France Digitale, the largest startup association in Europe, calls for a Data Act that matches its ambitions

Paris, August 2022

On February 23, 2022 the European Commission presented its proposal for a **Data Act**, which, as part of the **European Data Strategy**, complements the Data Governance Act.

France Digitale welcomes a text that establishes horizontal rules for data sharing among companies, users and governments, including for the switching between cloud service providers. **However, we draw the regulators' attention to the lack of clarity of certain provisions as well as their overlap with other pieces of European legislation**, which may make the implementation of the Data Act difficult.

For a Data Act that matches its ambitions, **France Digitale recommends to**:

A. Narrow down the scope of the proposal: the Data Act should only apply to **raw data** generated by a **clearly defined category of "products"**; the relation between products and **"terminal equipment"** under the e-Privacy Directive should be better specified.

B. Ensure consistency with the GDPR: the Data Act should allow for **profiling** and for the **sharing of data by third parties with other third parties** if: (1) one of the **legal bases** of the GDPR applies (2) **privacy-enhancing technologies** like pseudonymization are used.

C. Reinforce protection against unfair contractual clauses: the Data Act should protect **all types of companies**, and not just SMEs, from unfair contractual obligations; **model contractual terms** should follow Fair, Reasonable Non-Discriminatory (**FRAND**) principles.

D. Adjust B2G data sharing obligations: startups should only be obliged to share data, and especially trade secrets, with the public sector in a **restricted set of "exceptional circumstances"**, for **very specific purposes** and only with **clearly detailed safeguards**. Public sector bodies should **ask for startups' consent** before sharing data with third parties like statistical offices.

E. Set short and clear deadlines for provisions related to cloud providers: the timeframe to **remove switching charges** should be reduced from 36 to **18 months**, while the establishment of a **monitoring body** should take no longer than **6 months**.

F. Allow for the free-flow of non-personal data across borders except when concrete risks to fundamental rights, national security, or the trade secrets are identified. Moreover, **competent authorities** should provide a **"reasonable interpretation"** of data access requests by third-country governments.

G. Encourage experimentation and collaboration: the EU should engage with **open source** communities to develop **open interoperability standards** and **introduce sandboxes** for the operators of **Common European Data Spaces**.

H. Ensure compensation for data sharing with third parties: The ***sui generis* right** protecting derived datasets **should not be suspended.**

***Contact**: Agata Hidalgo, European Affairs Manager - agata@francedigitale.org*

SCOPE AND DEFINITIONS (Chapter I)

1. Limit the scope to raw data: recital 14 states that "*information derived or inferred from this data, where lawfully held, should not be considered within scope of this Regulation*". This is crucial as data treatment requires a significant investment by companies and may give rise to intellectual property rights. This formulation, however, seems to overlook other data processing practices that increase the value of datasets, including enhancement, enrichment, aggregation and others which may be developed in the future. **To ensure legal certainty, it should thus be specified that the Data Act only applies to raw data or, at most, to raw data and its relevant metadata.**

2. Formulate a clear and future-proof definition of product: according to recital 14 "*physical products [...] (often referred to as the Internet of Things)*" are covered by the Data Act. Art. 3(2) defines a product as a "*tangible, movable item, including where incorporated in an immovable item, that obtains, generates or collects, data concerning its use or environment, and that is able to communicate data via a publicly available electronic communications service and whose primary function is not the storing and processing of data*". Recital 15 explains that "*certain products that are primarily designed to display or play content, or to record and transmit content [...] for example, personal computers, servers, tablets and smartphones*" (which are "terminal equipment" for the purposes of the e-Privacy Directive) are instead not in the scope of the Regulation.
While France Digitale supports the choice of the Commission to adopt a broad definition of "product" rather than a list of items, which would require constant updating, **the current formulation gives rise to several problems.**

- First, **recital 32 seems to challenge the distinction above** by specifying that "*Internet of Things equipment is considered terminal equipment if it is directly or indirectly connected to a public communications network",* blurring the line between terminal equipment that it is in the scope of the regulation and terminal equipment that is not, while also extending user consent obligations of the e-Privacy Directive to IoT products.
- Second, **certain terminal equipment that is clearly outside of the scope of the Regulation may generate IoT-relevant data** when used to operate an IoT product, as in the case of a smartphone used to remotely activate a smart home device.
- Third, **certain products seem to equally perform functions that are within and outside of the scope of the regulation**. Smart watches, for example, are not primarily meant to store or process data, yet they display content from the smartphone to which they are connected and may send messages and make calls.

