JOINT POSITION PAPER

on the proposal for a Data Act

03 11 2022

Joint position paper

on the Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)

Further to the position papers and declaration statements of their respective European associations[1], this document constitutes FEDIL's and the Luxembourg Chamber of Commerce's additional contribution to the proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data.

INTRODUCTION

On 23 February 2022, the European Commission (hereafter the "Commission") published its proposal for a Regulation on harmonised rules on fair access to and use of data (also referred to hereafter as the "**Data Act"**).

The proposed Data Act is part of the European digital and data strategy launched by the Commission in 2020 in order to build a "*Europe fit for the Digital Age*". The Data Act complements other Commission's initiatives in the digital field amongst which the Data Governance Act (DGA) and the Digital Market Act (DMA).

The Data Act is a horizontal proposal which provides "*basic rules for all sectors*"[2]. Thus, the Data Act "*leaves room for vertical legislation to set more detailed rules for the achievement of sector-specific regulatory objectives*".

The proposed EU Data Act aims to regulate data access and use in order to "*ensure fairness in the allocation of value from data among actors in the data economy*"[3], "*open opportunities for data-driven innovation and make data accessible for all*"[4].

[1] FEDIL is member of BusinessEurope; the Luxembourg Chamber of Commerce is member of Eurochambres.
[2] Data Act, recitals, page 5.
[3] Data Act, recitals, page 2.
[4] EC press release, Data Act: Commission proposes measures for fair and innovative data economy, 23/02/2022

JOINT POSITION PAPER

on the proposal for a Data Act

GENERAL COMMENTS

Although FEDIL - The Voice of Luxembourg's Industry and the Chamber of Commerce of Luxembourg, together with their members, welcome the Commission's efforts to harmonise the rules on fair access to and transfer of data within the European Union (EU), the means to accomplish the objectives remain unclear given the multiple layers of EU legislations as well as the forthcoming sectoral legislations. As a result, its implementation becomes technically more complex.
Furthermore, the Data Act imposes huge constraints on the various stakeholders in terms of process, cost, technique, organisation, administrative and legal formalities to comply with the Data Act within a very short term of 12 months following the date of entry into force. There are many of those provisions that are simply unrealistic and not that easy for businesses to implement. We express our concerns that this is a constraint-based approach without any incentive and collaborative view that might result in the opposite effect than the one intended.

Moreover, we express our deep concern that forced disclosure of trade secrets cannot be favorable for EU attractiveness. It is essential that the proposed regulation does not set rules that will negatively affect businesses, resulting in the loss of competitive advantage. Our members insist on the necessity to protect intellectual property rights and trade secrets, notably for creative products for which it is important to be mindful on data to be shared. Rules must be proportionate and fit for purpose. Protection of trade secrets is a central concern for Luxembourg's industry, which is asking for more legal safeguards in this regard while one of the Data Act's goals is to establish trust in data sharing. The EU should as well consider finding solutions to elements of business confidential data, which does not enjoy protection today.

KEY MESSAGES

JOINT POSITION PAPER

on the proposal for a Data Act

1) Default of clarity in many definitions

- Definition of "*data*"
  - Too broad definition of "*data*" and not consistent with the objective of the proposed regulation to unleash the potential of the data economy.
  - Necessity to clearly define what kind of generated data fall into the scope and which ones do not.
    - ➔ Definition of data to be clarified and narrowed.

- Definition of "*product*"
  - Too broad definition of "*product*".
    - ➔ Suggestion of inserting the exclusions of products mentioned in Recital (15) in the article.

- Definition of "*related services*"
  - Too broad definition of "*related services*" resulting in difficulties to identify the frontier between the different related services.
    - ➔ Need to clarify the reason for the distinction with other physical products excluded in Recital (15).

- Definition of "*public emergency*"
  - Too broad definition which leaves large room for the Member States to qualify what an emergency situation is or is not.
    - ➔ The list of examples mentioned in Recital (57) shall be set forth in the regulation and expanded.

2) B2B and B2C provisions

- Different situations in B2B and B2C context
  - Chapter 2 tackles B2B and B2C data sharing aspects simultaneously, whereas data sharing situations and the parties involved vary from one context to another.
    - ➔ B2B and B2C should be treated in two different chapters.

- Obligation to make data accessible
  - Data accessibility must be provided "*by default*" by the manufacturer.
    - ➔ Represents challenges for businesses and creates an unbalance between more mature and less mature businesses as regards compliance costs.
  - Obligation for manufacturer to provide the "*nature*" and the "*volume*" of data to be generated.
    - ➔ Nature of data must be clarified as based upon the use of the product.
    - ➔ Volume of data should be deleted as very difficult to assess "before concluding a contract".

- Right of user to access and use data
  - Requiring the data holder to give access to data generated "*without undue delay*" leaves room for interpretation between the parties and may lead to abuses.
    - ➔ Replace by "*within a reasonable period of time agreed between the parties*", which would be more appropriate and adjustable to every situation when implemented in practice.

- Right to share data with third parties and data obligations of third parties receiving data.
  - Article 6 §2 (c) authorises sub-delegation of data to another third party "*when this is necessary to provide the service requested by the user*".
    - ➔ User must keep a control over data used by third parties and must authorise sub-delegation.

- Trade secrets protection
  - The Data Act provides that trade secrets shall be disclosed only if specific measures are taken to preserve their confidentiality, creating a risk for businesses and a significant loss of competitive advantage.
    - ➔ Model of non-binding contractual terms to be provided by the EC as in Article 34.
    - ➔ Ensure proper enforcement of other regulations regarding IP and patents such as Trade Secrets Directive.
    - ➔ More safeguards to be provided for confidential commercial information which differ from trade secrets.

