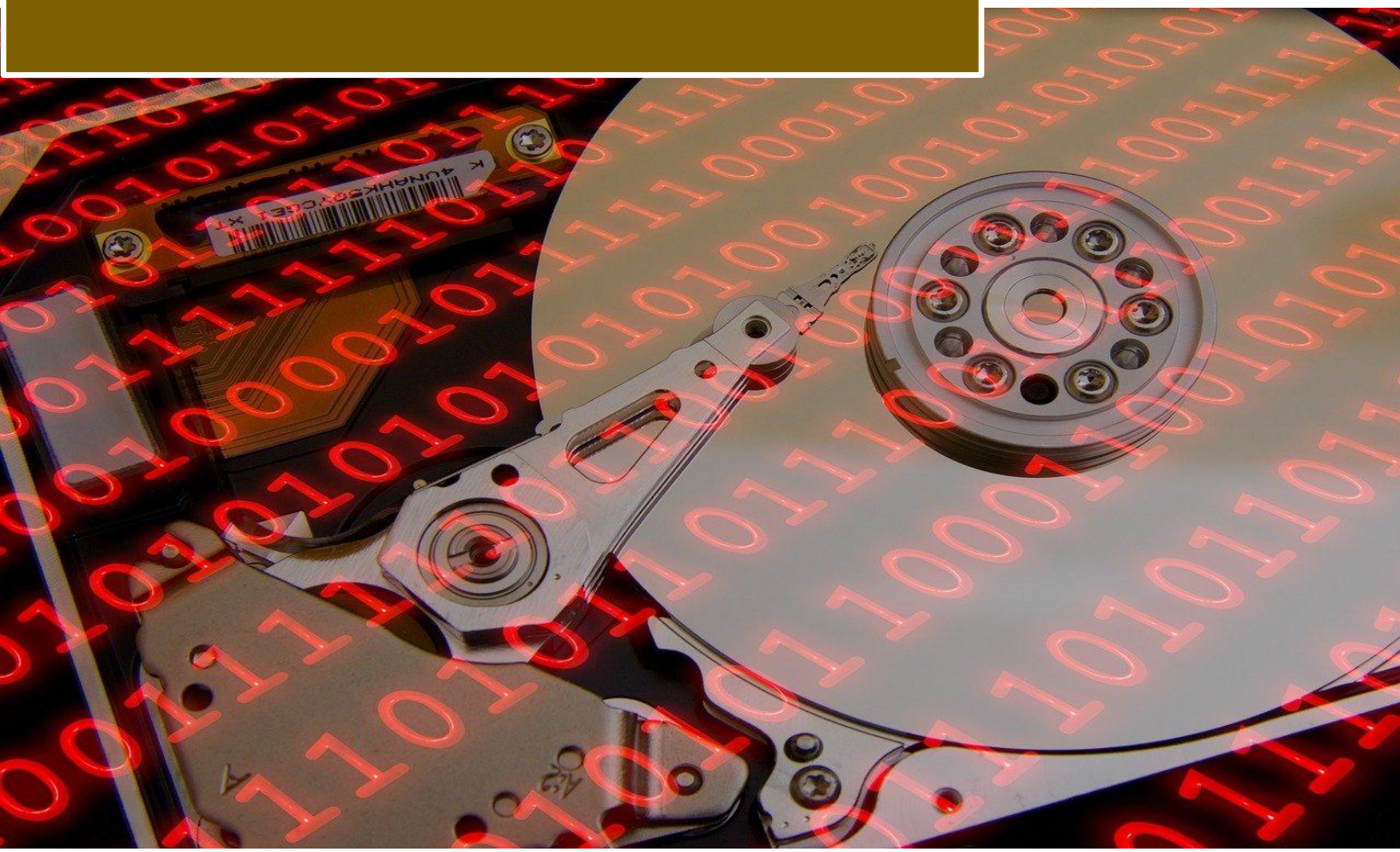
Policy Brief

The EU Data Act:

Unlocking Europe's Data Economy

NUP Jean Monnet / UNESCO Policy Briefs

32/2025



Co-funded by the European Union

Neapolis University Pafos

UNESCO Chair in Human Development, Security & the Fight against Transnational Crime and Illicit Trafficking in Cultural Property

unesco Chair

The NUP Jean Monnet / UNESCO working papers and policy briefs can be found at:

https://www.nup.ac.cy

Publications in the Series should be cited as:

AUTHOR, TITLE, NUP UNESCO/JEAN MONNET WORKING PAPER or POLICY BRIEF NO. x/YEAR [URL]

Copy Editor: G. Pavlidis

Neapolis University Pafos, School of Law

Pafos, 8042, Cyprus

The EU Data Act: Unlocking Europe's Data Economy

Executive Summary:

The EU Data Act (Regulation (EU) 2023/2854), adopted in November 2023 and entering into application in September 2025, constitutes a landmark step in the Union's digital strategy. Designed to remove barriers to data access and use, it establishes harmonised rules for fair data sharing, user empowerment, and business-to-government access in cases of exceptional need.

The Act complements the Data Governance Act, the Digital Markets Act, and the AI Act, forming a central component of Europe's broader digital regulatory architecture. Its objectives are threefold: to enhance fairness in contractual relations, to empower consumers and businesses to exercise control over connected devices and services, and to stimulate innovation through secure and trustworthy data availability. While hailed as a transformative instrument for Europe's data economy, the Act also raises challenges. Industry warns of compliance burdens, risks to trade secrets, and potential conflicts with international data transfer rules. At the same time, regulators face the task of reconciling the Act with existing EU frameworks, most notably the GDPR. This policy brief outlines the regulation's key provisions, evaluates its expected implications, and recommends measures to maximise benefits while mitigating risks.

Keywords

EU Data Act, Data Economy, IoT, Cloud Switching, Data Sharing, B2B, B2G, Artificial Intelligence, Digital Regulation

Background

The EU has long recognised the underutilisation of industrial and IoT-generated data as a barrier to competitiveness, innovation, and digital sovereignty. Although the General Data Protection Regulation (GDPR) secured individual data rights, it left gaps in addressing non-personal and co-generated data, particularly in business and industrial contexts. In February 2020, the European Data Strategy identified these gaps and pledged to create a regulatory environment to enable data access and reuse across sectors. The Data Governance Act, adopted in 2022, established trusted intermediaries and governance structures for voluntary data sharing. The Data Act, first proposed in 2022 and formally adopted in 2023, operationalises these ambitions by creating mandatory rules for access, use, and sharing of data generated by connected devices and digital services. The regulation is part of the EU's vision of creating common European data spaces across key sectors such as health, mobility, energy, and finance, where data circulates freely under clear rules, supporting both innovation and sovereignty.

Policy Directions and Key Measures

User Access and Portability: The Data Act introduces user rights to access and use data generated by connected products such as smart home devices, vehicles, or industrial sensors, as well as related services. Users may request that this data be shared with third parties of their choice, which empowers competition in aftermarket services and innovation. To make these rights effective, manufacturers are required to design products so that such access is technically possible by default.

Fairness in Business-to-Business Contracts: The Act addresses asymmetries in negotiating power, particularly for small and medium-sized enterprises, by preventing the imposition of unfair contractual clauses regarding data access. It introduces a blacklist and grey list of prohibited or suspect contractual terms, echoing consumer contract law, and foresees the publication of model contract clauses by the Commission to support fairer negotiations.

Business-to-Government Data Sharing: Another key measure concerns access by public authorities to privately held data in cases of exceptional need, such as natural disasters or pandemics. Such access is subject to strict conditions of necessity, proportionality, and respect for confidentiality, while also safeguarding trade secrets. The regulation requires that data holders receive compensation under fair, reasonable, and non-discriminatory terms when obliged to share data.

Cloud Switching and Interoperability: The Act further addresses lock-in effects in cloud and edge services by obliging providers to allow users to switch providers without undue barriers. Switching must be possible within 30 days, and providers are prohibited from imposing data egress fees once a transitional period has passed. Interoperability standards for data processing services will be promoted to strengthen the EU's cloud ecosystem.

Safeguards for Trade Secrets and International Data Transfers: Finally, the Act balances data-sharing obligations with safeguards for trade secrets and intellectual property. Providers and data holders are required to take all necessary measures to prevent unlawful access by third-country authorities, thereby mirroring concerns already raised in the GDPR about international data transfers.

