A Human-centric Roadmap for Europe

Aligning competitiveness and digital sovereignty with European values

Europe is at a crossroads, compelled to strengthen the competitiveness of businesses and to protect European digital sovereignty, while realising the vision of a single European digital market that protects and advances European values and the rights of its citizens. These competing imperatives imply trade-offs and balancing of priorities, but a human-centric approach to data policy provides a tool through which they can be aligned.

Human-centric data governance is a core concept of the European Data Strategy, but is rarely operationally defined, and has been used so casually and disingenuously that it has lost much of its meaning in popular discourse. In contrast, MyData understands human-centricity as giving individual people control and agency over the data about them, through a very specific set of operational principles, and how this in turn can create value for businesses, innovators, markets and societies. Members of the MyData community, including businesses, public sector agencies, researchers and data intermediaries, have been demonstrating what this means in practice for the last decade.

This roadmap describes how human-centric data governance can be a decisive tool for the European Commission in its work to strengthen and preserve the European digital single market.

Executive summary

While regulatory leadership has helped establish the EU as a global benchmark in data protection, this has not yet translated into digital competitiveness or economic leadership. The gap is widening as data-intensive sectors become increasingly central to economic growth and strategic autonomy. Europe's digital future depends on its ability to accelerate competitiveness while maintaining foundational European values of fairness, accountability, interoperability, and citizen empowerment, as articulated in the European Data Strategy and the Declaration on Digital Rights and Principles.

This roadmap proposes a concrete path forward. It presents human-centric data governance not as an abstract principle, but as a practical and scalable set of tools that empower individuals, unlock data value, and build trust, while reducing regulatory burdens and stimulating innovation. Based on a decade of practical and cross-sectoral experience in the MyData community, this approach has the potential to help the EU turn rights-based regulation into a competitive advantage.

In the lead-up to the European Data Union Strategy and Digital Package in 2025, the Commission has a unique opportunity to realign its digital agenda. This roadmap outlines five strategic recommendations to help the EU achieve this alignment by fostering ethical innovation, building resilient infrastructure, and reasserting its leadership on the global stage:

A. Create Market Incentives for Human-Centric Services
B. Set the next stage of AI development on a foundation of trust
C. Emphasise European Values in the Digital Package
D. Complement Cloud Investments with Edge Sovereignty
E. Reassert European Leadership Through Values-Based Partnerships

Each of these recommendations is accompanied by four concrete actions that we suggest the Commission consider in preparation of the European Data Union Strategy and the Digital Package scheduled for presentation to the European Parliament at the end of 2025.

A. Create Market Incentives for Human-Centric Services
In order to facilitate human-centric innovation and market value, the Commission should establish an incentive structure that rewards companies adopting ethical and user-centric data practices. Define a distinct category of human-centric data holders and processors based on operational criteria like consent management, personal data control, and fiduciary duties.

1. Provide public procurement and R&D advantages to qualifying firms, such as preferential evaluation or sandbox access.
2. Encourage Member States to offer tax incentives similar to green or R&D taxonomies.
3. Pilot a European Public DPO Service to reduce compliance burdens for SMEs committed to ethical data practices.
4. Create compliance and reporting exemptions for qualifying entities across GDPR and DGA obligations.

B. Promote Human-Centricity Across the AI Value Chain

To holistically and meaningfully support the development of trust-based AI systems and services across Europe, the Commission should explore mechanisms to embed human-centricity and people's agency across the AI value chain, from data collection to model deployment and refinement.

5. Embed sovereignty requirements in the Cloud and AI Development Act, ensuring support for data portability, reversibility, and personal agency.
6. Future-proof data regulations for the use of fiduciary AI agents by individuals and groups,
7. Pilot human-centric data governance in key Common Data Spaces, such as health, mobility, and skills.
8. Empower the AI Board to develop public participation mechanisms, including marketplaces for voluntary data sharing.

C. Emphasise European Values in the Digital Package

The upcoming digital package will inevitably be built on numerous compromises and trade-offs. The Commission should ensure that efficiency and lower burdens reward and encourage data innovation that is aligned with European values, offering simplification without sacrificing individual rights.

9. Expand the scope of the European Data Union Strategy to include relevant data portability and cloud infrastructure rules.
10. Develop a single compliance pathway for organisations meeting human-centric data standards across multiple regulations.
11. Articulate overarching principles of human-centricity to support clarity and regulatory alignment.
12. Design cross-sector Data Rights Contracts to enable seamless, enforceable control by individuals across services.

D. Complement Cloud Investments with Edge Sovereignty

Current efforts to assert European cloud sovereignty have limitations and should be reinforced with a hybrid digital infrastructure where cloud and edge systems work together to empower individuals, enhance resilience, and reduce dependence on non-EU providers.