- Dispute settlement
  - Members States shall certify a Dispute settlement body for some dispute between the data holder and the data recipient in B2B context. However, this kind of non-binding arbitration system does not exist in all Member States such as in Luxembourg. This will therefore incur huge administrative, cost and organisational burden to include and articulate such system in the current country legal landscape. Article 10 leaves many legal questions open and does not provide sufficient guidelines for Member States to set up a harmonised, efficient, fast and inexpensive system, which may also create a ground for fragmenting the practices across Europe.
    - ➔ Many clarifications to Article 10 are needed to enable Member States to implement such a body and to articulate it in their country's legal system.

3) B2G provisions

- Notion of "*exceptional needs*"
  - Too broad scope of exceptional needs allowing public sector bodies to request data access.
    - ➔ Data access request in exceptional needs situations must not become the normal trend.

- Compensation
  - No justification of the distinction between making data freely available in case of public emergencies and against reasonable compensation in other exceptional circumstances.
  - Time, technical, and organisational costs remain the same in both public emergencies and other exceptional needs situations.
    - ➔ Businesses shall be able to request compensation in cases of public emergency requests for data sharing.

4) Cloud switching

- Obligation for the Provider of Data Processing Services (PDPS) to remove obstacles to effective switching
  - PDSP shall ensure cloud switching to another data processing service, covering the same service type, which is covered by a different service provider.
  - Notion of "same service type" too vague.
    - ➔ Different use cases shall be considered to reflect complexity of cloud switching.
  - Lack of clarity of "obstacles" which could lead to a broad list of potential criteria labeled as such.
    - ➔ Responsibility of the switching should be shared between PDPS and customers. A collaboration should be built between the customer and the original and destination PDPS for a swift switching.

- Contractual terms concerning switching between PDPS
  - 1 month period is unrealistic to operate a "one size-fits-all" switching process and not reflecting the realities of services and elements of the infrastructure to be transferred.
    - ➔ (Reasonable) switching timeline should be agreed between the provider and the customer and not determined by the Data Act.
    - ➔ Reference shall be made to reversibility elements set forth in existing guidelines from the EBA or the DORA Regulation in order to specify the exit plan.
    - ➔ A list of requirements shall be defined in the contract terms and conditions for legal clarity.

- Withdrawal of switching charges
  - Financial burden rests only on existing provider whereas switching obligations should reflect the variation of complexities and choices involved in the switching process and establish a value accordingly.
    - ➔ As a minimum, switching charges should be compensated at cost.

JOINT POSITION PAPER

on the proposal for a Data Act

INDEX

JOINT POSITION PAPER

on the proposal for a Data Act

JOINT POSITION PAPER

on the proposal for a Data Act

LEGAL ASSESSMENT AND KEY MESSAGES IN DETAIL

I. SCOPE & DEFINITIONS (CHAPTER 1)

The scope of the Regulation is unclear due to the imprecision of several definitions.

A. Definition of data (Article 2 (1))

The definition of "*data*" is too broad and not consistent with the objective of the proposed regulation, while a clear definition of data is key for the fulfilment of the Data Act objective to enable data sharing.

For a common understanding and legal certainty, it is important to clearly define what kind of generated data fall into the scope and which ones do not. Indeed, several layers of data coexist (raw data vs inferred data / logs, technical logs, user tracking, data, meta data) and the practice reveals that not all data are relevant or necessary to users and some data are only of use to administrators.

Additionally, the reference to "*any compilation of such acts*" lacks clarity and adds fuzziness to the common understanding of the text. We wonder whether this would imply that filtering data herds, normalizing them, proceeding with statistics, and doing prediction or using machine learning algorithms results fall into the scope of the regulation or not.

Moreover, if the Commission refers to raw data, then, will it be appropriate to refer to compilation of data?

Consequently, we request the definition of data to be clarified and narrowed.

B. Definition of product and related services (Article 2(2) & article 3(3))

In our opinion, the definition of "*product*" is very broad and targets physical products which generate and collect data. However, Recital (15) excludes a specific set of products such as tablets, smartphones, personal computers which are designed for processing data and involve a human interaction. As a matter of clarity, we would suggest inserting directly in the text of the Regulation, those exclusions in the definition of product and not only in the Recital.

The definition of "*related services*" is also very broad which results in difficulties to identify the frontier between the different related services. Moreover, the large extent of services covered will inevitably lead to disproportionate complexity in implementation. To illustrate that, in our understanding, the excluded physical products mentioned in Recital (15) are also viewed as gateways to digital services. Nevertheless, they have a wireless internet connection which is a digital related service, provided by telecommunication operators. It appears, however, that fixed internet connection boxes are not excluded. The reason for such a distinction with other physical products excluded in Recital (15) needs to be clarified.

C. Definition of data holder (Article 2 (6))

The Data Act defines the "*data holder*" as either the one who has the" *right and obligation*" imposed by the law to make data available or the one having "*the ability to make available certain data*". In respect of the second aspect, we consider that the "*ability*" is a very broad notion that invites to interpretation. Indeed, "*ability*" does not necessarily mean that the data holder can make data available but rather that he will be required to develop new technical capabilities and infrastructures. This provision will be source of legal uncertainty and dispute, and we therefore recommend removing it.

D. Definition of functional equivalence (Article 2 (14))

The "*functional equivalence*" definition refers to "*a minimum level of functionality*". It is unclear what is meant by a minimum level of functionality. Here again, we wonder if the Commission will set some technical standards and a common minimum level of functionality that all companies providing data processing services should meet or not. If the Commission intends to do so, we question the legitimacy of the Commission to attain for itself such a role.

