Feedback of the Software & Information Industry Association in Response to the Consultation on Commission Adoption of the Data Act & amended rules on the protection of databases

Submitted to the European Commission

May 13, 2022

The Software & Information Industry Association (SIIA) (Transparency Register #632689945691-83) appreciates the opportunity to provide feedback in response to the Consultation on the Commission Adoption of the Data Act. SIIA strongly supports the overall objectives of the Data Act to foster innovation within the EU in the digital economy and to unlock the value of data, while ensuring responsible and accountable practices for the use, collection, and sharing of data.

SIIA is the principal trade association for the software and digital information industries worldwide. Our members include over 450 companies reflecting the breadth of the data-driven economy. They include B2B and specialty publishers, academic publishers, providers and users of financial information, education technology companies, creators of consumer and enterprise software, and many others. Although SIIA is based in the United States, our membership includes hundreds of companies that do business within the EU, including many companies that are headquartered in EU member states.

SIIA provides this feedback in the hope that it will achieve the Commission's and the Parliament's guiding objectives. We have concerns that despite laudable intentions, the regulation in its current form would impede business efforts to innovate and compete in a data-driven economy and impose barriers on the responsible use of data. Certain provisions of the regulation would increase compliance costs and impose barriers to commercial contracting that will hurt innovation and competition. In addition, limited protection for intellectual property and trade secrets will limit incentives to innovate. We also have concerns that the current text would cause businesses to create more rather than less data, contrary to the Commission's objective of data minimisation, which will increase the risk of cybersecurity vulnerabilities and exposure of personal data.

Recommendation 1: Clarify the Scope of the Regulation with Respect to Personal and Non-Personal Data

We concur with the EDPS and EDPB that the term "data" is used throughout the text to refer indistinctly, in most instances, to both personal and non-personal data.[1] Researchers have noted that what constitutes personal data is one of the "central causes of doubt" in the current data protection regime." There remains a lack of consensus across various supervisory authorities on the correct legal test or requirement that should be applied to categorize data as either personal or non-personal data, under the GDPR.[2] This ambiguity is likely to lead to confusion for businesses and consumers alike and generate significant implementation challenges.

We strongly recommend that the scope of the Data Act be expressly limited to non-personal data. In addition, the regulation should also provide as clear a boundary as possible between "personal data" and "non-personal data." Given the existing regulatory framework for personal data under the GDPR, conflicting obligations between the Data Act and the GDPR will both generate confusion and impede business compliance efforts and subvert the Act's objectives of fostering innovation and unlocking the value of business data. In addition, imposing obligations on businesses to share personal data, or datasets that included a combination of processed (including inferred) and raw data, will run directly counter to the Commission's goal of data minimisation and undermine efforts to protect privacy and security of personal information. To the extent this mixed data remains within the scope of the regulation, we recommend that careful attention be paid to which obligations should apply to each type of data, with due regard to the obligations set forth in the existing EU data governance regime.

We agree with, and encourage, further clarification with regard to Recital 15 and Article 3(2)(d), which implies that pre-existing contracts between data users and third parties are out of scope. We welcome additional guidelines on the permissions to third parties for obligations they fulfill that contribute to safe and responsible data use.

Recommendation 2: Sharpen Definitions to Minimize Privacy and Security Risks in the B2C Context

We provide two additional recommendations to focus on foundational definitions in order to minimize privacy and security risks and further the Commission's objectives of data minimisation and unlocking the value of data.

---

[1] EDPB and EDPS Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act) (4 May 2022), available at https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-22022-proposal-european_pl.

[2] *See* Lilian Edwards, 'Data Protection I: Enter the GDPR' in Lilian Edwards (ed), *Law, Policy and the Internet* (Hart 2018) 84; Michèle Finck, Frank Pallas, "They who must not be identified—distinguishing personal from non-personal data under the GDPR," *International Data Privacy Law* (Feb. 2020).

