Brussels, 12 May 2022

Orgalim position on the Data Act proposal

Executive summary

Orgalim represents Europe's technology industries, world leaders in connected products and production systems, which are becoming increasingly "intelligent" via data-based services. The transition to a data-driven economy is of paramount importance for the future growth and competitiveness of our industries.

We **support the objective of fostering Europe's data economy** but question a number of the policy instruments proposed in the Data Act to achieve its intended objective. The extensive new design, transparency and data access obligations imposed on data holders (including manufacturers) will have substantial costs for them, especially for small and medium-sized enterprises.

We highlight the following points in particular:

- We call for a **careful and balanced approach to data sharing**. Interventions such as mandatory data sharing should be targeted to clearly-demonstrated market failures. We believe that **freedom of contract** is the best tool to cater for the specificities of all types of market scenario.
- **Business-to-business (B2B) and business-to-consumer (B2C)** relations have different characteristics and a one-size-fits-all approach could be detrimental to the data economy.
- **Business-to-government (B2G)** mandatory data sharing is disproportionate and needs changes to ensure a workable and predictable environment for European companies, especially given the very broad scope of what are referred to as "exceptional needs" which can trigger public bodies' requests for access to business data.
- The proposed **safeguards** are either unenforceable or insufficient across all scenarios (B2B, B2C, B2G).
- **Smooth international data flows** are essential for the data economy to grow, for European companies to provide services in third countries, and for Europe to attract investments. We are very concerned that provisions on the transfer of, and access to, data in international contexts will pose new and unnecessary barriers and create uncertainty in the market.
- Orgalim welcomes proposals to make **switching** between data processing services easier and to increase **interoperability** in the data market, but some provisions should be clarified. We believe that standards should be developed by the industry.
- We are very **concerned about imposition of technical changes to existing connected devices already in use** to enable data access. Technical changes need contractual adaptations, which are likely to be costly as well as generating an extra administrative burden.

1. Introduction

On 23 February 2022, the European Commission published a proposal for a Regulation on harmonised rules on fair access to, and use of, data (hereafter the "Data Act")[1]. With this proposal, the intention of the Commission is to foster the European data economy by regulating access to, and use of, their data by certain stakeholders. The Data Act is part of a wider range of initiatives in the context of the Commission's European Strategy for Data[2] aimed at unlocking the potential of the data-driven economy and the digital transformation of Europe's industries.

Orgalim welcomed, and shares in principle, the objectives of the European Strategy for Data[3]. Europe's technology industries see the transition to a data-driven economy as not only inevitable, but also essential for their future growth and competitiveness. Our companies are world leaders in connected products and production systems, which are becoming increasingly "intelligent" via data-based services. The exchange of industrial data has become a vital part of commercial practice for our industries. Data flows make it possible to increase manufacturing productivity, tap into new efficiency gains and contribute to sustainability goals, whilst simultaneously enabling new data-driven services and business models.

However, we question the choice and feasibility of a number of the policy instruments proposed in the Data Act to achieve its intended objective. Please find below our concerns on the chapters of the proposed Regulation, structured as follows: scope and definitions (Articles 1-2), B2B and B2C data sharing (Articles 3-12), Unfairness test (Article 13), Making available data B2G (Articles 14-22), international flow of non-personal data (Article 27), portability and interoperability (Articles 23-26 and 28-30) and other provisions (Articles 31-42).

2. Scope and definitions (Articles 1-2)

2.1. Scope

Business-to-business (B2B) and business-to-consumer (B2C) relations have different contexts, characteristics and needs. The horizontal rules proposed in the Data Act follow a one-size-fits-all approach that does not reflect this reality. Industrial data economy transactions in a B2B context are very sensitive from an economic and trade secrets point of view, and therefore a specific approach should be sought to limit economic loss and legal uncertainty and to protect businesses' ability to provide value to their customers.

Moreover, there are concerns that businesses will have to follow additional sectoral data sharing obligations in addition to the horizontal obligations stemming from the Data Act. It is essential to maintain a balanced framework and **avoid a situation where cumulative rules overburden Europe's data economy** instead of fostering it.

The co-legislators should consider focusing the Data Act only on those sectors where clear market failures have been observed, on the basis of careful impact assessments. They should specifically consider having a differentiated approach on B2B (where freedom of contract should be the guiding principle) and B2C.