Most of all, businesses are concerned that the obligation to have a minimum equivalent level of functionality may result in a down-levelling of the cloud market and reduced innovation due to the standardisation of services. Indeed, when changing cloud provider, customers generally want to upgrade functionalities. Requiring the new provider of data processing services to "*deliver the same output at the same performance and with the same level of security, operational resilience and quality of service*" may set an obligation to invest in a functionality it never offered in the first place or that may have no customer demand for its target market. We believe this may result in practice in a strong intervention into business models (by forcing transparency on service models) and further constitute an impediment to innovation.

E. Definition of public emergency (Article 2 (10))

The definition of "*public emergency*" is very broad. Furthermore, as per the Recital (57), "*the existence of a public emergency is determined according to the respective procedures in the Member States or of relevant international organisations*". It results from this observation that there is a large room for the Member States to qualify what an emergency situation is or is not. Based on this approach, Member States can embed different types of events, which would be contradictory with a harmonisation goal. Implementing this definition may result in fragmentation of the Single Market and moreover does not include any safeguards to data security. Recital (57) also mentions a list of examples which are qualified as public emergency situations. For narrowing down the concept and ensure legal certainty, we ask for this list to be set forth in the Regulation and expanded.

Additionally, companies operating in different Member States might face challenges as they would potentially be subject to different legislation depending on where they are located (this could be particularly complexed in a context of group of Pan-European or Globally active). Therefore, the question arises as to what national law should prevail. We strongly recommend the legislator to align this topic with the OECD discussions on "government access to data held by private companies".

F. Missing definitions

The Data Act also contains some other notions that have not been defined, leading to legal uncertainty and enforcement obstacles, such as:

- Competing product
- Consumers
- Operators of data space
- Manufacturer
- Supplier
- Third party

In addition, it is specified that the Data Act is a horizontal legislation and that some sectoral texts will be built upon it. Therefore, it is crucial that the Data Act's definitions are specific, otherwise, there could be significant consequences on other texts if definition issues arise in the Data Act.

II. BUSINESS TO CONSUMER AND BUSINESS TO BUSINESS DATA SHARING (CHAPTER 2)

A. Suggestion to separate provisions on B2B and B2C data sharing

Chapter 2 tackles B2B and B2C data sharing aspects simultaneously, whereas data sharing situations and the parties involved vary from one context to another. Indeed, industrial and consumer connected products and related services generate different category of and volumes of data. Furthermore, information useful to businesses is not necessarily useful to consumers, and vice versa. Consumers are unlikely to be as interested in as much information and B2C data are usually connected to personal data covered by the GDPR.

Additionally, contractual obligations in B2B and B2C context are not the same, hence consumers and businesses should be protected by distinctive safeguards.

Logically, we recommend separating B2B and B2C requirements in two different chapters.

B. The obligation to make data accessible (Article 3)

According to Article 3 paragraph 1, the manufacturer is required to design and manufacture IoT products and to provide related services in such a way that the data generated by their use are **by default**, easily and securely accessible (can also be directly accessible, depending on the specifics) to the user.

Data accessibility "by default" could represent a challenge for some businesses in the state of their current process and system. For example, some businesses have created their data management system to have by default encrypted data and to create a secure environment, which makes the data impossible to access, whereas the Data Act encourages to change the approach in favour of an easy and secure transfer by default. **Therefore, some businesses will be unable to meet the obligations set forth in this article, unless they completely review their data management approach and paradigm.**

Likewise, the compliance cost will constitute an issue. Indeed, on the one hand, some businesses would not necessarily need to make higher investments to be compliant with the Data Act requirement, since they already have in place data governance policy (process delivery, data architecture, data segregation, etc.) that they would just have to adapt towards a new target group,

the users. On the other hand, businesses which are less mature with data management topic, would need to invest more in compliance to make it technically feasible. This would create an unbalance between more mature and less mature businesses.

Article 3 paragraph 2 aims at adding data-specific transparency obligations before concluding a contract for the purchase, rent or lease of a product or related service. Some minimum information listed in the said article must be provided to the user such as the nature and the volume of the data likely to be generated using the product or related services.

The enforcement of this provision would require further clarification on who shall provide the requested information. Indeed, in the chain of relationship in the B2C context for instance, the manufacturer is usually not part of the purchase agreement which is signed with the retailer.

The **"nature" of data needs to be clarified**. Several layers of data coexist (logs, technical logs, user tracking, data, meta data) which are not necessarily accessible (for e.g. tracking that a user wrote something in the safe) or useful to the user, but may be of great value to some administrators for technical tracking. If all data generated by products or related services are included, companies will face significant efforts complying with the obligation. Our comment is linked to the necessity of narrowing the definition of "data" that we expressed before.

Furthermore, the "**volume**" expected to be generated depends on the use of the product, the number of users, the frequency of use, etc…which is very difficult to assess "*before concluding a contract*". We suggest **deleting the information on "volume"** from the requirements.

C. Right of user to access and use data (Article 4)

Article 4 paragraph 1 provides that where data cannot be directly accessed by the user of the product, upon request of the user, the data holder is under the obligation to make available to the user the data generated via the use of IoT products or related services, without undue delay, free of charge, and (where applicable) continuously and in real time. The terms "*without undue delay*" leave room for interpretation between the parties and may lead to abuses. Our strong opinion is that this provision shall be replaced by the terms "*within a reasonable period of time agreed between the parties*", which would be more appropriate and adjustable to every situation when implemented in practice.