13. Mandate cloud–edge interoperability for personal sovereignty architectures, including agent-based delegation and revocability.
14. Mandate EU-wide standards for Sovereign Edge Environments, ensuring user control, auditability, and offline functionality.
15. Create public infrastructure for personal data services, modelled on initiatives like Athumi and tied to the European Digital Identity Wallet.
16. Condition EU-funded AI and edge projects on support for decentralised and sovereign data architectures.

E. Reassert European Leadership Through Values-Based Partnerships

The new International Digital Strategy should be elaborated to export human-centric governance by embedding operational safeguards in international instruments and fostering coalitions with aligned countries.

17. Promote mutual recognition of user rights through trade agreements and adequacy decisions, supported by inter-DG coordination and model clauses.
18. Establish recognition mechanisms for trusted intermediaries, aligned with Recommendation A's criteria and enforced via Digital Partnerships and MOUs.
19. Pilot sovereign data hosting agreements, modelled on Estonia's data embassy concept, and tied to cloud governance.
20. Launch a Joint Initiative on Human-Centric Data Governance with partner countries to align policy, standards, and experimentation with European values.

Competing imperatives for Europe

The European Union is at a pivotal moment in asserting a common market that leverages data for the benefit of society and for people. The Commission has been mandated with somewhat competing objectives: to simplify and implement a broad swath of groundbreaking data regulations aimed at simultaneously facilitating and reinforcing Europe's competitiveness and digital sovereignty, *and* ensuring that the European data market and regulatory framework protect and promote European values.

The challenge is in many ways structural. While the EU has established itself as a global leader in rights-based regulation and data protection through frameworks like the GDPR, evidence suggests this leadership has not translated into comparable economic and societal advantages. Shortfalls in GDP and venture capital investments of other economies are exacerbated by recent developments in artificial intelligence, blockchain applications, and other data-driven technologies. Simultaneously, recent investments in such technologies in the US and in China highlight the importance of a European values-driven approach to data policy that pursues benefits for individuals and societies as an overarching priority. European regulators are faced with the seemingly irreconcilable demands to relax red tape and regulatory demands so that European innovators can flourish and compete, while also ensuring that Europeans' digital rights are protected and promoted.

The MyData approach helps to square this circle, constraining the worst tendencies of bad actors in an imperfectly unregulated market, while creating opportunities for innovators and markets to flourish by empowering consumers. As the Commission elaborates the scope and focus of the European Data Union Strategy,[1] it should consider how the human-centric approach can institute structural changes that maintain strong regulatory constraints for incumbent and monopolistic technology companies, while removing red tape and creating opportunities for innovative businesses that create value for European citizens and the European market.

Human-centricity is not just a buzzword or a principle. Strictly conceptualised, a human-centric approach to data policy and services provides a concrete set of tools for empowering competitiveness and innovation, while reinforcing the values on which the European Data Strategy was based. Our current data environment is dominated by incumbent technology players whose services masquerade as "free" but in reality rely on

[1] European Commission, 2025

an exploitative model of data collection and advertising that costs European citizens, inhibits European competitors, and results in poorer services and consumer trust. This is the natural consequence of continued monopolistic dynamics in the global data economy, and a human-centric approach to empowering consumers with meaningful choice and data agency is a critical tool with which it can be combated. Europe does not need hyperscalers or its own incumbent technology players to be competitive. It needs a different model for a more level playing field.

This Roadmap provides a snapshot of the current environment since the 2020 EU strategy for data, and describes the benefits of a human-centric approach as a tool for addressing these challenges, before providing specific recommendations and proposals.

Landscape analysis

The GDPR and 2020 EU Data Strategy have established a global benchmark for data governance, influencing frameworks from California to China. While the EU's human-centric approach remains relevant, the data landscape has evolved dramatically since 2020, creating new challenges that require adaptation. The EU has expanded its regulatory framework through the Digital Services Act, Digital Markets Act, Data Governance Act, Data Act, AI Act, and European Health Data Space regulation, yet implementation gaps have limited their impact. Most notably, real-time data portability provisions in the DMA remain largely theoretical, while GDPR enforcement faces procedural obstacles and capacity constraints across Member States.

The rapid emergence of large language models and generative AI has transformed the data landscape, with the EU accounting for only 17% of foundation model development since 2017. This technological shift occurs amid intensifying global competition, with the productivity gap between the EU and US continuing to widen in data-intensive sectors. China's state-sponsored competition and geopolitical tensions around semiconductors and rare earth minerals further increase pressure for strategic autonomy in digital infrastructure. Meanwhile, regulatory innovation outside Europe – including India's ONDC retail ecosystem, Japan's data banking system, and smart data ecosystems in South Korea and the UK – demonstrates alternative approaches to stimulating markets.

Despite regulatory focus on data spaces, data sharing remains inhibited by multiple factors, restraining the European digital market's potential. The negative network effects targeted by the Data Act and Digital Markets Act persist, with no signs of structural changes to mitigate algorithmic self-preferencing, data lock-in, and multi-service ecosystem dependencies that contribute to monopolistic data silos. This market concentration is further complicated by the dominance of "personalised" AI services oriented toward corporate interests rather than "personal AI" designed for user empowerment.

