



Digital Council Position on EU Data Sovereignty

Introduction

Digital Council supports the European Commission's objective to strengthen the data sovereignty of the European Union. However, data sovereignty should not be reduced to the physical location of data in the EU or to the origin of the technology provider. Properly understood, data sovereignty means the ability of European companies, public institutions and citizens to exercise effective control over who accesses data, under what conditions, in which jurisdiction, with which technical safeguards and with what ability to switch provider or operating model.

Europe needs secure and trusted international data flows. Without them, it will not be possible to develop artificial intelligence, cloud services, cybersecurity, research, digital public services, industrial data spaces or cross-border supply chains. Trusted cross-border data flows are also essential for fraud prevention, combating financial crime, global threat intelligence, real-time risk monitoring and business continuity.

At the same time, the geopolitical environment, asymmetries in market access, third-country requirements to localise or disclose data and risks of unauthorised access to sensitive non-personal data require a more active and strategic EU approach.

Digital Council recommends that the EU proceed in a risk-based, technologically neutral and proportionate manner. Measures should protect genuinely sensitive categories of data and critical use cases, rather than creating blanket barriers to ordinary commercial, research, operational and security-related data flows.

The core of European data sovereignty should be based on legal certainty, interoperability, open standards, auditability, customer control over encryption keys, transparency of privileged access, cloud switching, portability, reversibility, supply-chain resilience and enforceable contractual safeguards.

European data sovereignty policy should strengthen competitiveness, not weaken it. New rules should therefore not add another complex compliance layer on top of the GDPR, the Data Act, the Data Governance Act, NIS2, the Cyber Resilience Act, DORA and sector-specific legislation. They must be clear, practically implementable and usable also for startups, small and medium-sized enterprises and smaller public buyers.



Core premise: sovereignty as control, not isolation

Digital Council recommends that the EU define data sovereignty as the ability to exercise effective control, not as isolation or blanket localisation.

The physical location of data in the EU may be relevant for certain sensitive use cases. On its own, however, it does not guarantee sovereignty. Data may be stored in the EU and still be exposed to risks through remote administration, subcontracting chains, privileged administrator accounts, legal obligations of a provider in a third country or insufficient control over encryption keys.

Conversely, some cross-border data flows may be secure, legitimate and necessary where they are based on a clear legal basis, contractual safeguards, technical measures, transparency and auditability. The EU's objective should therefore not be to keep all data in Europe at any cost, but to ensure that European organisations can make informed decisions about where and how their data is processed, who has access to it and what options they have for control, remedy and exit.

Digital Council proposes working with five dimensions of data sovereignty:

Legal control means clarity on the applicable law, who may request or disclose data, how requests from third-country authorities are handled and whether effective remedies are available.

Technical control includes encryption, key management, identity management, logging, monitoring, privileged access management, environment segmentation and security architecture.

Operational control means the ability to ensure service continuity, recovery after incidents, resilience against outages, crisis management and a functioning exit plan.

Economic control means the ability to switch provider, transfer data and workloads, avoid disproportionate vendor lock-in and use interoperable solutions.

Institutional control means auditability, supervision, certification, enforceability of rules and clear responsibilities between EU bodies, Member States, regulators and contracting authorities.

Protection of sensitive non-personal data



Digital Council supports the Commission's intention to improve the protection of sensitive non-personal data. Some non-personal data may have significant economic, security or strategic value. This may include data from critical infrastructure, industrial production data, cybersecurity telemetry, technical data from strategic sectors, selected research data, public-sector data or datasets usable for training and validating AI systems.

The Data Act already contains rules under which providers of data processing services must take appropriate technical, organisational and legal measures to prevent international and third-country governmental access to non-personal data held in the EU where such access or transfer would conflict with EU law or the law of a Member State.[4]

Digital Council nevertheless cautions against creating an overly broad or vague category of "strategic data". If not precisely defined, such a category could affect ordinary business processes, increase compliance costs and create legal uncertainty for companies and public institutions.

