Homo Digitalis submission to the public consultation on the European Data Union Strategy

We appreciate the opportunity to provide input on the European Commission's Data Union Strategy. While we support efforts to enhance coherence and clarity in the EU's data governance and acknowledge the goal of harnessing data for innovation and public benefit, we are concerned that the current approach may undermine existing safeguards in the name of simplification and competitiveness.

To ensure public trust and accountability, the Strategy must uphold and strengthen the protections established by the GDPR, the ePrivacy framework, and other relevant laws, in line with the EU Charter of Fundamental Rights.

1. Fundamental Rights are Essential, Not Obstacles

The Strategy seems to present legal tools such as the GDPR and ePrivacy rules as impediments to data access and reuse. Although implementation challenges exist, they usually result from inconsistent enforcement, political hesitation, and limited institutional resources, rather than from the protective nature of the laws themselves.

Where AI is developed to serve clearly defined public purposes and meets strict ethical, environmental, and governance requirements, publicly held datasets can be helpful. However, such initiatives must respect consent, transparency, and accountability at all times.

Legal clarity and practical guidance are welcome, but simplifying data governance must not weaken core principles such as purpose limitation, legal basis, data minimisation, and access to redress. These are foundational to public confidence and must not be dismissed as technical difficulties. We are particularly worried about proposals that could sidestep the GDPR via new regulations, which might dilute protections and oversight while avoiding formal reform.

The rights to privacy and confidentiality, as reflected in the withdrawn ePrivacy Regulation proposal, must continue to shape the EU's data governance. Withdrawal of the proposal should not be seen as an opportunity to reduce these protections. Instead, these rights should be preserved and integrated into all future policy and legislation under the Data Union framework.

The GDPR and ePrivacy frameworks must not be included in any future efforts to simplify or consolidate legislation. Instead, the focus should be on ensuring their full enforcement, consistency, and robust implementation. These legal tools are central to safeguarding personal data and must remain pillars of the EU's regulatory landscape.

2. Data availability Requires Robust Safeguards

We agree with the goal of making high-quality data more accessible for socially beneficial uses. However, the Strategy downplays the potential harms of industrial and non-personal data. In practice, much of this data, especially from IoT devices and platforms, can reveal personal information, enable profiling, or be repurposed in harmful ways.

The idea that more data automatically drives innovation must be challenged. Any broadening of access should be justified by a clear public interest and protected by enforceable safeguards.

Even pseudonymised or synthetic data can replicate bias or lead to discrimination, especially in AI applications. Therefore, access systems must include strict purpose limitations, strong technical measures, and data protection impact assessments where needed.

Publicly funded projects like data spaces or AI platforms should model strong safeguards, not enable opaque or exploitative practices. We must not assume that public investment automatically leads to public benefit. AI deployment must align with rights-based and ecological standards, taking into account the environmental costs of materials extraction, energy consumption, and ecosystem damage. Reusability must not compromise accountability, and interoperability must not become an excuse for unrestricted data use.

We endorse the European Parliament's 2021 Resolution on the Data Strategy, particularly its emphasis on grounding data governance in fundamental rights, transparency, and civic participation. The Resolution rightly notes the dangers of viewing industrial or non-personal data as neutral and promotes decentralised infrastructure and public control. These values should be more prominently embedded in the Strategy to prevent market concentration and monopolisation.

3. The GDPR is a Foundational, Not a Hurdle

The Data Act does not provide a legal basis for processing personal data. Any sharing or access involving such data must comply fully with the GDPR and ePrivacy framework. This legal complexity creates a real risk of unlawful processing, especially by third parties. We are concerned that the Strategy's references to flexibility and adaptability could be interpreted as encouragement to reinterpret or weaken the GDPR, something that is already occurring in other contexts.

While sector-specific guidance and improved cooperation between regulators are necessary, there is no evidence that the GDPR is fundamentally flawed. On the contrary, existing problems often stem from weak enforcement, limited resources, and poor alignment across jurisdictions. Dividing oversight between data protection authorities and new regulators created under the Data Act could undermine enforcement and create confusion. Data protection must remain central.

The EU should invest in improving regulatory capacity and coordination, especially for small and medium-sized enterprises and public sector bodies, rather than pursuing legal changes that might erode data rights.

4. International data flows and the promotion of rights

We understand the importance of international data flows for the digital economy. However, the protection of personal data must remain a core EU value, not a negotiable item in trade discussions.

Safeguards such as adequacy decisions, standard contractual clauses, and risk-based assessments are not protectionist tools. They are necessary to ensure that individuals' rights are respected and that data transfers comply with EU law. We urge caution against any language suggesting that localisation or transfer restrictions are inherently unjustified.

The increasing use of adequacy decisions for political purposes threatens to weaken their legitimacy. A sound data transfer policy must be based on legal substance, not geopolitical

considerations.

We also recommend that digital trade agreements preserve the EU's ability to regulate in the public interest. This includes setting rules around AI transparency, local data storage, and access to source code

5. Governance must be Transparent and Independent

Effective data governance requires transparency, independence, and alignment with fundamental rights. While regulatory coordination is desirable, it must not come at the cost of weakening the independence of data protection authorities or reducing democratic accountability.

Efforts to streamline oversight must reinforce existing structures rather than replace or centralise them. Public interest safeguards, including the involvement of civil society and affected communities, are critical to legitimate and fair governance.

6. Addressing the Environmental Impact of Data

The Strategy must also acknowledge and address the environmental consequences of digital technologies. As highlighted by the European Parliament, the ICT sector already consumes 5 to 9 percent of global electricity and contributes over 2 percent of greenhouse gas emissions. Data centres and cloud infrastructure require vast resources and generate significant waste.

A sustainable data policy must go beyond energy efficiency. It should question the assumption that more data is always better. Publicly funded projects should lead efforts to measure and minimise their environmental impact. This includes promoting data minimisation, circular design, and in some cases, deciding not to pursue certain technologies that are too resource-intensive.

Conclusion

The Data Union Strategy presents an important opportunity to improve how the EU handles data. However, this must be done without compromising fundamental rights or promoting the false idea that regulation holds back innovation. Legal clarity and simplicity can be achieved in ways that preserve dignity, accountability, and long-term public trust.

We urge the Commission and EU policymakers to ensure that this Strategy does not create pressure to roll back safeguards or weaken the Union's ability to respond to data-driven risks. A rights-based approach would enhance accountability, reduce reliance on extractive models, and prioritise the collective good over commercial interests. The focus must be on strong enforcement, not on shifting responsibility away from regulators and rights holders.