Article 4 paragraph 4 provides that users are prohibited to use the data to make competing products. The absence of definition of "competing product" will raise enforcement issues. We wonder, however, why competing related services are not included in the provision. The provision shall be extended to competing related services as well as follows: "*…to develop a product or a related service that compete with…*". Same request applies as well for Article 6.2. (c).

Article 4 paragraph 6 provides that the use of non-personal data shall only be governed by a **contractual agreement** between the data holder and the user. According to a literal reading of the article, manufacturers of products or providers of related services appear to be excluded from this provision. However, what about the situation when the manufacturer or provider of related services is also the data holder? Will they be entitled to access data or not? We consider, firstly, that contractual agreements shall never prevent manufacturers of products and providers of related services from accessing data "by default" to perform predictive maintenance, updates, and improvements of products and services. Secondly, contractual agreements should not prevent them from innovating, creating new products or related services. This could eventually lead to competitive disadvantage towards users or third parties. This article needs to be clarified more in this regard.

D. Right to share data with third parties and obligation of third parties receiving data (Article 5 and Article 6)

The proposed text does not provide a definition of "third party", leaving it up to users to define the third party of their choice, according to their preferences. Nonetheless, we note that gatekeepers as defined in the DMA are de facto excluded from such choice, according to Article 5 paragraph 2. As a matter of fact, the provision contradicts one of the Data Act's objectives, which is to empower users to dispose of their data. **In our opinion, the Data Act should not restrict users' freedom of choice of third parties, provided that other regulations, such as competition law, are followed.**

Further concerns on the article text focus on the fact that there is no provision governing the relationship between the user and the third party that we can read. In the absence of an obligation to formalise a contractual relationship between the user and third parties, one can anticipate user struggling in practice to seek for the third party's liability in the event of data breach (such as a data use beyond the agreed purpose and violation with the regulation, etc.).

Furthermore, it is highly likely that the user will lose control over the use of data by third parties whereas it is crucial that the user must keep a control over data used by third parties. Article 6 §2 (c) authorises sub-delegation of data to another third party "*when this is necessary to provide the service requested by the user*". Subdelegating data creates a chain of recipients, which may differ from the original intended use. We believe that sub-delegation must always be authorised by the user and not let to the discretion of the third party. **Third parties must also be required to fulfill transparency obligations regarding the use of data to both users and data holders. The right balance needs to be found for these provisions, as an overly complicated data control obligations or solutions that may not protect legitimate forms of data monetisation could discourage future service development in Europe.**

E. Trade secrets protection (Article 4 (3) (Rights of users) - Article 5 (8) (Sharing with third parties' context) - Article 8 (6) (Obligations for data holders' context) - Article 19 (2) (Public sector bodies' context)

The Data Act provides that trade secrets shall be disclosed only if specific measures are taken to preserve their confidentiality. Not only this provision is vague, but it also poses practical issues.

While we understand the rationale of the Commission that trade secrets shall never become a general excuse to deny data access, we cannot ignore that once trade secrets are disclosed, third party hold the information and could develop a derived product (not competing product) based on this information. Moreover, despite the signature of non-disclosure agreement, data holder does not have any oversight over the handling of trade secrets once disclosed.

With regards to trade secrets, it is essential that the Commission provides model of non-binding contractual terms to support the parties in drafting and negotiating contracts as provided for in article 34.

Furthermore, when breach happens, damage has in general already occurred since other companies could have already taken advantage of the information leaked on the market. In such a case, remedy cannot generally intervene in a short timeframe, if ever, and can hardly compensate the immediate prejudice. **Enforcement of other regulations regarding IP and patent is critical. E.g.: Trade Secrets Directive shall be used as a reference as well as transfer of IP rights (licensing) rather than forcing trade secrets disclosure.**

Lastly, we regret that the Data Act does not refer to and protect confidential commercial information which differ from trade secrets. More safeguards are necessary in this respect in accordance with competition law.

III. OBLIGATIONS FOR DATA HOLDERS LEGALLY OBLIGED TO MAKE DATA AVAILABLE (CHAPTER 3)

A. Conditions of data sharing: FRAND terms (Article 8)

The Data Act provides that data must be made available to data recipients "*under fair, reasonable and non-discriminatory terms [(FRAND terms)] and in a transparent manner*".

We firstly point out that FRAND terms may vary from one country to another and will be subject to court interpretation.

Moreover, Article 8 establishes a reversal of the burden of evidence on the data holder who will be under the obligation "*to demonstrate that there has been no discrimination*" in case of discrimination claim raised by the data recipient. The reverse burden of proof appears to be consistent with the approach set forth in the GDPR. However, we are in a context of non-personal data and we question on the rationale of such a reversal of the burden of proof. Furthermore, we also wonder to whom the data holder will have "*to demonstrate that there has been no discrimination*". Will it be to the data recipient or to the regulator or a judge, etc.? The provision imposes a substantial burden on the data holder and is not clear, which will certainly raise practical challenges in enforcement.

Lastly, the proposal does not stipulate objectives criteria for discrimination, as does the GDPR. In practice, this will also have to be settled before the courts and give rise to various interpretations depending on the jurisdiction involved.

We are of the opinion that this provision will raise the risk of market fragmentation.

B. Compensation (Article 9)

The rationale behind the proposed regulation is to enable and enhance the data market, rather than making users pay for access to their data. Indeed, we strongly support that the monetisation of data shall not be introduced.

However, we believe that the notion of "*reasonable compensation*" introduces ambiguity, since negotiations between the data holder and the data recipient might never end. Clarifying the costs incurred by the data holder is essential to a common understanding of the compensation. For instance, in the B2G context, Article 20(2)[5] provides for more details about what the compensation should include.