The EU should introduce a practical risk classification based on the following criteria:

1. the nature and sensitivity of the data;
2. the sector and its relevance to the public interest;
3. the likelihood and impact of misuse;
4. the availability of technical and contractual safeguards;
5. exposure to third-country law;
6. the impact on competitiveness, innovation and operational continuity;
7. the possibility of anonymisation, pseudonymisation, aggregation, federated processing or the use of synthetic data;
8. the availability of privacy-enhancing technologies and other technical controls that can reduce the need for data movement or disclosure.

Enhanced protection should be reserved for specific risk-based use cases, not applied broadly to entire sectors or all cross-border data flows. The EU should also provide regulatory certainty that privacy-enhancing technologies, strong encryption, customer-controlled keys, secure multi-party computation, data clean rooms, federated learning and other safeguards can be recognised as meaningful risk-reduction measures where appropriate.

International data flows: openness with trust



Digital Council supports the principle of “data free flow with trust”. Cross-border data flows are a basic condition for the functioning of the digital economy. They are essential for cloud, AI, cybersecurity, research, financial services, e-commerce, industrial supply chains, customer support, remote administration and cooperation between companies and public institutions.

They are also indispensable for fraud prevention, combating financial crime and cyber resilience. Modern fraud and cyber-risk monitoring often depends on the ability to identify global patterns, share threat intelligence, detect anomalies in real time and maintain geographically distributed infrastructure. Overly restrictive localisation requirements can therefore reduce resilience and operational effectiveness rather than increase them.

For personal data, a broad EU transfer toolkit already exists under Chapter V of the GDPR, including adequacy decisions, standard contractual clauses, binding corporate rules, certification mechanisms, codes of conduct and derogations.[5] For non-personal data, the EU should develop a similarly clear but proportionate framework for identifying and managing risks, without creating unnecessary duplication with existing rules.

The EU should respond actively where third countries impose unjustified localisation requirements on European entities, restrict data exports, discriminate against European providers, condition market access on the sharing of sensitive data or fail to provide sufficient safeguards against unauthorised government access. The EU’s response, however, should be graduated: diplomacy, regulatory dialogue, trade agreements, standards, mutual recognition and interoperability bridges should come first; restrictive measures should be used only where structural imbalances or abuse of the EU’s openness persist.

The Commission should also continue to support trusted and scalable mechanisms for international data transfers, including adequacy decisions where appropriate, standard contractual clauses, binding corporate rules, certification mechanisms, codes of conduct and other trusted transfer tools. Adequacy remains valuable, but it cannot be the only pillar of Europe’s international data strategy. A modern AI and cloud economy requires a broader, more resilient and more operational transfer architecture.

Practical barriers in third-country markets

European companies operating globally increasingly face a double bind. On the one hand, they encounter foreign data localisation mandates, local-processing expectations, regulatory approvals, sector licensing, security reviews or procurement conditions that



can function as market-access barriers. On the other hand, they must also comply with complex EU transfer requirements, including case-by-case assessments that can be difficult to apply in practice, especially for smaller entities.

Several major markets illustrate the practical challenges. China's framework for cross-border data transfers includes security assessment, standard contract and certification pathways for certain outbound transfers. India requires payment system providers to store payment system data in India. Türkiye has introduced its own standard contracts for transfers abroad. Uruguay allows model contractual clauses for international transfers but may still require prior authorisation in certain cases. Saudi Arabia and the UAE have adopted transfer regimes requiring specific conditions or safeguards for transfers abroad. South African procurement and data-cloud policy frameworks also illustrate how local content, local incorporation or domestic capacity objectives can interact with market access and procurement.[6]

These measures differ in purpose, legal design and intensity. They should not be treated as identical. Taken together, however, they show a broader trend: data-transfer rules, localisation expectations, licensing requirements, procurement preferences and local-entity requirements can cumulatively raise costs, slow market entry, reduce deal velocity, fragment global risk-management architecture and create pressure to duplicate infrastructure.