First, we recommend that the regulation exclude diagnostic and other non-structured data. Recital 17 states that "data" should include "data generated as a by-product of the user's action, such as diagnostic data, and [data generated] without any action by the user". Diagnostic and other non-structured data is not maintained in a manner that will be understandable by users. Sharing of this sort of information will create new exposure points for sophisticated bad actors. Moreover, requiring businesses to render data in an "accessible" format (see Article 3) and potentially retain data for a longer period of time will lead to the creation of substantially more data at a significantly higher cost. This will have a profound effect on the ability of smaller companies to pursue data-driven innovation. It will also run counter to the Commission's goal of data minimisation. We recommend the Commission solicit further expert opinion on this topic.

Second, we recommend that the regulation exclude virtual assistants. Article 7(2) specifies inclusion of "virtual assistants" in all references to "products or related services." We believe this inclusion will lead to serious privacy and security risks and will be virtually impossible to implement – much like the concerns above regarding non-structured data. Though the Commission addresses this topic in Recital 22, the impact assessment lacks a clear justification for including virtual assistants. We recommend the Commission solicit further expert opinion on this topic as well.

Recommendation 3: Strengthen Commercial and Innovation Incentives by Protecting Contractual Freedom

SIIA's members have vast experience in B2B markets. Our members include companies in Europe and around the world across the information industry. They include B2B and specialty publishers, providers of enterprise software, providers and users of financial information, providers of data analytics services, privacy-enhancing technology, and open-source cybersecurity software, providers of legal information, and more. These firms gather and provide data to other businesses pursuant to contracts. They negotiate contracts to achieve defined objectives with safeguards to ensure appropriate use of data, protection of intellectual property and trade secrets, and remedies to govern contractual breach.

We believe the draft regulation creates uncertainty about the ability of businesses to contract freely with one another. Specifically, Article 3(2), Article 4, and Article 5 appear to impose requirements well beyond those that businesses may elect to negotiate for. We recommend that the regulation state clearly that the principle of contractual freedom should govern B2B data sharing in most situations.

In addition, while we appreciate the attention given to the micro, small, and medium-sized enterprises (MSMEs) in Article 13, we recommend reworking this section to provide MSMEs with greater ability to make use of private contracts without requiring terms that may be too onerous for potential counterparties. The provisions of Article 13 can serve as model contractual terms to guide MSMEs in their negotiation of contracts. We would recommend that further detail be provided regarding these principles. Businesses require clear rules to understand what is and is not permissible. We fear the uncertainty around these will make it harder for MSMSs to enter into productive business relationships with non-MSMEs in a data-driven economy.

Recommendation 4: Strengthen Protections for Intellectual Property and Trade Secrets

Much more thought needs to be given to the Data Act's interaction with existing and intellectual property rights as the term "data" expressly covers nearly every possible manifestation of protected material. We appreciate the thought given between the interaction of the Data Act and the Database Directive in Article 35. With that said, grave concerns about the draft's treatment of intellectual property remain. In many instances, trade secret protection of source code and data supplements copyright protection, and the software industry has relied on that protection to provide the incentives to innovate. And in other instances, the subjective criteria used to create databases could be of enormous competitive and commercial value.

The compelled disclosure of this kind of information creates serious policy and legal risks. From a policy perspective, that compulsion not only will disincentivize EU firms from innovating, it will discourage cross-border sharing of this kind of information for fear of disclosure. Computer programs are "data," and are protected by copyright law as are databases that are original in their selection, coordination and arrangement, and copyright law places limits on the purposes for which both kinds of works may be used. In addition, to the extent that it compels copying of both databases and computer programs for competitive purposes (as opposed to interoperability), the Data Act may violate other international obligations involving copyright.

We do not believe that this is the intent behind the Data Act. To avoid unintended consequences, we recommend excluding protected intellectual property by, for example, amending Article 4 (on B2C and B2B data sharing) and Articles 23-24 (on switching between data processing services) to exclude computer programs or data containing trade secrets from any data sharing obligations: in many cases, for example when data is collected based on subjectively selected criteria, . Similarly, more thought should be given to protection of the original aspects of database creation and maintenance and whether Article 35 should clarify that the Data Act does not expand or contract copyright protection in any selection, coordination or arrangement.