2.2. Definition of data

In **Article 2(1)**, the proposed definition of "data" is too general. Connected products can generate a wide range of data, differing in nature, volume, processing levels and costs to make it accessible. It cannot be generally assumed that the sharing of all data is equally feasible from a technical, legal and commercial perspective. Crucially, the more data has

[1] Data Act: Proposal for a Regulation on harmonised rules on fair access to and use of data | Shaping Europe's digital future (europa.eu)
[2] Strategy for Data | Shaping Europe's digital future (europa.eu)
[3] Orgalim contribution to the Commission consultations on data and AI | Orgalim

been processed, the higher the possibility that it can expose trade secrets and intellectual property (IP). The definition should clearly state that **this regulation applies only to raw, unprocessed data**, taking into account the state-of-the-art, the nature, scope, complexity and cost of the access process; and notwithstanding the necessary safeguards that should also apply to the sharing of raw data. This is essential for companies both to be able to safeguard their competitive assets and to ensure compliance with competition law.

For other data, we believe that freedom of contract should allow businesses to tailor the definition of "data" to their reciprocal specific needs. As a concrete example of how freedom of contract is a better basis for this, please refer the "Orgalim legal guide to industrial data"[4].

2.3. Data holders and users

In **Article 2(6)**, the proposed concept of "data holder" is not easily or clearly applicable in industrial contexts and it does not take into account that **users can also act as data holders**. Component or even full-product manufacturers may not hold by default the data generated through the products they sell. In such cases the user or service providers may act as the data holder. The proposed Data Act does not take these situations into consideration, which results in an imbalanced approach towards users.

To foster an optimised data allocation in Europe, the Data Act should support data flows along the entire value chain, also including manufacturers and component providers. Data flows across the industrial value chain are arranged across manufacturers of components, manufacturers of final products, software providers and customers; and the rights along the flow of data are set through contracts. Imposing a simplified data holder-user dichotomy would change these processes and **create unnecessary confusion** and potential extra burdens (e.g. new contractual arrangements for compensation or for ensuring compliance with the Data Act) in contexts that are already working well. This burden must not be underestimated, because it impacts many entities and partners in a data sharing network, with repercussions across the whole data value chain.

The terms "data holder" and "users" urgently need to be clarified in line with industrial practice. Implications for "data processors" and the definition of "operators of data spaces" should also be clarified.

2.4. Related services

In **Article 2(3)**, the definition of "related services" is **too general**. It potentially includes all data processing services, Internet of Things (IoT) and Artificial Intelligence (AI) software, raising doubts as to whether redundancy and interactions with **Articles 23-26** and other legislation have been fully taken into account.

3. B2B and B2C data sharing (Articles 3-12)

3.1 Obligation to share data with users

Orgalim believes that mandatory data sharing is not a good way to regulate the market, especially when there is no clearly demonstrated market failure which makes it necessary and when **freedom of contract** and entrepreneurial freedom is a sufficient basis for the flow of industrial data to work properly. In preparation for this proposal, the Commission has referred to the case of SMEs not being able to access the data they produce through the connected products they own or rent because of their weaker bargaining position. This approach gives the false perception that the business user is always smaller than the company manufacturing the connected product. However, many manufacturers

[4] Orgalim legal guide to industrial data, p. 9.

are SMEs themselves and smaller companies often supply connected products, for example machinery, to business clients of a comparable or even larger size. The B2B-B2C data sharing provisions of the Data Act were designed to address only a subset of cases in the market, but the proposal would now apply them to all cases, going as far as encompassing both B2B and B2C. We believe that freedom of contract remains the best principle for contractual arrangements to be tailored to the specificities of every market scenario. If there are any imbalances or gaps, they should be addressed by EU competition law, or well-targeted sector-specific legislation.

Obligations "that data generated by their use are, by default, easily, securely and [...] directly accessible to the user" (Article 3) create regulatory conflicts with data security requirements, e.g. from Articles 25 and 32 of the General Data Protection Regulation (GDPR), and contradict the Commission's efforts to strengthen data and cybersecurity via product rules (e.g. the Radio Equipment Directive - RED) and EU standardisation.

The proposed text does acknowledge the need for the scope of the new data sharing obligations to be limited, and we do support an exception to the obligation to share data for micro and small enterprises. However, in light of the very substantial new administrative burden placed on companies, Orgalim asks to **extend this exception to medium-sized enterprises**. The quantity of connected products produced by medium-sized enterprises is sometimes too small to produce economies of scale and compensate for the burden of the new design and data access obligations. This is the case especially in industrial settings when companies offer products that are tailor-made for their clients, which are often unique pieces and where therefore the loss would be even higher.