The complexity of foundation models can lead to consumer disengagement with data control, occurring against a backdrop of declining trust in digital services. Growing public skepticism toward data collection and use threatens the adoption of digital services and raises questions about traditional consent mechanisms. This trust deficit is particularly significant as Europe faces a continuing degradation of social trust, and data scandals regularly dominate the news cycle. While regulatory measures and technological advances continue apace, trust-based initiatives remain sporadic and speculative, without corresponding investment in an evidence-based approach to building systemic trust.

Current legal frameworks present additional challenges, as the definition of personal data fails to address other data types with personal impacts that individuals might wish to control. This definitional limitation is particularly problematic in the context of AI, where discourse about individual data empowerment and protections fails to engage with important human outcomes related to non-personal data. Simultaneously, novel governance mechanisms, including data stewardship, data trusts, and social licenses for data have emerged, challenging traditional notions of top-down data governance by data "owners" but lacking clear pathways to scale.

The European cloud market presents another significant concern, with European providers holding a minor share, which implies reliance on US-based hyperscalers. This dependency creates potential vulnerabilities in data sovereignty, including exposure to foreign surveillance, loss of strategic control, and challenges in ensuring compliance with EU laws, particularly given recent political developments in the US and their inherent unpredictability.

Despite dramatic investments in infrastructure such as the Common European Data Spaces, specific business models for data sharing remain few and largely hypothetical. Without clear economic incentives for participation, the ecosystems and infrastructure being developed are unlikely to succeed. This uncertainty disproportionately affects European SMEs, which experience EU regulations primarily as costs and obstacles rather than opportunities, feeling underrepresented in regulatory discussions that shape the digital market.

The delayed implementation of key regulations, particularly the European Health Data Space, represents a significant opportunity cost for advancing human-centric solutions and individual data empowerment. The EHDS has substantial potential to demonstrate how a human-centric approach to personal data management can create value for individuals, businesses, and society while improving quality of life and personal outcomes. Its stalled progress mirrors broader challenges in achieving legal and procedural interoperability for cross-border data flows, even in the most advanced regulatory and technological contexts.

As the term "human-centric" becomes increasingly common but rarely clearly defined, there is a risk of diluting the normative vision of protecting and empowering individual users that underpinned the original European Data Strategy. The evolution of the data landscape demands a renewed commitment to this vision, coupled with pragmatic solutions to the complex challenges facing Europe's data economy.

Data empowerment: catalysing innovation and sovereignty

The MyData approach is a framework that emphasises **individual control, transparency, and interoperability.** It sees data as a resource that should benefit individuals, businesses, and society, but whose full potential is blocked by the de facto control over data exercised by a small number of large organisations operating with outsized network effects and incumbent advantages. It asserts a set of principles and governance models for giving individuals control over their data, and thereby facilitating data portability and re-use, creating value for people, business and societies.

Implementing these principles can enhance competitiveness by fostering market efficiency and innovation, strengthening the quality of data and outputs for European AI factories, and raising consumer expectations in the market for stronger data autonomy and better services. Empowering individuals to share their data seamlessly between service providers requires interoperability at technical, semantic, and organisational registers, disrupting entrenched data silos that are often controlled by large corporations, and creating a more level playing field. By enabling data to flow more freely while maintaining user control and privacy, MyData unlocks opportunities for startups and SMEs to innovate. SMEs, often constrained by limited access to data, can use this framework to compete on a more equal footing with larger companies, driving growth and diversity in the European market.

This practical emphasis on interoperability demands development and adherence to open standards and secure data-sharing protocols, which are a precondition for seamless cross-border and cross-sectoral data flows. The development of services and infrastructure in parallel with standards setting helps to strengthen the sustainability and uptake of large-scale ecosystem investments like Common European Data Spaces.

Importantly, the MyData approach facilitates the development of new business models based on the portability and re-use of data currently inhibited by market forces. This potential can be seen in the launch and development of data intermediaries that have been awarded Operator status by MyData Global for how they operationalise the idea of human-centric data in practice in Europe and beyond. Regulatory measures to support such novel business models also contribute to the quality of competition in the European data market.

Lastly, it is worth noting that this approach has the potential to advance compliance by design, insofar as governance models and infrastructures that empower individuals with control over their data will categorically limit access to personal data, and thereby reduce the potential for malfeasance and non-compliance, and by extension, the costs of compliance and regulatory monitoring.

Innovation in empowering users with agency has the additional advantage of building **trust in digital products and services.** Trust is a cornerstone of competitiveness in the

digital age. As data scandals and misuse erode consumer confidence, companies that prioritise privacy and transparency can be expected to gain a significant market advantage. The MyData approach inherently embeds trust into its framework by giving individuals greater control over their data and ensuring that data use aligns with their expectations. This trust-centric model can enhance user engagement, foster customer loyalty, reduce bureaucracy, and drive the adoption of digital services, ultimately contributing to economic growth.