Implications and Challenges

The economic potential of the Data Act is significant. By unlocking industrial and IoT data worth billions of euros, the regulation is expected to boost Europe's competitiveness in artificial intelligence, machine learning, and predictive analytics. SMEs in particular stand to benefit from fairer contracts and enhanced opportunities to develop new services, while consumers will enjoy greater control over the data they generate, increasing trust and encouraging uptake of smart technologies.

Nonetheless, the regulatory complexity of the Act poses challenges. Its overlap with the GDPR raises interpretative issues when personal and non-personal data are intertwined, and enforcement will require close coordination between national authorities, the European Commission, and existing regulators in data protection, competition, and sectoral domains. Companies also express concern over the vague definition of "exceptional need" in the context of business-to-government sharing, which could generate legal uncertainty.

Business concerns are particularly acute for IoT manufacturers, who face the burden of redesigning products to enable user data access. Questions about the effectiveness of safeguards for trade secrets remain unresolved, as industry actors worry about the risk of involuntary disclosure in both business-to-business and business-to-government contexts. Cloud providers, meanwhile, anticipate revenue losses due to the ban on exit fees, even if these measures are intended to spur innovation and lower costs for customers.

At the geopolitical level, the Act reflects Europe's ambition for digital sovereignty by reducing dependence on foreign cloud providers and by setting a global standard for data governance. However, the strict restrictions on data transfers to non-EU jurisdictions may create tensions in international markets and risk affecting Europe's global competitiveness.

Practitioner's Corner:

Operational Insights & Strategic Considerations

Anticipate Model Contractual Terms (by Sept 2025): The Commission will publish non-binding model contractual clauses for both data-sharing agreements and cloud/data processing service contracts. Practitioners should monitor these drafts and adapt contracts ahead of their formal adoption to ensure compliance with fair, reasonable, and non-discriminatory (FRAND) standards.

Designate a Legal Representative (if non-EU): Non-EU entities offering connected products or covered services within the EU must appoint a legal representative in at least one Member State where they operate. Compliance officers should identify obligations early, choose jurisdictions strategically, and ensure the representative is fully briefed.

Map Data Scopes and Limitations: The Act grants users rights to raw or pre-processed data generated through connected products, but explicitly excludes derived or inferred data. Organisations should classify datasets accordingly and document which categories fall within the Act's scope.

Negotiate Trade Secret Safeguards: Data holders may withhold or suspend sharing if disclosure risks causing serious economic harm and confidentiality protections are inadequate. Contracts should integrate tailored trade secret clauses and set clear thresholds for invoking refusal rights.

Plan for Enforcement and Dispute Resolution: Member States must designate competent authorities and, where multiple exist, appoint a data coordinator as a single point of contact. Certified dispute settlement bodies may also be created to resolve disagreements over FRAND terms. Practitioners should map the national enforcement architecture and explore dispute bodies as practical tools.

Prepare for Mid-Term Evaluation: The Commission will evaluate the Data Act within three years of its application and may propose amendments. Implementation strategies should therefore include feedback mechanisms and flexibility for future regulatory changes.

Account for GDPR Interactions: The Data Act remains subordinate to the GDPR. When data sets contain both personal and non-personal elements, organisations must ensure lawful processing through privacy impact assessments, anonymisation, or pseudonymisation strategies.

Concluding Remarks

The EU Data Act is a pioneering initiative that moves Europe's data economy from principles to practice. By mandating access, fairness, and interoperability, it has the potential to stimulate innovation, empower consumers, and strengthen digital sovereignty. Success depends on effective implementation. Ambiguities in definitions, tensions with existing frameworks such as the GDPR, and industry concerns about compliance and confidentiality must be managed carefully. Clear guidance from the Commission, sector-specific codes of conduct, and robust enforcement mechanisms will be crucial. The Act represents both opportunity and challenge. If implemented with adequate support for SMEs, rigorous oversight, and international dialogue, it could catalyse Europe's transition to a data-driven economy. If not, risks of fragmentation, litigation, and compliance fatigue may blunt its intended impact.

Further Reading

- Regulation (EU) 2023/2854 on harmonised rules on fair access to and use of data (EU Data Act), OJ L, 2023 (link)
- European Commission, "European Strategy of Data," COM(2020) 66 final (link)
- OECD Recommendation on Enhancing Access to and Sharing of Data (2021)(link)