This is particularly problematic in sectors such as payments, cybersecurity, cloud services and AI, where resilience depends on integrated monitoring, global expertise, real-time analytics and the ability to operate across jurisdictions. The EU should therefore address third-country barriers through trade policy, digital partnerships, regulatory dialogues and international standard-setting, while avoiding measures that would replicate the same barriers inside the Single Market.

Simplifying EU transfer governance

The EU should also look inward. A credible data sovereignty policy must not only respond to barriers in third countries; it must also ensure that EU rules are coherent, predictable and practically usable.

The current framework for international personal data transfers is often experienced as legally complex and operationally burdensome. Transfer Impact Assessments, divergent supervisory interpretations, lengthy approval processes for Binding Corporate Rules and overlapping contractual requirements can create disproportionate costs, especially for SMEs, schools, public institutions and smaller service providers. In some cases, organisations are effectively expected to assess foreign surveillance laws with a



level of legal sophistication that is unrealistic outside large multinational compliance teams.

Digital Council therefore supports a simplification-oriented approach. The Commission should assess whether existing Chapter V mechanisms can be made more scalable and predictable, including by:

- enabling portfolio-based or group-level assessments for similar transfers using the same safeguards;
- clarifying that practical likelihood and actual risk of foreign government access are relevant to transfer assessments, rather than applying an unworkable zero-risk standard;
- streamlining and accelerating BCR approvals, including through clearer timelines and stronger mutual recognition among supervisory authorities;
- updating and expanding standard contractual tools where legal gaps or duplicative arrangements arise;
- accelerating codes of conduct and certification mechanisms under Articles 40 and 42 GDPR for cloud services and international transfers;
- providing clear guidance on the role of privacy-enhancing technologies as recognised safeguards;
- reducing duplicative contractual requirements where equivalent safeguards are already in place.

This should be framed as simplification and operationalisation of existing legal tools, not as a lowering of protection. The objective should be to maintain a high level of protection while making trusted data flows practically manageable.

Data localisation: a legitimate tool only in limited cases

Blanket data localisation should not be the default instrument of European data sovereignty policy. Localisation may be legitimate for a narrow group of critical use cases, for example certain defence, security, judicial, health, energy or highly sensitive public-sector systems. Even in these cases, however, it must be justified by a specific risk, technologically feasible, legally reviewable and accompanied by requirements for cybersecurity, interoperability and reversibility.

For ordinary commercial, research, operational and security-related data flows, blanket localisation would likely lead to higher costs, market fragmentation, reduced service availability and weaker innovation. It could also disproportionately affect startups and



SMEs, which often rely on global cloud infrastructure precisely because it enables them to scale more quickly and affordably.

The EU should therefore distinguish between:

- **data residency**, meaning the location of data in a given jurisdiction;
- **operational sovereignty**, meaning control over operations, privileged access and service continuity;
- **legal sovereignty**, meaning the ability to resist unauthorised access or conflicts of law;
- **technical sovereignty**, meaning customer control over keys, architecture, logging and security measures;
- **economic sovereignty**, meaning the ability to transfer data and switch provider.

This distinction is essential. Without it, the EU risks adopting formally “sovereign” rules that do not in fact strengthen control over data, but merely increase costs and administrative burden.

Cloud, AI and vendor lock-in

One of the greatest practical risks for European companies and public institutions is not only where data is stored, but whether data, applications and workloads can be effectively moved. Real data sovereignty requires the ability to switch provider, combine multiple providers, use hybrid architectures and avoid a situation where technical dependence on one ecosystem prevents rational decision-making.

The Data Act strengthens rules on switching between providers of data processing services, including cloud and edge services, and sets a framework for data portability, digital assets and interoperability. It also requires providers to remove obstacles to switching and phases out switching charges, including data egress charges, by January 2027.[7]

Digital Council recommends that the Commission place particular emphasis in the area of data sovereignty on:

- exporting data in standardised and machine-readable formats;
- open APIs and interoperability;
- technical reversibility of services;
- contractually embedded exit plans;
- preventing disproportionate egress fees and hidden switching costs;



- customer control over encryption keys;
- transparent lists of subcontractors;
- auditable access logs;
- clear allocation of responsibility between provider, customer and subcontractors;
- support for open standards and open source components where they are secure, maintainable and economically realistic.