The majority of platforms and services that have implemented this human-centric approach have done so by placing people's data directly under their exclusive control, either in the form of personal data stores or through specific governance agreements. This has the potential to directly address **European sovereignty** concerns by pushing data control to the edge and reducing control by non-European companies or in jurisdictions where the enforceability of GDPR and related regulations is suspect. This shift encourages the growth of European alternatives that are better aligned with EU values and regulations.

In summary, this approach to human-centric data empowerment and governance can offer three key advantages to regulators seeking to align European competitiveness and strategic autonomy with European values:

First, this approach destabilises the tension between regulation and innovation. By creating structured yet flexible frameworks for data governance, it **allows businesses to innovate without compromising on individual rights or privacy**. Structurally embedding human-centric data sharing and decentralised data control with the individual as the point of integration reduces the need for heavy regulatory oversight, enabling a more dynamic and adaptable market environment.

Secondly, the MyData approach views individuals not as passive subjects but as **active agents** in the data economy. By giving people greater control over their data, MyData transforms data into a shared resource that benefits both individuals and society. This aligns with the European declaration on digital rights and principles, and also has uncertain but promising potential for strengthening and actualising individuals as European digital agents, consumers, and citizens.

Finally, MyData provides a blueprint for **ethical competitiveness**. In an era where data ethics are increasingly scrutinised, and trust deficits are exacerbated by political polarisation and geopolitical conflict, Europe's commitment to privacy and trust can become a global benchmark. Thought leadership by the MyData community in the areas of children's data rights, consent, and regulatory technology provide an asset for the design of human-centric European data policy. By demonstrating that a human-centric approach can coexist with economic competitiveness, Europe can lead the way in creating digital markets that are both thriving and values-driven.

Recommendations and concrete actions

A: Create **market incentives** for human-centric services, products, and infrastructure.

The European Commission should establish concrete economic incentives that reward businesses for developing and implementing human-centric and ethically sustainable data practices. This should be based on clear criteria, combining clear financial benefits with advantages for market position and reduced compliance costs, to stimulate innovation and competition that aligns with European values.

To determine which businesses and organisations should be eligible for these incentives, the Commission should consider establishing a distinct category for human-centric data practitioners. This category should be based on verified practices, contractual obligations, or product or service architectures that align with the concept of human-centric data practices, as articulated in the European Data Strategy and the MyData Declaration. This may include some or all of the following:

- The implementation of full user transparency, access, and control over data sharing and integration,
- The implementation of tools to exercise data portability rights under the GDPR and the Data Act, including revocation of consent,
- Auditable user consent and audit trails enabling explainable data lineage,
- Personal data fiduciary duties to individual consumers and users,
- Open APIs and interoperable, standards-aligned architectures (e.g., Solid, SSI, UMA)

Concrete actions:

1. *Provide public procurement & market access incentives,* such as (a) preferential scoring and weighted evaluation criteria for EU-funded public procurement tenders and R&D calls, (b) exclusive eligibility for pre-commercial Procurement (PCP) Pilots to co-develop solutions with public authorities, (c) preferential access to AI Sandboxes and AI Factories or (d) lowered entry requirements or co-financing obligations on public procurements or grants.

2. Encourage Member States to adopt *coordinated national tax incentives* for businesses that meet these criteria, including tax relief or credits, similar to the incentives created through R&D tax incentives and green taxonomies.[2]

[2] https://finance.ec.europa.eu/sustainable-finance/tools-and-standards/eu-taxonomy-sustainable-activities_en

3. Pilot a *European Public DPO Service* to provide on-call, pro bono data protection officers for SMEs committed to human-centric data practices but unable to afford full-time compliance expertise. Modeled on the principle of public defenders in the legal system, this service would uphold the fundamental right to data protection by ensuring that ethical small businesses are not penalized for their size. Funded through existing SME or digital transformation programs, the service would lower compliance burdens, prevent violations, and promote responsible innovation aligned with EU values.

4. Create *compliance and reporting exemptions*, including exemptions for the DGA's annual activity reporting requirement for DISPs and DAOs, the GDPR's Data protection impact assessments (DPIAs) requirement, and GDPR ROPA obligations for all companies that meet these criteria, regardless of size.

B: Set the next stage of AI development on a foundation of trust

As Europe transitions beyond the era of foundational models towards widespread deployment of operational, embedded, and user-facing AI systems, there is a pressing need to establish a strong foundation of trust, accountability, and individual empowerment. This next stage of AI development shape the competitiveness of European innovation and fundamentally influence how individuals, communities, and institutions interact with AI in their daily lives.