Article 9 paragraph 3 provides that the agreed compensation is not preclusive of other Union law or national law implementing Union law from excluding compensation or providing for lower compensation for making data available. This provision shall be accompanied by safeguards if a Member State uses this right, notably by duly justifying why this category of data should be excluded from compensation and explain how this should be necessary and proportionate.

[5] Article 20. (2) "*Such compensation shall not exceed the technical and organisational costs incurred to comply with the request including, where necessary, the costs of anonymisation and of technical adaptation, plus a reasonable margin.*"

C. Dispute settlement (Article 10)

We understand that the dispute settlement body is intended to settle dispute between data holders and data recipients, i.e., in the context of B2B data transfer. Each Member States shall certify an existing dispute settlement body or, in the absence of which, establish and certify such a body, based on the criteria set forth in Article 10(2). As per Article 10(8), the dispute settlement body appears to be a kind of "*non-binding arbitration*" since the decision is binding on the parties only if the parties have explicitly consented to its binding nature prior to the start of the dispute settlement proceedings.

While we praise the intention of a less formal dispute resolution, the current proposal considers an overly decentralised system that affords Member States and authorities the discretion to enforce rules differently and lead to different practices across the EU. This may be contrary to the aims of creating a harmonised legal framework under Article 114 of the TFEU.

Further, it is worth of note that the non-binding arbitration system does not exist in all Member States systems such as in Luxembourg. The Data Act, by imposing the establishment of such a body, will considerably increase the burden on each Member States in terms of organisation, cost, training of the body members, etc. but also to include and articulate such a system in the country's legal landscape. Article 10 leaves many legal questions open and does not provide sufficient guidelines for Member States to set up a harmonised, efficient, fast and inexpensive system, as explained hereafter:

- The decision of the dispute settlement body is not necessarily binding, which will raise questions about the usefulness of this mechanism since the decisions will not be enforceable,

- If the parties decide that the decision is binding on them, the question of **enforcement** of the decision will then arise. In Luxembourg, this would probably require modification of local laws for the decision to be enforceable or it would be needed that the Data Act assimilates the decision to an arbitral decision for instance, in order to allow the decision to benefit from the applicable regime to the enforcement of arbitral decision,

- If the decision is binding but not enforceable under local law, this means that the parties will still need to bring the case to court to have a judgement that will be enforceable. In such a case, would it be possible and ultimately what would be the benefit of having a dispute settlement body?

- There are also many procedural considerations that would be raised in practice such as what would happen if the dispute settlement body does not render its decision within the 90-day period of time set forth in Article 10(7)? Following the decision of the dispute settlement body, would there be a kind of appeal right and before which jurisdiction? If a party is not satisfied with the decision of the dispute settlement body, would this party keep the right to file a lawsuit before the court as per Article 10(9)? What is the meaning of "*the right of the parties to seek an effective remedy before a court or a tribunal of a Member State* "?

- The dispute settlement body will not be able to decide all types of disputes (such as dispute on compensation which is not included), which could lead in practice to fragmenting the disputes that can be heard by the dispute settlement body and those that must be brought before a court. This will be difficult to manage in practice and it is very likely that the parties will bring the entire dispute before the court to have a binding decision.

These examples of legal uncertainties and gaps will complexify the implementation of such a body in the Member States and will create a ground for fragmenting the practices across Europe.

Therefore, if the Data Act does not allow for the creation of a body with harmonised and efficient rules in the EU, one may wonder whether the Member States should not be allowed to use their own dispute resolution systems on the basis of existing local systems.

The Luxembourg legal system already provides for alternative dispute resolution mechanisms. In this respect, mediation would be a very appropriate mechanism for business-to-business disputes which has proved to work in practice and has the advantage of allowing companies to maintain the dialogue, which is important in the business relationship to reach an agreement.

IV. UNFAIR TERMS RELATED TO DATA ACCESS AND USE BETWEEN ENTERPRISES (CHAPTER 4)

The instrument of an unfairness test includes a general provision defining unfairness of data sharing-related contractual term complemented by a list of clauses that are either unfair or presumed to be unfair.

In situations of unequal bargaining power, contractual agreements on data access to and use or the liability and remedies for the breach or the termination, which exempt the "stronger" party from liability for negligence or give the 'stronger' party the exclusive right to interpret any term of the contract, shall be deemed unfair and non-binding. This concerns "take-it-or-leave-it" situations where one party supplies a certain contractual term and the micro, small or medium-sized enterprise cannot influence the content of that term despite an attempt to negotiate it.

It seems to us that some terms such as "Grossly deviates" and "good commercial practice" as well as "unilaterally imposed" are very unspecific and subject to interpretation. For a better understanding, a closer look at good commercial practice shall be considered and an analysis of existing general case law shall be undertaken.

As far as we understand, it is the contracting parties that supply the contractual terms who have the burden of proving they were not unilaterally imposed on the other party. Nevertheless, proving a negative fact is a very difficult task in practice. We believe this provision is unenforceable and creates an unbalance between the parties that is neither justified nor proportionate.

V. BUSINESS TO GOVERNMENT DATA SHARING (CHAPTER 5)

A. Obligation to make data available based on exceptional need (Article 14)

Our understanding is that all data holders, except micro or small enterprises, shall make data available to public sector bodies, Union institutions, agencies, which demonstrate exceptional need for the data. The access to data will be for free in case of public emergency and against a reasonable compensation in the other cases. Compensation should be foreseen for both emergency and non-emergency cases given the effort for companies will be the same in both cases, potentially even higher in emergency cases.

