

29 January 2021

ITI Comments to the Data Governance Act Proposal

The Information Technology Industry Council (ITI) welcomes the publication of the Data Governance Act proposal from the European Commission. We particularly appreciate the launch of an open consultation providing the opportunity for stakeholders to submit their views on this important proposal.

As the premier advocate for the global technology industry, representing over 70 global companies active across the whole spectrum of technology, ITI and its members believe that preserving an enabling environment for data-driven innovation is essential to ensure Europe's global competitiveness and security. A robust and innovation-friendly framework for data governance is a key element to achieve the fundamental goals of facilitating data re-use and data sharing under clear EU-wide rules.

ITI appreciates the goal of the Data Governance Act to make public sector data more open and reusable, and we support the proposal to create a mechanism to enhance the re-use of sensitive public-sector-held data, with a smart approach that is also geared towards ensuring compliance with third parties' rights. However, **further improvements are needed to the current proposal in order to ensure harmonisation with current legislation, facilitate international data flows and collaboration, enable cloud use and prevent onerous obligations that could lead to unintended barriers for innovation.** In order to guarantee predictability of the legal framework, we encourage policymakers to clarify the scope of application of Chapter III on data-sharing service providers to avoid disrupting successful data collaborations; precisely clarify the conditions protecting commercial confidential information; and ensure that obligations for data-sharing service providers are proportionate and clear.

In addition, more clarity is needed around the provisions regarding international data transfers (articles 5 and 11) and access requests from third countries (articles 11 and 30). As opposed to personal data, non-personal data pose no risks to fundamental rights. Taking this into account, any additional obligations regarding non-personal data should be clearly motivated, proportionate and should avoid unnecessary burdens for companies, which may result in disincentives to data-reuse and data-sharing.

You can find our specific remarks and suggestions below. We appreciate the opportunity to provide feedback at this stage of the legislative process, and we remain committed to serving as a resource to policymakers as this fundamental discussion on data governance progresses.

Reuse of public sector data

ITI shares the Data Governance Act's goal of enhancing the re-use of publicly held data. We believe that open government data is a tremendous source of economic growth that is, as of yet, largely

Global Headquarters
700 K Street NW, Suite 600
Washington, D.C. 20001, USA
+1 202- [REDACTED]

Europe Office
Rue de la Loi 227
Brussels - 1040, Belgium
+32 (0)2 [REDACTED]

@ info@itic.org
 www.itic.org
 @iti_techtweets

untapped. We believe that it can also help addressing societal challenges in relation to environment, healthcare and mobility while creating more responsive and efficient governments and safer cities. The EU can capitalise on this large potential for innovation and economic growth by facilitating the removal of barriers to widespread open data use, including those related to the quality, usability and compatibility of datasets. Ensuring that data is made public under an open license and following an “open by default” principle is a key measure to achieve this goal. For this reason, we welcome a predictable legal framework that allows for re-use of sensitive publicly held data as defined by article 3(1), which we believe can be beneficial for promoting data sharing and re-use and can positively impact innovation.

Article 5 of the proposal leaves it open to each public sector bodies to decide on the conditions to make the data in scope of the Data Governance Act available for reuse. This may create fragmentation and represent a burden for data re-users, thus hindering the creation of a single market for data and running counter to the purpose of the DGA. We therefore encourage to **establish such conditions at Union level to ensure harmonisation**.

ITI welcomes the provisions in article 5(2) calling on public bodies to make sure the conditions for data re-use are proportionate, non-discriminatory, justified and not used to restrict competition. We also note the importance to precisely define how data subject to **commercial confidentiality, trade secrets and intellectual property rights** will be protected from re-use. The absence of clear safeguards may disincentivise industry collaboration with the public sector, limiting flexibility in contracting terms and curtailing innovative business models for data sharing, given the possibility of sensitive commercial information being made available to third parties.