To align with the AI Continent Action Plan, particularly Pillars 2, 3 and 5, the Data Union Strategy should aim to enable individuals and groups to effectively exercise their rights through emerging tools and technologies. Maximising individual agency and capacity in this regard will help to produce high-quality data for the AI continent strategy, while fostering a resilient and competitive AI ecosystem grounded in trust.

Concrete actions:

5. Use the *Cloud and AI Development Act to embed individual data sovereignty requirements from the ground up*. To ensure that cloud and AI systems are structurally aligned with the rights, preferences, and agency of individuals, the Act should mandate "sovereignty by design"—requiring technical and governance frameworks that give natural persons meaningful control over how their data is accessed, shared, and used in AI workflows. The core principles elaborated in Recommendation A should be enforced through interoperable interfaces and auditability mechanisms. Embedding these requirements can be achieved through a combination of infrastructure rules that mandate support for human-controlled data storage interfaces, require auditable data lineage tools within AI development environments and cloud data pipelines, and technical standards for integrating individual data permissions into compute workflows.

6. *Future-proof data regulations for the use of fiduciary AI agents* by individuals and groups, to increase the capacity of European citizens and consumers to effectively exercise their digital rights at scale and with the help of emerging technologies. In anticipation of the emergence of AI Agents that help people to manage complex data sharing preferences and ecosystems, the Commission should ensure that regulatory language describing the delegation and exercise of rights, including consent, revocation and data portability rights, does not create uncertainty or legal obstacles to the use of such agents by European individuals or groups. In particular, the Commission should review GDPR Article 80 on delegation, DGA Chapter 3 definitions of intermediaries, and DMA Chapter 9 on data portability, to remove language that might be misused by data processors or data controllers seeking to refuse legitimate requests and consent preferences exercised through AI agents.

7. *Pilot the production of human-centric data for AI Factories through data spaces.* Establish governance frameworks based on human-centricity and individual empowerment for the EU Common Data Spaces that are most likely to engage with natural persons and personal data (eg: Health, Skills, Finance, Energy, Smart Cities, and Mobility) as a means for producing discrete high-quality data sets for use in Europe's AI factories and Data Labs. Instruct the Data Spaces Support Centre to develop and disseminate resources and guidance on developing such governance frameworks, including rulebooks, rolebooks, and codes of conduct that elaborate the involvement of natural persons and personal data in data spaces. Clarify legal grounds for processing personal data in the context of data spaces.

8. Instruct the AI Board to *scope mechanisms for public engagement and empowerment of individuals and communities.* To complement the risk-based logic of the AI Act, the AI board should actively cultivate and facilitate the engagement of individuals and groups in AI governance. The AI Board should be mandated to define and promote mechanisms for ongoing public engagement on the AI services, to validate the implementation of safeguards in the AI Act and to strengthen trust-based AI services based on companies' "social license to operate". In particular, the public should be consulted to test and provide feedback on the scope of legitimate interest in the context of the GDPR and AI models. Active and explicit public consultations on AI services and safeguards in Europe should be designed and leveraged to help European companies establish a social license to operate, not just in legal terms, but through demonstrable public alignment and legitimacy. These mechanisms should also help define criteria for human-centric AI certification, aligned with European values of transparency, accountability, and individual agency.

C: Emphasise fundamental European values in the upcoming **digital package.**

The Digital Package,[3] planned for presentation to the European Parliament Q4 2025,[4] is a regulatory initiative aimed at streamlining the EU's expanded digital policy to ensure it better supports SMEs and midcaps through clearer, more coherent, and business-friendly data and compliance rules, and is based on an ongoing fitness check of the EUs digital policy. The EC Communication on Implementation and Simplification explicitly references the European Data Union Strategy as an important contribution to this process,[5] but to date, consultations on the EDUS have focused almost exclusively on assessing the effectiveness and impact of the DGA, the FFDR, and the ODD.[6]

In preparing the digital package, we encourage the commission to:

9. *Enhance the effectiveness of the DGA chapter 3* by specifying intermediary definitions. Specifically, the Art. 10 category of Data Intermediation Service Providers (DISPs) should be complemented with a category of "Data intermediation application service providers" (DIASPs), which would not be subject to the full list of conditions in Art. 12. This adjustment would lower regulatory burdens for European businesses with a strong potential for innovation, while adding clarity to the DGA, and emphasising the Act's dual purpose to both address the market failures resulting from abuse of market power by monopolistic actors, while giving European people and businesses the means and opportunities to benefit from their own data.

10. Develop a *single compliance pathway* for organisations meeting human-centric data management standards across all digital regulations (see Recommendation A). This could be operationalised through a principle of "regulatory equivalence," whereby demonstration of individual consumers' agency and control over their data satisfies regulatory obligations across multiple acts and sectors. This

---

[3] The EC Communication on Implementation and Simplification notes (https://commission.europa.eu/document/download/8556fc33-48a3-4a96-94e8-8ecacef1ea18_en?filename=250201_Simplification_Communication_en.pdf, pg 6) that the Digital Package will build on an evaluation of "whether the expanded digital acquis [defined in footnote as "the General Data Protection Regulation, the Data Governance Act, the Data Act, the Cybersecurity Act, the Cyber Resilience Act, the EU Chips Act and the Artificial Intelligence Act"] adequately reflects the needs and constraints of businesses such as SMEs and small midcaps, going beyond necessary guidance and standards that facilitate compliance. Among others, a European Data Union Strategy will address existing data rules to ensure a simplified, clear and coherent legal framework for businesses and administrations to share data seamlessly and at scale, while respecting high privacy and security standards."