Our members indicate that:

- For the sake of overall data protection, public sector bodies would also need to provide proper data security safeguards (at time of compliance) that demonstrates equivalence to the data holder's prevailing standard. This will provide security in the EU industry about protecting trade secrets and business confidential data as well as any personal data contained in the data set.
- Some storage services might hold encrypted data which decryption key belongs only to the data owner. In the case of exceptional needs, the storage provider will be able to meet the requirements, but the data may not be accessible by public sector bodies. Public sector bodies will have to obtain the decryption key from the data owner to be able to further use the data, who decides whether to provide the key or not. In Luxembourg, it is not mandatory for the data storage service provider to be able to decrypt the data. The co-legislators should keep in mind that the relationship is not only bilateral but can be multilateral.

While we understand the rationale behind the exclusion of micro and small enterprises, as laid out in Article 14 (2) and detailed in Recital (56) "*to limit the burden on businesses, micro and small enterprises should be exempted from the obligation to provide public sector bodies and Union institutions, agencies or bodies, data in situation of exceptional need*", with the expanding data economy, many more start-ups have data-driven business models and hold data which shall be useful to the public sector. In other words, this exclusion does not align with what the proposed Regulation is intended to achieve. Incentivising SMEs on a voluntary basis to share data could also be beneficial.

B. Notion of exceptional needs (Article 15)

The exceptional needs provision expands the possibilities for public sector bodies to request data beyond "force majeure" situations. In addition, the scope of these circumstances could be construed widely, increasing the likelihood of unclear situations, and it should be avoided that this exceptional legal ground to request data becomes the normal trend to request data access by public sector, due to the broadness of the cases of recourse. We are of the opinion that B2G data sharing is supposed to be a last resort measure.

C. Modalities of data request (Article 17)

We welcome the detailed approach in Article 17. This being said, even though sanctions in case of non-compliance with the public authority's request appear to be necessary (since in the absence of which businesses could be quite reluctant to comply with the request), we question the risk of fragmentation of the internal market due to non-uniform application of sanctions by the Member States.

D. Compliance with data request (Article 18)

Data sharing obligation in the context of B2G is not subject to any contractual obligation. Further safeguards shall be provided in article 18 concerning the contractual obligations between data holders and public bodies pertaining to intellectual property and trade secrets protection.

Article 18 paragraph 6 provides that "*where the data holder wishes to challenge the request, the matter shall be brought to the competent authority referred to in Article 31*". It is worth of note that data holders do not have access to remedies in case of disputes against public sector bodies regarding the use of data. We recommend adding the ability to use the dispute settlement mechanism set forth in Article 10 into Article 18.

On another note, data handling by public sector bodies raises security concerns, since public sector bodies are increasingly targets of cyberattacks. Public sector bodies must consider risks including cybersecurity risks and implement security measures to protect data. We regret that no provision addresses this fundamental point in the Data Act.

E. Compensation (Article 20)

As far as compensation is concerned, the distinction between making data freely available in case of public emergencies and against reasonable compensation in other exceptional circumstances is not justified. Indeed, time, technical, and organisational costs remain the same in both public emergencies and other exceptional needs situations. Therefore, businesses shall be able to request compensation in cases of public emergency requests for data sharing. Furthermore, the cost for pseudonymisation or anonymisation which are burdensome processes, should never be for free and included in the compensation calculation, since it is costly, time and resources consuming for businesses.

F. Contributions of research organisations or statistical bodies in the context of exceptional needs (Article 21)

Article 21 stipulates that public sector can share data with individuals or organisations in view of carrying out scientific researches, analytics or official statistics. Individuals or organisations shall act on a "*not-for-profit basis*" or in the context of a "*public-interest mission*" recognised in EU or Member States law.

These "not-for-profit" status and public-interest mission notions are too vague and should be clarified. Businesses consider that they should at least be active in the field of the concerned research and present guaranties of qualification for performing the work. Otherwise, it would open the path to many abuses.

VI. SWITCHING BETWEEN DATA PROCESSING SERVICES (CHAPTER 6)

As a general comment on chapter 6, we fully support the objective followed by the proposal to unleash the cloud market and end with vendor lock-in practices.

However, provisions applying to data processing services are too vague and the process provided therein is not realistic to implement. It will be quite a challenge for providers of data processing service (PDPS) to comply with the requirements as currently set forth in the proposal.

A. Removing of obstacles to effective switching (Article 23)

As per Article 23 paragraph 1[6], providers of a data processing service shall ensure that their customers can switch to another data processing service, covering the same service type, which is

[6] Article 23 § 1: providers of a data processing service shall take the measures provided for in Articles 24, 25 and 26 to ensure that customers of their service can switch to another data processing service, covering the same service type, which is provided by a different service provider. In particular, providers of data processing service shall remove commercial, technical, contractual and organisational obstacles, which inhibit customers from:

- terminating, after a maximum notice period of 30 calendar days, the contractual agreement of the service;
- concluding new contractual agreements with a different provider of data processing services covering the same service type;
- porting its data, applications and other digital assets to another provider of data processing services;

maintaining functional equivalence of the service in the IT-environment of the different provider or providers of data processing services covering the same service type, in accordance with Article 26.

provided by a different service provider. In particular, providers of data processing service shall remove commercial, technical, contractual and organisational obstacles. This obligation shall only apply to obstacles that are related to the services, contractual agreements or commercial practices provided by the original provider.

- Regarding the "*same service type*", PDPS agree on the fact that the notion of "same type of services" is vague and need further clarification, notably up to which level it should apply (stop at); whether it is the way that is provided to the end customer meaning based on the functionalities they use or whether it is at a higher level. The service types proposed by PDPS are actually pushed by the customers. For instance, when an IaaS (Infrastructure-as-a-Service) service is founded on different technologies as such, it mostly relies on the customers' requirements in terms of technology they would like to use. Some additional features might need to be put in place for the switching process.