The definition of product is therefore unsatisfactory in light of current uses of connected items. **A more future-proof definition of "product" would therefore take into account that of "terminal equipment" and set more clear-cut criteria to establish which devices are within and which are outside the scope of the Data Act.**

3. Align definitions with those in the Digital Governance Act (DGA): as the Data Act is complementary to the DGA, **the definitions of "data holder " and "public sector body" in art. 2 should be identical in the two texts**. Moreover, a definition of "metadata" is absent from the Data Act despite being mentioned at several points in the text (e.g. art. 24 and 29) **the definition of "metadata" provided in the DGA should therefore be reused.**

B2C and B2B DATA SHARING (Chapter II)

4. Ensure consistency with the GDPR: art. 6(2)(b) prohibits third parties to "*use the data it receives for the profiling of natural persons within the meaning of Article 4(4) of Regulation (EU) 2016/679, unless it is necessary to provide the service requested by the user*". This, however, **overlooks the fact that the GDPR allows for profiling on legal bases other than "necessity", including "legitimate interest" and "consent"**. If the current formulation is maintained, users will see their right to data portability restricted and startups will no longer be able to process data to improve their services, train algorithmic models, build a customer-brand relation and provide personalized offers.
Similarly, art. (6)(2)(c) prevents data sharing by establishing that third parties shall not "*make the data available it receives to another third party, in raw, aggregated or derived form, unless this is necessary to provide the service requested by the user*". This again **fails to account for the other legal bases in the GDPR as well as for techniques, like pseudonymisation or anonymisation, which allow for the safe sharing of data** across multiple parties in compliance with the GDPR. As it stands, the Data Act would limit the ability of startups to compete with large players that have direct access to first-party data.
To be aligned with the GDPR, the Data Act should therefore allow for profiling and the sharing of data by third parties with other third parties under two conditions: (1) the application of one of the **legal bases enshrined in the GDPR** (2) the application of **privacy-enhancing technologies** like pseudonymization and encryption.

UNFAIR TERMS FOR B2B DATA ACCESS AND USE (Chapter IV)

5. Reinforce protection against unfair contractual clauses: article 13(1) establishes that "*A contractual term [...] unilaterally imposed by an enterprise on a micro, small or medium-sized enterprise as defined in Article 2 of the Annex to Recommendation 2003/361/EC shall not be binding on the latter enterprise if it is unfair*". France Digitale considers that, in this context, the maturity of a company in data sharing is as important as its size. To ensure a level-playing field, therefore, **the prohibition to impose unfair contractual clauses should be extended to all types of companies, not just SMEs**.
At the same time, we notice that the notions of "unfair contractual clauses" and "good commercial practice" would benefit from some further clarification. This could be achieved by establishing that **contractual clauses shall be Fair, Reasonable and Non-Discriminatory (FRAND)**. Indeed, FRAND is an established contractual mechanism developed in the context of telecommunications standards and it can already be found in art. 8(1) of the Data Act as well as in art. 6(1) of the Digital Markets Act (DMA). To ensure their consistent application in data sharing agreements, **the European Commission should draft guidelines on the interpretation of FRAND in the context of the Data Act**. This could complement the model contractual terms envisioned in art. 34 (see point 18)

B2G DATA SHARING FOR EXCEPTIONAL NEED (Chapter V)

6. Narrow down the notion of "exceptional need": art. 14 creates an obligation for companies to share data with public sector bodies in case of "exceptional need", which is understood as a "public emergency" (art. 15). Such a vague definition, however, lacks any consideration of proportionality and could lead to different interpretations in different contexts, thus hampering legal certainty. To ensure a consistent and proportional application of this obligation, **the term "exceptional need" should be narrowed down**,

for example by adopting the well-established criterion of "force majeure" or by providing a list of situations that may account as public emergency (e.g. natural disasters, public health crises, man-made disasters, etc.).