Cloud and AI infrastructure will be as strategic for the European economy as energy, transport or financial infrastructure. European policy should therefore support the development of Europe's own capacities, but it should not prevent access to the best available technologies from trusted providers. The objective should be greater ability to choose, not administratively created dependence on a narrower group of suppliers.

Provider origin should not replace measurable security safeguards

For sensitive use cases, it may be relevant to assess jurisdictional risk, ownership structure, operational control, supply chains or exposure to third-country law. Digital Council, however, does not recommend using company origin as a simple substitute for measurable security, legal and operational safeguards.

European origin of a provider does not automatically guarantee a high level of security, interoperability or operational resilience. Non-European origin of a provider does not automatically mean an unacceptable risk. The decisive factor should be a concrete risk assessment: who controls the infrastructure, who manages the keys, who has privileged access, how requests from third-country authorities are handled, what contractual and technical barriers exist against unauthorised access, and what options exist for audit and remediation.

The Commission's proposed Cloud and AI Development Act introduces an EU-wide assessment framework for cloud and AI sovereignty, with sovereignty assurance levels that include criteria on processing in the Union, independence from third countries and, at higher levels, EU ownership and control combined with the possibility of recognising third-country providers.[8] This makes it especially important that sovereignty criteria are applied carefully, transparently and proportionately.

Digital Council recommends a balanced framework.



For standard services, the key criteria should be measurable security outcomes, interoperability, contractual safeguards and the ability to exit.

For highly sensitive public or critical services, stricter requirements may be legitimate, including requirements for operational control in the EU, limitations on privileged access from third countries, independent audits or dedicated sovereign environments.

Such requirements, however, must be transparent, proportionate, technologically feasible, realistic in timing and reviewable. Where future EU sovereignty assurance frameworks interact with international data transfers, they should not rely solely on adequacy decisions, but should recognise the full set of lawful GDPR Chapter V mechanisms where appropriate, including SCCs, BCRs, codes of conduct and certification mechanisms.

Impact on startups, SMEs and European competitiveness

Digital Council considers competitiveness to be one of the main tests for any new initiative in the field of data sovereignty. Europe already faces a complex regulatory environment. If new rules added further unclear obligations, duplicative reporting or costly legal assessments, the burden would fall most heavily on startups, small and medium-sized enterprises and smaller public institutions.

That would be counterproductive. Data sovereignty should strengthen Europe's capacity to innovate, not create further barriers to the adoption of cloud, AI and data analytics. According to Eurostat, 53% of EU enterprises used paid cloud services in 2025, which shows the growing importance of cloud for the European economy.[9] The Commission's Data Union Strategy also identifies streamlining data rules as one of its core priorities.[3]

Digital Council therefore recommends introducing the principle: **no new obligation without simplification**.

New measures should be accompanied by practical tools:

- a simple risk-assessment template;
- model contractual clauses;
- sector-specific examples of good practice;
- guidance for startups and SMEs;
- clear allocation of responsibilities between infrastructure providers, customers and intermediaries;
- transition periods;



- the possibility of using certified or pre-assessed services;
- regulatory sandboxes for data spaces, AI and sensitive data use cases;
- a single contact point for interpretation of the rules.

The EU should also continuously assess the impact of proposed measures on costs, technology availability, speed of AI adoption, investment in data infrastructure, startups, SMEs and public buyers.

Digital Council recommendations to the European Commission

Digital Council welcomes the European Commission's efforts to strengthen the EU's data sovereignty. Data is a strategic asset of the European economy, and its secure use will be essential for the development of AI, cloud services, industrial data spaces, research, public services, fraud prevention, cybersecurity and the competitiveness of European companies.

European data sovereignty policy should, however, be based on control, proportionality and openness towards trusted partners. The right objective is not to keep all data in Europe regardless of context, but to ensure that European organisations have real control over their data, transparent safeguards, enforceable rights and genuine freedom of choice.