Article 5(4) (a) allows public sector bodies to impose obligations to access and re-use data within a secure processing environment provided and controlled by the public sector. This negates the possibility of using highly secure environments that are provided by the private sector, such as cloud environments. We encourage EU legislators to **focus on the control of the data instead of the ownership or provision of the underlying infrastructure**. The security protections of public clouds can be more robust, scalable, and cost effective than those available on-premise. This is confirmed by independent research including the “Cloud Computing Risk Assessment” conducted by the European Union Agency for Cybersecurity (ENISA). We suggest tweaking the language so as to remove the word “provided”, which seems to assume that cloud services cannot be used for such “secure processing environment”.

We suggest further specifying the language in the second sentence of **Article 5(5)**. The norm as it reads in the Commission’s proposal entitles the public sector body to verify any results of processing of data undertaken by the re-user and reserve the right to prohibit the use of results that contain information jeopardising the rights and interests of third parties. While we agree with the fundamental goal of ensuring the protection of sensitive information, **the possibility for intervention is here overly broad** when broadly referring to third party rights and interests without further safeguards. In order to better reflect this balance, **we suggest further specifying the reference to “third party rights and interests”** with a more precise reference to “clear violation of other’s IP rights, sensitive commercial information, trade secrets or privacy”. In addition, we suggest ensuring the **appropriate due process safeguards** and the possibility to challenge decisions made by public authorities.

We welcome the provisions in article 5(7) laying out that public sector bodies should not exercise the right of the maker of a database as provided by Article 7(1) of Directive 96/9/EC. While the database

right protects the investment of the database maker, public sector bodies do not need to have their investment protected in the same way as companies, as their databases are part of fostering their public mission and not part of an investment or business plan.

More clarity is needed on the definition of “highly sensitive” data as referenced in article 5(11). We recommend that, in order to maximise transparency, **the DGA makes it clear that any such decision should be taken through a regular legislative procedure, instead of relying on delegated acts**, with the involvement of the co-legislators and ensuring the necessary participation of stakeholders.

The establishment of a single information point in Member States as proposed by article 8 is also a welcomed development. We believe such initiative can have a positive role in advancing legal certainty and facilitating access to data for companies.

International Data Transfers of Non-Personal Data Held by Public Authorities

The cross-border movement of data is the lifeblood of all industries and all sectors. Where data flows, growth and innovation follow. Cross-border data flows and access to digital services and technologies enable “born global” small and medium-sized enterprises (SMEs) by offering them new ways to reach customers, markets and technologies. In order to enable the immense potential of digital trade, we believe strong protections for privacy and cybersecurity can and need to go hand-in-hand with the transparent, non-discriminatory transfer of data across borders. The discussions on the Data Governance Act should take into account the importance of global flows of data for innovation and economic growth and incentivise companies to participate in the data economy and collaborate on data across borders.

As various Member States have recently [pointed out](#), ITI believes that the EU should be aligned with like-minded third-countries, bilaterally and in multilateral settings, in an effort to tackle unjustified barriers to digital trade and data flows. We also agree with these Member States that **the EU should distance itself from considering any prohibitive measures like data localisation, or measures of similar nature**.

For this reason, additional clarity is needed as regards the provisions spelled out by **article 5 (7-11)** on safeguards for the international transfers of sensitive and highly-sensitive data held by public authorities. While we agree that it is of the outmost importance to safeguard intellectual property rights and trade secrets, we believe it is also of paramount importance to put in place clear rules that create legal certainty and do not provide disincentives for companies to re-use data. We are especially concerned about the **proportionality** of the suggested measures, which may restrict the flow of non-personal data outside of the EU.

We are concerned about the potential implications of introducing an **“adequacy-like” mechanism** deciding on the level of protection of non-personal data in third countries as **proposed in article 5(9)**. First, this procedure would represent a significant **shift from the current framework** for the transfer of non-personal data. In addition, this mechanism seems to create a considerable workload for the European Commission and/or the entities responsible for implementing the system. Given that non-personal data do not pose the same risks as personal data, for instance with regard to fundamental rights, we are sceptical about the proportionality of introducing such a mechanism.