Recommendation 5: Provide Safeguards Around B2G Data Sharing

As reflected in Recital 10, there are many laws and regulations in the EU and member states that govern B2G data sharing, which also regularly occurs through voluntary acts by businesses. While we support the objectives of Articles 14-16 regarding B2G data sharing in situations of "exceptional need," we are concerned that these Articles lack sufficient safeguards to protect data from misuse, to minimize cybersecurity vulnerabilities, to protect individual privacy, and to protect unnecessary disclosure (and exposure) of intellectual property and trade secrets.

Article 15 states that businesses have an obligation to make data available where there is an "exceptional need," defined as one in which the data necessary to respond, prevent, or assist the recovery from a "public emergency" and in certain other situations to enable the government body to

fulfill "a specific task in the public interest." Article 2(10) defines "public emergency" as "an exceptional situation negatively affecting the population of the Union, a Member State or part of it, with a risk of serious and lasting repercussions on living conditions or economic stability, or the substantial degradation of economic assets in the Union or the relevant Member State(s)." The requirements are limited by Article 16(2), which does not extend the obligations under the regulation to matters involving criminal or administrative offenses, tax administration, and other situations. Nevertheless, the definitions remain exceedingly broad. They provide significant leeway for discretion by individual public sector officials. More concerning, they open the door to vastly different interpretations by member states.

The nature of B2G data sharing as contemplated by the regulation is not dissimilar from the issue presented in the *Schrems* cases with respect to certain national security powers of the U.S. government. In the most recent of those cases, the Court of Justice of the European Union (CJEU) determined that the United States did not provide "effective administrative and judicial redress for the data subjects whose personal data are being transferred" under Article 45 of the GDPR, when "read in the light of Articles 7, 8, and 47 of the [EU Charter of Fundamental Rights]."[3] Although the judgments of the CJEU dealt with GDPR and the sharing of data outside of the EU, the fundamental rights of privacy and redress, set forth in Articles 7, 8, and 47 of the EU Charter, apply with equal force to actions by public sector bodies within the EU. We do not believe that Article 15, in its current form, provides sufficient protection of those fundamental rights.

To achieve this, we recommend that the regulation include additional safeguards to protect personal and proprietary information, address how the proposed obligations and requirements fit within the existing landscape of B2G data sharing laws and regulations, and provide rules to ensure alignment across the member states.

Recommendation 6: Eliminate the Restriction on International Transfers of Non-Personal Data

We have serious concerns about the restrictions on international transfers of non-personal data in Article 27. These restrictions go beyond those of the GDPR without any meaningful connection between the non-personal data in question and the fundamental rights afforded to EU citizens.

The presumption against transferring data outside of the EU will have drastic effects on the EU economy. A study[4] by DigitalEurope estimates that two-thirds of European SMEs transfer data over international borders. Restricting flows of non-personal data will hurt their competitiveness and potential for growth. It is also likely to affect the scope of services that non-EU companies are able to provide to consumers and businesses within the EU which will have compounding effects. Another

[3] Court of Justice of the European Union, Judgment in Case C-111/18, paras. 188-199 (16 July 2020).
[4] DigitalEurope, "Schrems II Impact Survey Report" (Nov. 2020), available at https://www.digitaleurope.org/resources/schrems-ii-impact-survey-report/.

study[5] by DigitalEurope estimates that the EU could generate €2 trillion and two million jobs by the end of the decade by allowing international data transfers. Both studies focused on restrictions of personal data. We suspect the impact of Article 27 would compound the negative effects.

Recommendation 7: Incorporate International and Expert-Driven Standards for Interoperability

We support the call for interoperable data processing systems contained in Article 29. To foster interoperability with services used beyond the EU, which would aid EU-based businesses seeking to expand globally and also assist non-EU companies in providing services within the EU, we recommend that Article 29 incentivize adoption of industry-developed and/or international technical standards for interoperability.

[5] DigitalEurope, "Data Flows and the Digital Decade" (June 2021), available at https://www.digitaleurope.org/resources/data-flows-and-the-digital-decade/#overview.