  Additionally, in higher level of the stack, for instance at the platforms or services levels, which are most often tailor made, switching process as set forth in the current proposed regulation will be unpracticable. Moreover, by requesting PDSP to offer the same service type and the switching process between two PDSP, it is unlikely that PDSP will start producing harmonised services across them and the side effect of this provision would lead to a reduced choice for the customers in the EU market.

  Practically speaking, from one project to another, it is not that easy to proceed with the switching from one PDPS to the other, at least not as simple as specified in the dedicated provisions.

  In our opinion, the different facets and possible use cases have not been considered deeply enough in the Data Act provisions which seem to be based on a too "simple" scheme of switching process that does not reflect the complex reality of cloud switching.

- The meaning of "*obstacles*" is unclear as well. It could lead to a broad list of potential criteria that could be labelled as such. From a compliance perspective, it seems to be quite heavy and very difficult to implement if not clearly defined further.

  In practice, it will not be easy to switch from a cloud service to another. Indeed, as far as the switching process is concerned, all the obligations should not uniquely burden upon the original PDPS. There is not so much diversity of infrastructures, but as mentioned platforms and services are generally tailor-made which renders the switching impractical. This will lead to standardisation and will reduce the choice in the market which is against innovation. We recommend considering a collaborative approach, a joint operation between the customer requiring the switching and PDPSs, both originated and destination one. A highly part rely on the customer, especially if it is a B2B customer.

  The responsibility of the switching should be shared between PDPS and customers. The different steps of the switching process must be considered and to whom allocate them to in terms of responsibility.

  Generally, customers have the application landscape to manage as well as business requirements in terms of business continuity and risk management. Hence, they have constraints regarding the migration hours, etc. to mitigate their risk properly. Therefore, a big part of the switching also relies on the customer side. A coordinated plan together with the customer and the PDPS must be set up accordingly.

  PDPS can make the environment to extract data and make the transfer easier.

B. Contractual terms concerning switching between providers of DPS (Article 24)

Article 24 paragraph 1 states that the rights of the customer and the obligations of the provider of a data processing service in relation to switching between providers of such services shall be clearly set out in a written contract. Contractual terms shall include (a) clauses allowing the customer, upon request, to switch to a data processing service offered by another provider or to port all data within a mandatory maximum transition period of 30 calendar days, (b) an exhaustive specification of all data and application categories exportable during the switching process and (c) a minimum period for data retrieval of at least 30 calendar days, starting after the termination of the transition period.

(a) The period of 1 month to operate a "one size-fits-all" switching process appears completely unrealistic. The needed period of time depends on the services and the elements of the infrastructure to be transferred upon the choices of the customer. For instance, the former PDPS cannot bear the responsibility to get the extracted data being readable for the new PDPS. It could to the best be made sure that there is an environment for customer to extract the data in a standardised format which is easier to transfer from one PDPS to another. This also raises legal question about the freedom of the parties to negotiate the time needed for the switching. This is a prescriptive provision and not coherent with the current B2B practices.

The Data Act shall avoid setting deadlines that do not reflect realities and within which there is a risk that PDPS will deliver a shoddy work to please customers. For the PDPS to offer a customised switching process based on the services to be switched, the (reasonable) switching timeline should be agreed between the provider and the customer and not determined by the Data Act.

(b) The exhaustive specification of data should be the responsibility of the data controller (i.e. the customer/user in the Data Act) and not the one of the original provider of DPS since generally customers know best which data is processed (data are not necessarily known by the service provider (especially when the latter is only in charge of the infrastructure layer), but launched at the application level).

Article 24 paragraph 2 provides that where the mandatory transition period is technically unfeasible, the provider of DPS shall notify within 7 working days after the switching request has been made, duly motivating the technical unfeasibility with a detailed report and indicating an alternative transition period, which may not exceed 6 months.

PDPS value that the 7 working days to oppose the technical feasibility of the switching request is unrealistic and the 6 months alternative is also not appropriate and shall be agreed between the parties as well.

We would suggest that reference to be made to the reversibility elements set forth in guidelines from the EBA or the DORA regulation which do not limit the options of the parties (ie. customers and service providers) but require them to specify what the exit plan would be, based on the services at stake and the continuity required by the customer. Accordingly, we would suggest limiting the requirement for the parties in the Regulation to define in the contract terms and conditions the reversibility process and the exist plan. In this way, the following will be defined:

- the means of accessing the customer's data at the end of the contract (means of transfer),
- the request to the origin service provider to provide data in a standardised format,
- information to enable the customer to change provider,
- how long will this information (customer data and infrastructure information) remain available,
- what reversibility services from the Service Provider would be available, and their price (i.e. hourly rate and duration). Indeed, it is often difficult to determine a flat fee as the amount of services to be performed is not yet known, so only an hourly rate could be defined per type of profile needed for this migration.
- Service Provider's obligation to answer clients' questions (at a reasonable cost) to facilitate the client's drafting of their exit plans (with their new service provider if the clients do not take over the IT in house).
- Service Provider's obligation to continue providing the existing services until the transition, provided the customer continues to pay for the related services.
- Remedies in case of bankruptcy of the Service Provider allowing the customer to have access to the data and to the required information to facilitate reversibility to new service provider.