Secondly, considering the limited number of existing adequacy decisions in the realm of personal data, **there is a risk that the procedure outlined in 5(9) becomes a bottleneck for the transfers of non-personal data** held by public authorities outside of the EU and a disincentive for companies to re-use data, defeating much of the proposal's aims. We urge lawmakers to also **consider the scalability and flexibility of this mechanism**. As it would be based on individual decisions for each third-country, we are doubtful about its adaptability to today's global scale of international transfers. Against this background, the European Commission should take into account long-standing international agreements such as the Berne Convention or the TRIPs agreement that have brought together a number of like-minded countries on IPR protection.

Third, more clarity would be needed around the criteria that will inform the decision that protection of non-personal data granted by a third-country legal framework is equivalent to that of the EU. For instance, it is unclear how the Commission will assess that the third-country legal framework is "effectively applied and enforced," as per article 5(9)(b), or provides "effective judicial redress", as per article 5(9)(c).

Finally, we are concerned about the transparency of the procedure outlined in articles 5(9) and 29 (2). A procedure based on **implementing acts** and assisted by an advisory Committee may lack the necessary transparency and stakeholder participation.

In addition, we urge policymakers to clarify the obligations that would apply to data re-users, as referenced in **recital 16 and article 5(10)**, in cases where the Commission has either not issued an implementing act or the Commission does not find an equal level of protection of non-personal data transferred to a specific third country. In these cases, we support exploring clear and practical paths for data re-users to legally transfer data in absence of an "adequacy-like decision," based on a risk-based approach and considering the sensitivity of the data. As mentioned above, it is important to consider the proportionality of the obligations, especially given that non-personal data do not pose risk for fundamental rights. Overly strict obligations may also run the risk of disincentivising data re-use for companies due to the complexity of the legal framework.

Requirements for Data Sharing Services Providers

ITI welcomes the goal of the proposal to increase trust in data sharing service providers to encourage B2B data sharing and data reuse. We however urge policymakers to **clarify the scope of the requirements for data sharing services providers** as provided by article 9. For instance, the inclusion in the scope of organisations that "make available the technical or other means to enable such services", or those providing "a specific infrastructure for the interconnection of data holders and data users", as specified in article 9(1)(a), seems broad and unclear. In fact, such a broad scope could be read to include the vast majority of current, and successful, contractual B2B data sharing that the Commission wishes to encourage and promote, not disrupt. To increase clarity, we suggest factoring in article 9 a more specific definition of the scope as detailed in recital 22 of this proposal.

It is also unclear whether third-party technology providers that enable data intermediaries "through technical or other means" to provide its intermediation services must also notify that technology. The language in the current text is overly broad and could include anything used by an intermediary to provide its services. We caution against imposing disproportionate and burdensome **notification procedures** on administrative bodies and businesses alike, and question the value of notifying all

means used by an intermediary that enable it to deliver its services, as this could potentially disincentivise, rather than facilitate, greater data collaboration in Europe.

We believe additional clarification is needed with regard to **article 11(7-8)**, referencing an obligation for data sharing service providers to put in place technical, organisational and legal measures to prevent transfers or access to non-personal data that is unlawful under EU law. It is in fact unclear which additional measures should be undertaken in addition to those taken in compliance with existing laws, and which cases and what procedure competent authorities as referenced in article 12 should follow to assess the appropriateness of such measures. Any obligation of such kind needs to be proportionate to the nature of non-personal data and clear in order to avoid legal uncertainty.

Finally, as a general comment on this section of the Data Governance Act proposal (articles 9-13), we strongly encourage policymakers to ensure that the obligations on data sharing for organisations in scope of this section remain consistent with other pieces of legislation that are being discussed at EU level, such as E-Privacy, the Digital Services Act and the Digital Markets Act as well as existing legislation such as the General Data Protection Regulation (GDPR). As the discussions on these files continue in parallel, it is important to make sure that the policy objectives pursued remain compatible in order to ensure legal certainty.

Data Altruism

We welcome the provisions on data altruism put forward in Chapter IV of the Data Governance Act. We believe that a general authorisation framework for data altruism schemes and the harmonised consent form at EU level can have a positive effect in facilitating data sharing and increase availability of data.