[4] The 2025 Commission work programme - Annex 1 (https://commission.europa.eu/document/download/7617998c-86e6-4a74-b33c-249e8a7938cd_en?filename=COM_2025_45_1_annexes_EN.pdf) lists new initiatives included in the 2025 Work Plan, including a "Digital package (legislative, incl. impact assessment, Q4 2025)".

[5] Ibid.

[6] See, for example, the 'Have Your Say' questionnaire on the European Data Union Strategy at https://ec.europa.eu/eusurvey/runner/PC_DUS2025?surveylanguage=en.

approach could be further strengthened by providing "compliance by design" templates that inherently satisfy multiple regulations through human-centric architecture.

11. Develop *"Data Rights Contracts"* for individual consumers and citizens that operate seamlessly across sectors and existing EU regulations. These contracts would serve as legally and technically actionable frameworks through which individuals and organisations can agree on the terms of data access, usage, sharing, retention, and withdrawal. By offering a harmonised layer that aligns with the GDPR, Data Act, Digital Markets Act, and sectoral data spaces (e.g. health, mobility, skills), Data Rights Contracts would reduce legal friction, simplify compliance, and enhance trust between data holders and data contributors. They could be implemented as modular templates, capable of being enforced via APIs or smart contracts, and could be managed on behalf of individuals by trusted intermediaries.

12. *Ensure a broad regulatory scope and mandate for the European Data Union Strategy* to ensure a coherent approach to simplification and enable the Strategy to best identify opportunities to improve regulations for how European companies and citizens engage with data. The scope of the EDUS should not be defined by institutional mandates within the Commission's organisational structure, but should engage meaningfully with the full scope of regulations and initiatives to the extent that they are relevant to its core objectives. At the very least, this should include an assessment of regulatory requirements and criteria that are common across regulations (eg: data portability requirements in the GDPR (Article 20), the Data Act (Articles 4–6, 23–26), the DMA (Article 6(9)), the Payment Services Directive 2 (PSD2) (Articles 66–67), and the European Health Data Space (EHDS) (Articles 3–4, 14), and key substantive issues like that of the European cloud and digital identity, which are addressed by initiatives and investments in addition to regulation.

D: Complement cloud investments with infrastructure for personal sovereignty at the edge.

Recognising the practical and economic constraints on rapidly expanding the market share of European cloud providers, the Commission should invest heavily in edge computing infrastructure that provides data sovereignty to European consumers and citizens. By pushing data sovereignty to the edge, Europe can reduce its dependence on foreign cloud infrastructure whilst creating new opportunities for European technology providers specialising in personal data management solutions.

This could be pursued through the following concrete actions:

13. *Mandate Cloud–Edge Interoperability for Personal Sovereignty Architectures* Require infrastructure developed under the Cloud and AI Development Act—including AI Gigafactories, Data Labs, and related services—to implement robust integration pathways with human-controlled environments operating at the edge. This includes requiring standardised APIs, harmonised data formats, and secure exchange protocols to support cross-boundary functions such as dynamic consent signalling, data revocation, and agent-based delegation. These interoperability requirements should ensure that centralised cloud services can interface with decentralised personal data systems—such as personal data stores, wallets, and user-deployed agents—without overriding individual control or data minimisation principles. The Cloud and AI Development Act should allocate funding for testing and validating such interfaces under real-world deployment scenarios.

14. *Mandate EU-Wide Standards for Sovereign Edge Environments* The Commission should use delegated or implementing acts to develop technical specifications for "Sovereign Data Nodes"—defined as user-controlled, edge-hosted environments capable of independently managing personal data and executing AI functions. These standards should cover local consent management, data lifecycle auditing, verifiable minimisation, and offline operation. While compatibility with cloud-based services must be maintained, the emphasis should be on enabling autonomous edge-based governance of data, including the ability to function under limited or no connectivity. This creates a baseline for sovereignty-first architectures, ensuring that individuals and small-scale operators retain effective control regardless of upstream cloud integration and local connectivity.

15. Create *Public Infrastructure for Personal Services and Data Sovereignty*. The Commission should initiate a European Personal Cloud programme, administered at either the Union or Member State level, that enables individuals to access secure, sovereign digital storage and compute capacity under their own control. This could be modelled on existing initiatives such as the infrastructure developed by the Flemish Public Data Utility, Athumi, could leverage architectures like Solid, and could interoperate with the European Digital Identity Wallet to foster third-party innovative services and facilitate seamless user control across public and private digital services.