7. Strengthen safeguards for the sharing of trade secrets: art. 19(2) states that "*Disclosure of trade secrets or alleged trade secrets to a public sector body or to a Union institution, agency or body shall only be required to the extent that it is strictly necessary to achieve the purpose of the request*". **As trade secrets are the core of a company's competitiveness, the Data Act should clarify which purposes would justify the sharing of trade secrets**. This is particularly relevant when the public sector body at hand is a statistical agency, a research organization or another semi-public organization which may be more or less directly in competition with the company.
Moreover, the same article establishes that, in the case of sharing of trade secrets, "*the public sector body or the Union institution, agency or body shall take appropriate measures to preserve the confidentiality of those trade secrets*", but it fails to indicate what such measures would be. To guarantee a proportionate access to trade secrets by public sector bodies and their adequate protection, **public sector bodies should, *a minima*, (1) declare the purpose for which trade secrets would be used (2) explain in what way the trade secrets would contribute to the achievement of such purpose (3) detail the measures that would be taken to protect them.**

8. Ask for companies' consent before sharing data with statistical offices and research organizations: art. 21(1) gives Public Sector Bodies the right to share data obtained from businesses with research organizations to carry out "*scientific research or analytics compatible with the purpose for which the data was requested*" or with national statistical institutes and Eurostat "*for the compilation of official statistics*". **This provision is problematic in at least three ways.** First, it establishes a right to share data with a third party **without asking for the data holder's consent**. Second, it does so **without specifying whether trade secrets and IP-protected data are included** and if so, if the third party (the research or statistical organization) has any particular obligation to protect them. Third, the Public Sector body's right to share data with third parties is for **purposes *other* than the one for which the data was originally requested**. In particular, for research organizations, it is enough for the purpose to be "compatible" with the original one, while for statistical offices, it can simply be "the compilation of official statistics", which is clearly not an "exceptional need". In light of these considerations, **the Data Act should establish an obligation for Public Sector Bodies to ask for businesses' consent before sharing their data with research and statistical organizations**, even when the data was obtained under an "exceptional need" procedure.

SWITCHING DATA PROCESSING SERVICES (Chapter VI)

9. Introduce a reversibility requirement: art. 23(1) mandates data processing services to remove all "commercial, contractual, technical and organizational obstacles" hampering, among others, the portability of data and the functional equivalence between service providers. **This article could be strengthened by adding the removal of all obstacles to the *reversibility* of data, that is, the ability to retrieve a user's data to enable its porting to another service provider**. The reversibility requirement could then also be added to the contractual terms for switching providers listed in art. 24(1)

10. Shorten the deadline for the complete withdrawal of switching charges: art. 25 gives cloud providers and other data processing services a maximum of 3 years since the entry into force of the Data Act to remove charges on customers who wish to port their data to another service. This timeframe, however, is **too long compared to the average life of a startup (3 years) and the pace of evolution of digital markets**. **A more appropriate span would be, for instance, 18 months**.

11. Establish a short and clear deadline for the introduction of a monitoring mechanism: art. 25(4) empowers the European Commission to create a monitoring mechanism to follow the evolution of switching charges and ensure their complete removal by the deadline established in the Data Act. As it currently stands, however, **the provision does not specify *when* such a mechanism would be operational,** which could seriously reduce its relevance. Given its importance for the effective implementation of the Data Act and in line with the point above, **the monitoring mechanism should become operational no later than 6 months after the entry into force of the Data Act**.