If policy makers ultimately decide to introduce a user right of access to data, the depth of the legislative intervention should be reviewed, as the provisions in **Articles 3 and 4 seem excessive and too detailed**. Once the right of access is established, it should be up to the parties to find contractual arrangements to apply that right, based on (the residual) contractual freedom. The proposal leaves open the question of which party is subject to the pre-contractual information requirements regarding the collection and use of data. This responsibility could fall upon the product manufacturer, the provider of the related service, or the point of sale. It is equally unclear how this information would be effectively communicated to the user ahead of a purchase – for example, updated software terms cannot be reflected on product packaging or accompanying materials.

Orgalim calls for clarification on the scope of the limitation for data holders to reuse data. **Article 4(6)** states that "*The data holder shall only use any non-personal data generated by the use of a product or related service on the basis of a contractual agreement with the user.*" The risk that this might completely block any reuse of data by manufacturers and data holders in general is high and looks likely to **deeply disrupt the flow of industrial data across the value chain**. It might also pose an obstacle to the manufacturer's ability to collect data from its own products for innovation purposes or to feed and further optimise AI systems. With these provisions, the proposed Data Act risks creating as many new obstacles to the data economy as it intends to remove.

3.2 Obligation to share data with third parties

Orgalim stresses that there are **significant commercial and confidentiality implications** in the imposition of data sharing also with third parties. The scope of this obligation seems too broad, and the safeguards provided are not sufficient. The dynamics of further sharing data with other parties beyond third parties should also be clarified. If there are any imbalances or gaps, they should be addressed by EU competition law or well targeted sector-specific legislation.

We are also concerned about the fact that this obligation applies to both B2B and B2C scenarios, as **in B2B companies can already share data with third parties** based on contracts[5]. The scope of the obligation to share data with third parties, including restrictions on eligible parties, should be considered carefully and be based on an impact assessment with a view to avoiding the restriction of businesses' freedom to choose their service providers.

If the obligation has to remain in place, policymakers should consider limiting it to B2C cases.

[5] See eg: Orgalim legal guide to industrial data, p. 10.

According to **Article 8(3),** the data holder should not discriminate between comparable categories of data recipients and it would be up to the data holder to demonstrate that there has been no discrimination. Although we understand the intention of the provision, the **burden of proof appears disproportionate** and there is no measure in place to avoid data recipients abusing their right to make unfounded allegations without any proof being required. Also, in practice it is unclear what kind of proof data holders are required to present. Article 8 should still allow companies to agree freely with trusted parties in addition to what is mandated under Article 5 – i.e. joint development where more strategic data is shared with chosen partners.

3.3 Safeguards, IPRs and trade secrets

Orgalim finds the **safeguards proposed throughout the Data Act insufficient**. Data sharing often entails exposure of trade secrets and IPRs, which are the fruit of investments and key enablers of companies' business models. IPRs, trade secrets and know-how should be safeguarded to protect innovation. Forcing companies to share data continuously and with multiple entities (users, third parties, public bodies…) and even with competitors without appropriate safeguards, might lead **businesses to reconsider the extent of their participation in the data economy**. As long as protection of data holders' IPR and trade secrets are not a condition for users to exercise the right to access data, users cannot be expected to take all necessary steps to protect data holders' data protection rights. In other words, there needs to be a **balance between access rights and data protection rights.** The way the Data Act is proposed, users have **no real incentive for the protection of manufacturers' rights**. Not only should such rights be protected effectively to safeguard the competitiveness of our companies, but also to comply with international conventions and trade agreements with global partners. How compliance is to be controlled, proven and enforced remains open since the data holder lacks sufficient remedies or control mechanisms. The proposal also currently leaves open the question of what happens if the data recipient and data holder cannot agree on reasonable protection measures.

The obligation on users and third parties set out in **Articles 4(4) and 6(2)** not to use accessed data to develop competing products is **neither sufficient nor enforceable in practice**. It is also unclear why such articles only focus on products and exclude the development of competing **services**. This would create significant distortion effects in the service market at a time when all companies are digitalising their businesses. Above all, it is unclear how in practice the data holder would even become aware of a misuse of its trade secrets. It even appears from **Article 11(3)** that there are situations where the data holder would have to accept data recipients' actions breaking protections applied to data, which is concerning. It must also be considered that in globally connected value chains, the data might be accessed by non-European competitors who are not subject to the enforcement of the above-mentioned obligation. A high number of costly legal disputes must be expected if safeguards are not clearer and broader.