16. *Condition EU-Funded AI and Edge Projects* on Sovereign Data Compatibility. All AI development environments and edge computing infrastructure supported directly or indirectly by EU funds should be required to demonstrate compatibility with decentralised data architectures. This includes infrastructure such as AI Gigafactories and edge nodes, which must be designed to support user-hosted

agents, permit fine-grained user control over data input and withdrawal, and maintain compliance with the principle of data minimisation under the GDPR.

E: Leverage a values-driven approach to reassert European leadership and influence

The EU's new International Digital Strategy asserts the geopolitical centrality of digital policy and promotes Europe as a trusted global partner. In order to effectively assert European values of human-centricity on the global stage, implementation of the strategy should deepen its practical commitment to human-centric data governance beyond lip service, and as concrete systems of digital operations, institutions, and market practices that can be exported, scaled, and adapted. To anchor Europe's international digital engagement in European values, the Commission should take steps to embed personal data sovereignty measures into cooperation efforts. Specific measures related to functional equivalency recognition, agent-based control models, and sovereign hosting frameworks should be embedded into relevant diplomatic, trade, and technical cooperation instruments to effectively promote and disseminate Europe's rights-based approach through joint initiatives, mutual recognition mechanisms, and multilateral coalitions. By positioning Europe as the premium market for trustworthy digital services and actively exporting its human-centric approach through trade agreements and technical standards, the Commission can shape global data governance norms whilst strengthening European competitiveness in values-driven digital markets.

17. *Promote Human-Centric Standards Through International Agreements and Trade.* The Commission should ensure that international data flow frameworks negotiated through trade agreements and adequacy decisions include reciprocal provisions for individual data portability, revocability, and agent-based control (see Recommendation A). Rather than imposing GDPR compliance per se, the EU should promote mutual recognition frameworks that align on functionally equivalent rights and emphasise data governance frameworks that prioritise the control and empowerment of citizens and consumers, particularly in emerging digital partnerships. Inter-DG coordination should be initiated between DGs TRADE, JUST, and CNECT (potentially an inter-service task force or working group), mandated to elaborate model clauses and to provide interpretative guidance on how individual data rights such as portability, revocability, and agent-based control can be integrated into trade agreements and bilateral instruments. These tools would support functionally equivalent protections for natural persons in cross-border data flows and provide a common reference for future negotiations with value-aligned countries.

18. *Establish Mutual Recognition of Functionally Equivalent Data Intermediaries* The inter-DG coordination described above should also be tasked with

elaborating criteria, model clauses, and assurance mechanisms for the recognition of functionally equivalent data intermediaries operating in third countries and entrusted to uphold user control, consent, revocability, and purpose limitation across jurisdictions. The criteria for such recognition should align with those proposed under Recommendation A, which proposed a distinct category of human-centric data practitioners. This should be operationalised through instruments such as Digital Partnership Agreements, data governance MOUs, and international cooperation frameworks (e.g., G7, OECD). Model clauses developed for this purpose would serve as contractual foundations for cross-border data processing involving recognised intermediaries, supporting legally robust and rights-respecting personal data flows beyond the Union.

19. *Pilot Sovereign Data Hosting Agreements*

The Commission should advance the development of Sovereign Data Hosting Agreements, modelled on Estonia's "data embassy" approach, to ensure that EU personal data stored or processed outside the Union remains subject to EU law and rights-based governance. These agreements should include enforceable legal, technical, and contractual safeguards, particularly for cloud and edge infrastructure, and should be included as a governance mechanism under the forthcoming Cloud and AI Development Act. To demonstrate feasibility, the Commission should pilot such agreements with aligned partners that benefit from reciprocal adequacy or digital cooperation frameworks, such as Japan, South Korea, or Canada. This approach would strengthen legal continuity, enhance digital strategic autonomy, and offer a scalable model for exporting Europe's trusted data governance standards.

20. *Assert Global Leadership together with Values-Aligned Countries*

The Commission should establish a Joint Initiative on Human-Centric Data Governance with strategic partner countries under existing or planned Digital Partnerships. This should provide a structured forum to coordinate policy, regulatory, and technical approaches to promoting personal data sovereignty and innovation-friendly data sharing. It should support the development and alignment of model clauses, institutional templates, and implementation tools for mechanisms such as sovereign hosting and recognition of functionally equivalent intermediaries described above, while also enabling cross-border experimentation through sectoral pilots. Engagement with expert and practitioner networks already developing user-centric data governance models will ensure that European values are translated into globally relevant operational practice.

References

Bloomberg Law. 2024. "Trump's Privacy Board Purge Threatens EU-US Data Transfer Pact." Accessed January 26, 2025. https://news.bloomberglaw.com/health-law-and-business/trumps-privacy-board-purge-threatens-eu-us-data-transfer-pact.