INTERNATIONAL DATA TRANSFERS (Chapter VII)

12. Support the free-flow of non-personal data except when concrete risks are identified: art. 27(1) mandates all companies operating in the EU to take "technical, legal and organizational measures" to prevent the international transfer or governmental access of non-personal data if this would conflict with national or Union law. As this obligation is very broad, it could lead to overcompliance, that is, to the interruption of most international data transfers. This, in turn, **would have extremely detrimental effects on European startups and scaleups, which remain heavily dependent on global data processing services**. To avoid such side effects, the Data Act should instead **allow for the international transfer of non-personal data except when this poses a concrete risk to the fundamental rights of individuals, the security or defense of Member States or the trade secrets of companies**, as listed in recitals 77 and 78.

13. Clarify the chain of responsibility between data processing services and competent authorities in answering third country data access requests: art. 27(4) states that, if a data access request is legitimate according to the criteria set out in the Data Act, the data service provider shall give access to a "*minimum amount of data permissible in response to a request, based on a reasonable interpretation thereof*". **However, it is not clear if "minimum amount of data" and "reasonable interpretation" of the request should be made by the data service provider or by the competent authority**. France Digitale considers that the latter would be better suited for the task.

INTEROPERABILITY (Chapter VIII)

14. Introduce sandboxes for Common European Data Spaces: art. 28 lists the essential requirements that the operators of data spaces should comply with to ensure interoperability of data sharing mechanisms and services. As data spaces are brand-new structures, however, operators of data spaces should be given the opportunity to experiment with different solutions. In the same vein of the AI Act, therefore, **the Data Act should lay down the legal framework for sandboxes for European Data Spaces.** Such sandboxes could operate, for example, with the data provided by **data altruism organizations** recognized under the DGA. Moreover, such sandboxes could benefit from

the support of **Testing and Experimentation Facilities (TEFs)** as it is already the case for AI sandboxes under the AI Act.

15. Clarify the role of open source in the definition of open interoperability standards: art. 29 lists the criteria that open interoperability specification and standards for data processing services should have to enable the portability of data between providers. While this is a welcome development, **the role of open source in the definition of these specifications and standards remains unclear**. Open source norms effectively reduce obstacles to the transfer of data and make portability more fluid, while also increasing trust among contributors. **By including open source norms in its interoperability specifications, the EU could embrace a standardization process that is modern, collaborative and better adapted to dynamic innovation cycles**.

IMPLEMENTATION AND ENFORCEMENT (Chapter IX)

16. On model contractual terms: art. 34 mandates the European Commission to draft model contractual terms to help businesses negotiate data access agreements. **Such model contractual terms will prove very useful to startups and scaleups but should be strenghtened with the inclusion of Fair, Reasonable and Non-Discriminatory (FRAND) conditions** (see Ch. IV). Moreover, **startups should be consulted** during the drafting process to ensure their needs are taken into account.

SUI GENERIS RIGHT UNDER DIRECTIVE 1996/9/EC (Chapter X)

17. Protect companies' right to compensation: art. 7 the Database Directive 1996/9/EC allows data holders to prevent the "extraction and/or reutilisation" of the content of databases that required "significant investment" to be "obtained, verified or presented" (*sui generis* right). This incentivizes startups like smart watch manufacturers to process IoT-generated data to produce new datasets, which can then be sold to third parties, constituting an additional revenue stream and contributing to the data economy. **Art. 35 of the Data Act, however, suspends the *sui generis* right and thus the possibility to ask for compensation from third parties** when sharing "*databases containing data obtained from or generated by the use of a product or related service*". With this formulation, the presence of one data point generated by an IoT product or service in a dataset would be enough to prevent the monetization of the whole dataset. **This would force startups to find other ways to protect their derived datasets**, such as Intellectual Property on the source code, trade secrets on algorithms, trademarks or copyrights, **leading to increased costs, slower data sharing and less innovation**. Since the scope of the Data Act should be limited to raw data (see point 1), and art. 35 refers to derived datasets**, this provision should be deleted from the proposal**.