Article 6(2) should include an exception clause, stating that a data holder is not obliged to share data with a third party if this party is deemed to be a potential competitor. It should be possible to recognise as potential competitors third parties which are planning or likely to enter the relevant market within the foreseeable future.

It should also be ensured that the provisions of the Data Act are consistent with other governance models and, in particular, leave sufficient room for data governance models developed in European data initiatives such as Gaia-X or the European data spaces. Especially for smaller actors in the data economy, spaces for data governance will be very important, in order to reduce transaction costs and increase legal certainty.

3.4 Compensation

It appears that the majority of newly imposed data sharing obligations do not even allow data holders to be compensated for data access. In the proposed Data Act, this is the case when users request direct access to data (**Article 3(1)**) or even in some B2G scenarios (**Article 20(1)**). It is unclear why, for the latter scenario, compensation is foreseen only for non-emergency cases, although the costs to the data holder may be the same or even higher and a reasonable compensation could be negotiated following the ending of the emergency.

New obligations without compensation will **limit the Research and Development (R&D) and innovation effort** that manufacturers invest in connected products and they **even risk driving some manufacturers out of the IoT market** because it would not be profitable anymore.

In the case of compensation from third parties qualifying as SMEs, **Article 9(4)** introduces a transparency requirement for data holders to disclose the basis of calculation of the price for receiving data. The level of **detail requested is disproportionate** and, again, leads to a high risk of exposure of trade secrets to competitors without any safeguard.

We ask for adequate **compensation to be possible across all data sharing scenarios and based on contracts**. Even in exceptional cases, such as micro or small enterprises and for public emergencies in B2G, at least cost-based compensation should be allowed.

4. Unfairness test (Article 13)

Orgalim strongly supports the principle of contractual freedom to arrange data economy transactions in industrial contexts. Last year we published the Orgalim legal guide to industrial data , with the aim of providing guidance to support the development of balanced practices in B2B data sharing contexts. An unfairness test imposed on contractual agreements is detrimental to both contractual and entrepreneurial freedom.

While we support the general objective of reducing the detrimental effect that unilaterally imposed contractual clauses can have on SMEs, the definitions and scope of application of the unfaimess test (**Article 13**) need to be revised, to prevent it causing a significant amount of legal uncertainty, including for SMEs. For example, it is unclear how the contractual counter party could know or verify the SME status and what would happen if the status changed.

5. B2G data sharing (Articles 14-22)

The Commission is proposing a broad scope for mandatory disclosure of business data. Orgalim calls for moderation in any requirement to open private industrial data, especially without sufficient safeguards for trade secrets and IPRs, and when no compensation can be sought for sharing such data. An exceptional business-to-government (B2G) data sharing regime might be acceptable **only if based on *truly* exceptional needs** and with appropriate safeguards in place.

The conditions triggering the proposed mandatory B2G regime are too broad, and the **definition of public emergency is legally unclear**. Specifically, imposing mandatory B2G data sharing merely on the grounds that such data is needed by public bodies to fulfil their tasks is **disproportionate** and does not fit the concept of "exceptional need". The explicit mention of the use of such data by statistical offices, whose sole and continuous purpose is the collection of data, underlines the concerns regarding the wide interpretation of "exceptional need" already included in the proposal.

Businesses should be able to seek **appropriate compensation** regardless of which type of "exceptional need" the public body's data access request is based on. Opting for data altruism should remain a private choice of businesses and a framework for this is already foreseen in the proposed Data Governance Act, with no need for further intervention.

Safeguards should be introduced to avoid abuse of **Article 15(c)(1)**. Since there is no market rate for industrial data, public bodies may end up making excessive use of data access requests regardless of the fairness of the price.

Technical and organisational safeguards should not apply only to personal data (**Article 19(1)b**), but also to industrial data, and especially trade secrets and IPRs. These B2G obligations also apply to derived and inferred data held by companies, which are very likely to expose valuable commercial information which would endanger the companies' market position if revealed.

6. International flow of non-personal data (Article 27)

Orgalim fundamentally questions the need for, and suitability of, **Article 27**, which foresees that providers of data processing services should take all reasonable technical, legal and organisational measures, including contractual arrangements, in order to prevent international transfer or governmental access to non-personal data held in the EU where such transfer or access would create a conflict with EU law or the national law of the relevant Member State. The data economy is by nature cross-border, and industrial data flows are no exception. European companies need certainty regarding their ability to exchange non-personal data internationally to operate their business with their affiliates, comply with their international contracts, freely choose their global partners, and also to exercise their business models in third countries. This is particularly important for Europe's technology industries, which are strongly export-oriented and depend on international trade for their success, representing over a third of the EU's manufactured exports.