D.A. Consortium Inc. 2018. "D.A. Consortium, Hitachi and Japan Post to Begin Verification Test of 'Information Bank.'" September 10, 2018. Accessed February 2, 2025. https://www.dac.co.jp/english/press/2018/20180910_ib.

Draghi, Mario. 2024. *The Future of European Competitiveness.* European Commission. Accessed January 26, 2025. https://commission.europa.eu/topics/strengthening-european-competitiveness/eu-competitiveness-looking-ahead_en.

European Commission. 2024a. *European Data Market Study 2024–2026: First Landscape Study.* Brussels: European Union. Accessed January 26, 2025. https://digital-strategy.ec.europa.eu/en/library/results-european-data-market-study-2024-2026.

European Commission. 2024b. *The Digital Decade.* Special Eurobarometer 551. Accessed February 2, 2025. https://europa.eu/eurobarometer/surveys/detail/3174.

European Commission. 2025. "Commission Unveils New Strategy on How Productivity Will Be Boosted by Digital Tech." Accessed January 26, 2025. https://data.europa.eu/en/news-events/news/commission-unveils-new-strategy-how-productivity-will-be-boost-digital-tech.

Eurofound. 2024. "Trust in Crisis: Europe's Social Contract Under Threat." Accessed January 26, 2025. https://www.eurofound.europa.eu/en/blog/2024/trust-crisis-europes-social-contract-under-threat.

Jean Monnet Program. n.d. *Institutional Challenges in EU Regulatory Frameworks.* Accessed January 26, 2025. https://www.jeanmonnetprogram.org/archive/papers/01/010301-04.html.

Konrad-Adenauer-Stiftung. "Cadenabbia Memorandum on the European Cloud Policy." Last modified December 5, 2023. https://www.kas.de/de/monitor/detail/-/content/cadenabbia-memorandum-on-the-european-cloud-policy.

Letta, Enrico. 2024. *Much More Than a Market: Report on European Competitiveness.* European Council. Accessed January 26, 2025.

https://www.consilium.europa.eu/media/ny3j24sm/much-more-than-a-market-report-by-enrico-letta.pdf.

MyData Global. 2023. "EU Health Data Space Must Be Individual-Centric to Benefit All Stakeholders." Published December 13, 2023. Accessed January 26, 2025. https://mydata.org/2023/12/13/eu-health-data-space-must-be-individual-centric-to-benefit-all-stakeholders.

Open Network for Digital Commerce. n.d. "Learn About ONDC." Accessed February 2, 2025. https://ondc.org/learn-about-ondc/.

Salesforce. 2019. "State of the Connected Customer Report Outlines Changing Standards for Customer Engagement." https://www.salesforce.com/company/news-press/stories/2019/06/061219-g/.

Science Europe. 2020. *GDPR-Related Challenges for Cross-border Research Collaboration in the Context of the COVID-19 Pandemic.* Accessed January 26, 2025. https://scienceeurope.org/media/1vyibyds/20200701_gdpr_overview_challenges_solutions_final.pdf.

Svenskt Näringsliv. 2024. *What's Wrong with the GDPR?* Confederation of Swedish Enterprise. Accessed January 26, 2025. https://www.svensktnaringsliv.se/material/skrivelser/xf8sub_whats-wrong-with-the-gdpr-webbpdf_1005076.html.

Telecoms.com. 2024. "European Cloud Players Face Declining Market Share as US Hyperscalers Clean Up." Accessed January 26, 2025. https://www.telecoms.com/public-cloud/european-cloud-players-face-declining-market-share-as-us-hyperscalers-clean-up.

Verhulst, Stefaan G. 2024. "The Need for New Methods to Establish the Social License for Data Reuse." *Medium.* Accessed January 26, 2025. https://medium.com/data-policy/the-need-for-new-methods-to-establish-the-social-license-for-data-reuse-e7c67bdc4aff.

Wilson, C., T. Davies, V. Narayan, A. Airan, V. Lähteenoja, C. Rossini, and S. Tomlinson. 2023. *In This Together: Combining Individual and Collective Strategies to Confront Data Power.* MyData Global. Accessed January 26, 2025. https://mydata.org/publications.

About MyData

MyData Global is an award-winning non-profit registered in Finland, with members in over 40 countries and across six continents. The MyData Operators group includes over 70 data intermediaries that have satisfied the technical criteria of human-centricity as elaborated in the MyData White Paper. MyData is named in the EU Data Strategy as a movement that empowers consumers with granular control in response to "risks of discrimination, unfair practices and 'lock-in' effects." More information is available at https://mydata.org/.

About this publication

Citation information: MyData (2025) Roadmap for Europe: Aligning competitiveness and digital sovereignty with European values.

Published July 18 1, 2025.

Download this publication at https://mydata.org/publications

Join MyData Global at mydata.org/membership
Email us at hello@mydata.org
Follow us on X @mydataorg
Visit us at mydata.org