Digital Council recommends that the European Commission:

1. Define data sovereignty as effective control over data, not as blanket localisation

Data sovereignty should not be reduced to the physical location of data in the EU. Data location may be relevant for certain sensitive use cases, but on its own it does not ensure control over access, encryption keys, infrastructure operations, requests from third-country authorities or the ability to switch provider.

The EU should work with a broader understanding of sovereignty that includes legal, technical, operational and economic control over data.

2. Introduce a practical classification of sensitive non-personal data

Digital Council supports targeted protection of sensitive non-personal data, especially where such data has economic, security or strategic value. This may include critical



infrastructure data, industrial data, cybersecurity telemetry, selected research data, public-sector data or datasets usable for training and validating AI systems.

The Commission should, however, avoid an overly broad or vague category of “strategic data”. Enhanced protection should be based on a concrete assessment of risk, impact of misuse, sector, technical safeguards, exposure to third-country law and available risk-reduction measures, including privacy-enhancing technologies.



3. Preserve trusted international data flows

Cross-border data flows are essential for cloud, AI, cybersecurity, fraud prevention, financial crime prevention, research, financial services, e-commerce, industrial value chains and customer support. The EU should therefore build on the principle of “data free flow with trust”.

Europe should be open towards trusted partners, while being able to respond to unjustified localisation requirements, discriminatory rules, restrictions on data exports, weak safeguards against government access or requirements to share sensitive data as a condition for market access.

4. Address third-country market barriers through trade, diplomacy and interoperability

The EU should use trade policy, digital partnerships, regulatory dialogues and international standard-setting to address third-country measures that function as de facto localisation or market-access barriers. This includes situations where transfer restrictions, licensing requirements, procurement preferences, security reviews or local-entity requirements force European companies to duplicate infrastructure or fragment global operations.

The EU should also support multilateral approaches to trusted data flows, including OECD work on Data Free Flow with Trust and interoperability with accountability-based global frameworks such as the Global Cross-Border Privacy Rules system.[10]

5. Use data localisation only as an exceptional and justified tool

Blanket data localisation should not be the default solution for European data sovereignty policy. It may be legitimate for narrowly defined critical use cases, for example certain defence, security, energy, health or highly sensitive public-sector systems.

Even in these cases, localisation must be based on a specific risk, technologically feasible, reviewable and accompanied by requirements for cybersecurity, interoperability and reversibility.

6. Strengthen cloud switching, interoperability and reversibility

Real data sovereignty requires the ability to switch provider and transfer data, applications and workloads without disproportionate technical or economic barriers. Sovereignty without the ability to exit a provider is merely formal.



The Commission should further support standardised and machine-readable formats, open APIs, technical reversibility of services, contractually embedded exit plans, subcontractor transparency, auditable access logs and customer control over encryption keys.

7. Avoid using provider origin as a simple security criterion

For sensitive use cases, it may be relevant to assess jurisdictional risk, ownership structure, operational control, supply chains or exposure to third-country law. These criteria, however, should not replace concrete security, contractual and technical safeguards.

European origin of a provider does not automatically guarantee security, and non-European origin does not automatically imply unacceptable risk. The decisive factors should be transparent risk assessment, measurable safeguards, auditability, access control, the possibility of remediation and the ability to switch provider.

8. Operationalise existing GDPR Chapter V transfer tools

The EU should continue to support adequacy decisions, but should not rely on adequacy alone. It should make the full set of GDPR Chapter V mechanisms more scalable and operational, including SCCs, BCRs, certification mechanisms, codes of conduct and other trusted transfer tools.

The Commission should assess targeted simplifications that would reduce duplicative transfer assessments, streamline BCR approvals, clarify the use of SCCs in complex transfer scenarios and provide greater legal certainty for organisations relying on recognised technical safeguards and privacy-enhancing technologies.

9. Prevent duplication with the existing European data framework

The European data and digital framework already includes the GDPR, the Data Act, the Data Governance Act, rules on the free flow of non-personal data, NIS2, the Cyber Resilience Act, DORA and sector-specific regulation. New measures on data sovereignty should therefore not create another parallel compliance regime.