C. Withdrawal of switching charges (Article 25)

This provision is viewed as unfair by FEDIL members and the Chamber of Commerce. The Data Act creates a lot of burden on existing providers which have the responsibility to manage the switching whereas they ignore where the data will go to, which type of services will be switched, which new functionality or technical requirements (such as data format) might be required for the new cloud services, which renders the phase out difficult to assess, to foresee and to anticipate in terms of cost.

The switching obligations should reflect the variation of complexities and choices involved in the switching process and establish a value accordingly (as a minimum, switching charges should be compensated at cost). Therefore, it is unfair to transfer all responsibility on providers including the switching financial cost for any type of services without distinction. It is once again a prescriptive provision contrary to the freedom of contract.

More importantly, the rationale to intervene on cost allocation is unclear considering the absence of any market failure signs. In current conditions, destination providers provide credit offers and support to attract new customers to off-set data transfer costs imposed by the originating provider (not unlike other markets). Removing the possibility to recover costs for data transfer when switching, these costs will be recovered via other services, likely raising entry costs. It is not clear how the nascent cloud market will benefit from raising entry cost for new cloud customers.
Should a balanced compensation scheme not be agreed, providers will likely cover the cost from data transfers with revenues otherwise used for infrastructure investments.

D. Technical aspects of switching (Article 26)

Article 26 paragraph 1 indicates that providers of data processing services (…) shall ensure that the customer, after switching to a service covering the same service type offered by a different provider of data processing services, enjoys functional equivalence in the use of the new service.

We consider that clarification is needed on who between the original and the destination data processing services, carry the responsibility of ensuring the functional equivalence. Businesses indicate that it is not feasible to know what other functional equivalence are offered by others. Moreover, customers choose one provider out of another one because of the set of functionalities and parameters offered. In any case, the responsibility should be shared and proportionate.

Furthermore, when moving to a next cloud provider, customers want to upgrade functionalities. The Data Act sets an obligation for a provider to invest in a functionality it did not necessarily offer in the first place, which creates a risk of down levelling the cloud market and of stifling innovation.

VII. INTEROPERABILITY (CHAPTER 8)

A. Essential requirements regarding interoperability (Article 28)

Article 28 paragraph 1 lists essential requirements to be followed by operators of data spaces to facilitate interoperability of data, data sharing mechanisms and services such (a) the dataset content, (b) the data structures, data formats, vocabularies, classification schemes, taxonomies and code lists shall be described in a publicly available and consistent manner, (c) the technical means to access the data, (d) the means to enable the interoperability of smart contracts within their services and activities shall be provided.

Our members point out that data controller would be the customer. Therefore, in terms of data set content, access etc. the responsibility should not only be on the provider side but on the customer's side who decides on the content, the means of accessing to them etc. The provider of DPS is only able to provide advice to its customer on interoperability parameters while the customer will have the final world on the set up according to its requirements.

B. Interoperability for data processing services (Article 29)

Article 29 paragraph 4 stipulates that the Commission is enabled to mandate the development of harmonised standards for the interoperability of data processing services.

Generally speaking, industry driven standards are more innovation friendly. Furthermore, there are enough feedbacks from industry to set the appropriate and relevant standards. Since it is technical, specific technical standardisation bodies should be attributed the role of proposing standardisation, and not the Commission. Moreover, we would recommend involving all stakeholders in a collaborative manner, mostly industry.

VIII. INTERNATIONAL ACCESS AND TRANSFER (CHAPTER 7)

As per Article 27, providers of data processing services shall take "all reasonable technical, legal and organisational measures, including contractual arrangements" in order to prevent transfers that would create conflict with EU law or Member states law. Where a decision or judgement of a court and any decision from an administrative authority of a third country requires access or sharing of non-personal data held by a provider of DPS, their enforceability will be subject to an international agreement or, in the absence of which, in the event certain conditions are met (if it has been verified that the third country's legal system (1) requires the reasons and proportionality of the decision to be set out, that the court order or the decision is specific in character, and (2) that the reasoned objection of the addressee is subject to a review by a competent court in the third country, (3) which competent authority is empowered to take duly into account the relevant legal interests of the provider of such data.

From businesses' standpoint, this provision will complexify the management of data for several reasons:

- To remain competitive, they need to ensure to have support of companies outside EU as well, notably in international group context.

- From a practical standpoint, the obligation not to transfer or give access to data in the event that it would conflict with EU law or Member States law is too vague and too broad. A provider of DPS may host data from many countries and cannot perform a legal watch of the different countries' legislation. It can be for instance justified for some type of sensitive sectors such as financial data but extending this provision to all data will be very complicated to manage for businesses and would add costs. **The implementation of this provision will be challenging in terms of organisation and people and may increase the risk of discontinuity of the service.**

- **Moreover, the proposed Data Act application of the GDPR rules for the transfer of non-personal data appears to be disproportionate and not appropriate.** Such a move will increase the compliance burden on companies without a tangible benefit. Moreover, the Article 27 requirements should not be placed on businesses but addressed at the international level.

IX. DATE OF ENTRY INTO FORCE

The Data Act provides that the obligation contained therein would apply from 12 months after the date of entry into force of the Data Act.

Considering the constraints imposed by the Data Act from a technical, organisational, processing, administrative and legal standpoints, the period of 12 months appears to be too short and not realistic at all. **A minimum of 2 years should be left to each Member States and stakeholders to implement the Data Act requirements.**

Contacts:

FEDIL

Céline TARRAUBE

Adviser Digital & Innovation

celine.tarraube@fedil.lu

T: (+352) 43 53 66 – 610

M: (+352) 621 497 370

Chamber of Commerce

Mona-Lisa DERIAN

Legal Advisor

monalisa.derian@cc.lu

T: (+352) 42 39 39 – 366