European Data Spaces

The Data Governance Act lays important foundations for the future development of voluntary, industry-led European data spaces governed by clear and transparent rules to help companies in Europe and globally seize the potential of large datasets.

ITI firmly believes that participation in European data spaces **should remain voluntary in order to avoid disincentivising investment in data innovation or put at risk IP rights or trade secrets**. Companies are already undertaking significant activities in this field on a voluntary basis. Also, participation should be open, non-discriminatory and not subject to arbitrary conditions. Companies should in all instances remain in full control of their data and not lose any rights on the latter when participating in voluntary data-sharing agreements. Further, extensive data-sharing schemes could put into question how companies can share data but still comply with the EU's existing competition and data protection rules including the GDPR.

In setting up the Data Spaces, there should be a sector-specific business case with clear value proposition for participating companies for each data space. This will be essential to provide incentives for companies to share data and to make data spaces operational.

In addition, **B2B data sharing should remain in all cases voluntary and that contractual freedom should remain the fundamental principle for B2B data sharing**. There are several issues that must be addressed before sharing and using such data. First, entities may be subject to a wide array of legal

obligations depending on the data use, and the jurisdictions where the data is stored and processed. Second, entities need to consider all contractual obligations as well as its impact of upstream and downstream agreements on the data collection, use and disclosure. Third, different sectors have completely different needs to share or acquire data with or from other businesses. Even businesses within the same sector might have completely different data strategies. Due to these considerations, voluntary agreements between companies constitute today the main tool for business-to-business data sharing, and several consultations at the EU level in the past few years seem to confirm that there is no demand to create legal obligations in this area. Therefore, maintaining the current flexibility of voluntary agreements is the appropriate way forward.

Access request from third countries

When it comes to data access requests from third countries for law enforcement purposes, we encourage a balanced approach that respects and upholds agreements with third countries. ITI supports rule-of-law based law enforcement requests for information such as the Mutual Legal Assistance Treaty (MLAT) process, requests to companies through appropriate channels, or bilateral arrangements established via the CLOUD Act. **The obligations regarding third-country access requests contained in article 30 should be clarified**, in order to make sure there is legal certainty for companies to comply with European law when facing data access requests.

Given that **non-personal data is less likely to be subject to access requests** for law enforcement purposes, it would be useful to better understand which specific situations the Commission envisions when talking about such access requests. For instance, providing lists of examples of past – or future – cases in which requests of such kind have been issued could be helpful for data re-users.

We encourage policymakers to clarify the meaning of “all reasonable technical, legal and organisational measures to prevent transfers” in article 30(1) which data re-users would need to put in place in those cases where a third-country access request creates a conflict with Union or Member State law.

Finally, additional **clarity is needed with regards to the exemptions provided by article 30**, especially in paragraph 3. The obligations that would fall on a company subject to the access request of a third country without an international agreement with the EU seem complex and may create a high degree of legal uncertainty. ITI believes that the burden on companies to establish the legitimacy of the request and liaise with the competent EU authorities should be proportionate, in order to avoid disincentives to data re-use and sharing.

Data Innovation Board

ITI welcomes the creation of the European Data Innovation Board and its advisory role to identify cross-sector data standardisation needs. Those standards are essential in facilitating cross-industry data sharing, also within the Common European Data Spaces. We applaud the opportunity to include stakeholders in the Board’s work to make sure the fundamental input of the industry and other stakeholders is taken into account. We encourage the Commission to make sure the participation in the Board’s work is open equally to all stakeholders. ITI is committed to serve as a resource for the Board and welcomes the possibility of contributing to its work.

The European Commission's Impact Assessment to the DGA highlights that technical difficulties are an important barrier to data sharing in Europe. As such, we stress that technical solutions and standardisation should be the basis to achieve better data interoperability and portability. The European Data Innovation Board's approach to standardisation should be coordinated together with industry and recognise the specificities of sectors and use cases. This is particularly important in the context of the EU Data Strategy and to develop sector specific data spaces, and to make them cross-interoperable. To that end, we suggest that the Data Governance Act encourages cooperation with other European and international bodies to guarantee a harmonised approach on the development of data spaces.