Digital Council recommends the principle of “no new obligation without simplification”. New rules should clarify and complement the existing framework, not add duplicative reporting, unclear responsibilities or another administrative layer.



10. Take into account the impact on startups, SMEs and smaller public buyers

Data sovereignty rules must be practically usable also for organisations that do not have extensive legal, security and procurement teams. Overly complex or costly requirements could slow the adoption of cloud, AI and data analytics precisely among smaller companies and institutions.

The Commission should prepare simple risk-assessment tools, model contractual clauses, sector-specific examples of good practice, guidance, transition periods and the possibility of using certified or pre-assessed services.

11. Support European technology capacities in an open way

Europe needs to develop its own cloud, AI, semiconductor, cybersecurity and open source capacities. This ambition is legitimate, but it should not be pursued primarily through restrictions that narrow competition or limit European organisations' access to trusted technologies.

European technological sovereignty should be open: its objective should be greater ability to choose, interoperability, control over critical dependencies, supply-chain resilience and the ability to switch provider.

12. Regularly assess impacts on competitiveness and resilience

Every new measure in the field of data sovereignty should be assessed not only from the perspective of security, but also according to its impact on costs, investment, innovation, service availability, startups, SMEs, public buyers, fraud prevention, cybersecurity and cross-border trade.

European data sovereignty will be successful only if it strengthens security, trust and competitiveness at the same time. These objectives are not in conflict, provided that the EU chooses a risk-based, technologically neutral and practically implementable approach.



Sources

- [1] European Commission, “Targeted consultation on safeguarding the EU’s data sovereignty”, published 8 July 2026; opening 8 July 2026, closing 15 September 2026.
- [2] European Commission, “Proposal for the Cloud and AI Development Act (CADA)”, published 3 June 2026; the proposal is part of the broader package to strengthen the EU’s cloud and AI ecosystem, investment and infrastructure.
- [3] European Commission, “Data Union Strategy – Unlocking Data for AI”, 19 November 2025; the strategy identifies three priority areas: scaling up access to data for AI, streamlining data rules and strengthening the EU’s global position on international data flows.
- [4] European Commission, “Data Act explained”; the Data Act applies since 12 September 2025 and includes safeguards against unlawful third-country government access to non-personal data held in the EU.
- [5] European Commission, “Rules on international data transfers”; the GDPR transfer toolkit includes adequacy decisions, standard contractual clauses, binding corporate rules, certification mechanisms, codes of conduct and derogations.
- [6] For selected examples of third-country rules and frameworks, see: Reserve Bank of India, “Storage of Payment System Data”, 6 April 2018; Türkiye Personal Data Protection Authority, announcement on standard contracts for transfers abroad; Uruguay URCDP Resolution No. 50/022 on model contractual clauses and prior authorisation; Saudi Data and AI Authority, updated regulation on personal data transfers outside the Kingdom; UAE Government, data protection laws; South African Government, National Data and Cloud Policy / Public Procurement Act context.
- [7] European Commission, “Data Act explained”, Chapter VI on switching between data processing services; the Data Act aims to enable customers to switch seamlessly and removes switching charges, including data egress charges, from 12 January 2027.
- [8] European Commission, “Cloud and AI Development Act”; the Commission’s description of the proposed sovereignty levels includes requirements related to Union-based processing, independence from third countries, EU ownership and control at Level 3, and possible recognition of third-country providers.
- [9] Eurostat, “53% EU enterprises used paid cloud services in 2025”, 3 February 2026.



[10] OECD, “Cross-border data flows”; OECD describes Data Free Flow with Trust as promoting free flow of data while ensuring trust in privacy, security and intellectual property rights, and identifies adequacy, intergovernmental arrangements, trade agreements, standards and privacy-enhancing technologies as complementary instruments. Global CBPR Forum, “About the Global CBPR Forum”; the Forum administers CBPR and PRP systems and aims to facilitate data protection and free flow of data globally.