While the protection of industrial data is a legitimate purpose, the approach of the Data Act to mirror the GDPR appears excessive and disproportionate. It would impose on business and technical data a level of protection that is usually required to protect fundamental rights. From a practical standpoint, EU companies are already struggling to assess the adequacy of non-EU laws with EU privacy laws. It would be even more **difficult and costly for them to perform transfer impact assessments** on a wide variety of non-EU laws and international agreements in the realm of confidentiality, trade secrets, patents, and intellectual property rights. It is not clear how the Commission foresees that data processors could enforce these provisions on a daily basis, and therefore how these provisions can be prevented from **inflicting unnecessary damage on the European data economy** – the very economy that the Data Act is intended to foster.

If the intention is to restrict access to European industrial data by **third countries' public bodies**, then the text should be changed to a more risk-based approach led by businesses themselves that will determine the mitigation measures to put in place, and then make business decisions based on the residual risks. The scope of this provision should be narrowed down, as it currently affects all transactions between businesses to and from the EU.

7. Portability and interoperability (Articles 23-26 and 28-30)

7.1. Switching between data processing services (Articles 23-26)

Orgalim welcomes the objective of making switching between data processing services easier. However, it should be clarified to what extent the new switching rights imply obligations on the manufacturers of the connected products when their "related services" are cloud-based. Provisions should reflect the variety of data processing services, the volume and complexity of data, the shared responsibilities between data processing services and customers, and the need for specialist technical assistance and project management. Furthermore, the obligation for data processing services to ensure "functional equivalence" in the new environment after switching should be clarified. Ensuring "functional equivalence" would not only raise security concerns as data processing services would need to open access to their IT systems, but also trigger automatic liability as the functionality and service levels would not be available in the new environment.

7.2. Interoperability (Articles 28-30)

Orgalim supports the objective of increasing interoperability to remove unnecessary barriers to the industrial data economy. The standardisation effort to achieve this should, however, remain open, inclusive and industry-driven and in line with the development of standards at international level. The Data Act should put safeguards in place recognising differences between services to avoid a full downward harmonisation of services that would hamper innovation. It is essential for EU industry competitiveness that industry representatives continue to be involved in the development of

standards as well as in dialogue with the Commission to share their knowledge. Existing industry initiatives fostering and providing interoperability should be taken into account.

8. Other provisions (Articles 31-42)

In light of the scope and depth of the new obligations imposed on data holders, and in particular on manufacturers, the transitional period before the start of application of this regulation should be longer than the proposed 12 months (**Article 42**). The new requirements for the design of connected product need a much longer compliance period, and many businesses will have to reconsider their entire data strategy under the new rules. This will require analysis, important decisions on their business models, and then adaptation of their manufacturing processes, which will take longer than 12 months. The fact that the scope of the new obligations also encompasses medium-sized enterprises is an additional reason to **grant at least 36 months before the regulation is applied**.

The proposal assigns the **enforcement** and applicable penalties of the Data Act to one or more authority per Member State. This increases the possibility for fragmented application of the regulation across countries. However, the European Single Market for data needs full predictability to deliver on its potential.

It would be **unjustified to request a technical change to existing connected devices already in use** to enable data access. Technical changes need contractual changes which are likely to be costly and to create an extra administrative burden.

9. Conclusions

Orgalim supports the objective of fostering Europe's data economy. In B2B scenarios, this would be best achieved through voluntary measures incentivising data sharing and based on **freedom of contract**, rather than mandatory opening of industrial data. If any market imbalance appears, it can be addressed by EU competition law and sector-specific legislation, in order to tailor the measure to the specific problem.

The Data Act appears to be too broad and to impose too many new obligations for it to actually help the data economy. Instead, we are concerned that it is likely to have the contrary effect of lowering investment in connected devices and cloud services developed by EU businesses while **driving many businesses out of the industrial data market and adversely affecting EU industry competitiveness in the global market**.

Orgalim invites the European Parliament and the Council of the EU to take these views into account during the legislative process of adoption of this Regulation.

Orgalim aisbl
BluePoint Brussels
Boulevard A Reyers 80
B1030 | Brussels | Belgium

+32 2 206 68 83
secretariat@orgalim.eu
www.orgalim.eu
VAT BE 0414 341 438