September 3rd, 2021

Joint answer to EC consultation on Data Act

Who we are and why our input matters

We are the Belgian, Dutch, French and German CIO-associations, communities of Chief Information Officers (CIO's) and other senior leaders that are responsible for digital technologies and digital transformations within private or public organizations. These are all European business users of digital technologies. We don't represent ICT suppliers and consultants.

The European Commission is preparing a proposal for a regulation, known as the "Data Act", to facilitate access to and use of company data and to review the rules on the legal protection of databases. Data is a valuable intangible asset for our members, public or private organisations that use digital services and produce data in the course of their business activities**. Our associations welcome this text which they see as an opportunity to free up inter-company data sharing and as an essential and coherent complement to other existing or planned regulations,** notably: the GDPR, Platform to Business, Digital Markets Act and the Artificial Intelligence Act. Regarding the Data Act, we encourage the Commission to:

1. Consider the position of business users when drafting the Data Act and restore a fair balance in the data economy
2. Ensure that business users keep full control over their data
3. Improve data portability and possibilities to switch cloud providers
4. Ensure fair contract terms between providers and business users regarding data
5. Protect European business data from extraterritorial access

General considerations on the Data Act in light of our associations' work

Indeed, for our associations, the Data Act is an opportunity to create a framework of trust to allow European companies to enhance and safeguard the value of their data. **The twofold challenge of this text is therefore to secure horizontal access and circulation of sensitive company data and to guarantee the protection of these information assets, particularly in the face of extraterritorial legislation** such as, but not limited to, the US CLOUD Act. Insofar as data exchanges and processing are now largely based on cloud computing services provided by non-European suppliers, the regulation of the practices of these intermediaries is essential.

A strong and fair regulatory framework for the use and sharing of data, which ensures transparent and shared responsibility between different parties, such as business users of digital technologies and providers of digital solutions and services (hereinafter: suppliers) is key to our members. Therefore, our associations strive through their actions to:

1. To stop the abuse of vendor lock-in and unfair practices by suppliers of digital solutions and services and to ensure fair market practice in the digital technology markets. **Restrictions on access or data transfer are one of the main sources of lock-in.**
2. To ensure that digital products and services - including software - which enter the European market, are demonstrably safe and comply with European regulations. **This compliance covers in particular the field of data, with the GDPR, and the future Data Act.**
3. To ensure that **control over data remains with business users of digital technologies** without this leading to additional costs or being frustrated by other impeding practices.

Our four associations have mobilised their members extensively to participate directly in the consultation on the Data Act. They are also at the disposal of the European Commission to cooperate and exchange experiences and knowledge in order to make sure that the future data regulation delivers on its promises. The scope of this future regulation is very wide - with important consequences for our members - so we would like to set out a number of guiding principles and points of vigilance. This position is accompanied, in annex, by a large amount of documentation, resulting from work with our members, which we are making available to the Commission.

Summary of our positions on selected sections of the questionnaire

Our associations wish to draw the Commission's attention to 4 sections in particular.

Section II. Business-to-business data sharing

The fairness of cloud computing services is the guiding principle for business-to-business data sharing. Business data not only has a commercial value, but is also indispensable today, on the one hand, to feed algorithms (without data, there is no AI) and to refine the knowledge about the end-user/beneficiary to improve the services offered. In this context, the inter-company exchange of data within the same vertical or complementary sectors of activity brings added value for the end customer (extension, deepening, customisation of services) as it allows a seamless user experience. With the development of cloud computing, inter-company data exchange relies on intermediaries such as digital service providers. This leads to an overly powerful position for suppliers of digital technologies.

Through the Data Act, we invite the Commission to provide a clear framework allowing the European Union to regain control over the actions of players in the cloud market, by deciding on the rules that apply to data sharing, rules that need to be fair, equitable and transparent. **The**

value derived from the data should be fairly distributed and not be appropriated by third party intermediaries.

In this perspective, it is decisive to guarantee that data owners retain full control over whether they share or transfer data, to whom, and on what terms. The evolution of digital services within companies transformed the concept of data use, storage, ownership, and control. The digitization of the economy led to creating business solutions where data is jointly owned by the digital service providers, in particular software publishers and cloud computing service providers, and its business customers. Commercially highly sensitive datasets should be protected, in particular when considering the overall shift of IT solutions to cloud-based services to take into account the security considerations, which makes most of the suppliers of such services gatekeepers in a practical sense**. Business processes, which are part of a company's know-how, are also part of this sensitive data whose ownership and value must be protected.**

Section IV. Clarifying rights on non-personal Internet-of-Things data stemming from professional use.

Data generated by “smart” objects are becoming a fundamental part of the Digital economy, so the access to these data is crucial for the future growth of European Businesses.

The supplier of a connected ‘smart’ object plays a crucial role in deciding on the data which is produced by the object, but the most important is his role on allowing, or not, the access to this data by third parties. In case he is the only one who can collect, interpret and turn the data in value, the fairness of the market is seriously disturbed. As long as the collection of the data is not disturbing the correct and safe functioning of the object, the data should be available at a reasonable cost to the whole ecosystem and allow value creation for every player.
To have a fair data ecosystem that can play its constructive role, we ask the European Commission to publish new rules to prevent a manufacturer from limiting/closing the access to the data source for its own commercial purposes. A balance needs to be struck between the commercial/service interests of the manufacturer, those of its business user community and the very important data security considerations.

Section V. Improving portability for business users of cloud services

Data mobility is a key element of customer independence towards IT suppliers. Hence we strongly support the ambition to improve portability for business users of cloud services. In particular considering that self-regulatory ('SWIPO') codes of conduct did not achieve their objectives, due to the structural unbalance of means between business users and providers of digital services. Self-regulation failed to efficiently mitigate unfair practices and we don't expect this to change as long as market conditions favour the suppliers.

A clear European framework with clear prohibitions would therefore be key to foster Europe's competitiveness and innovation. To prevent vendor lock-in, business users need to be able to easily switch cloud providers with their data and applications and need fair conditions to have access and get a copy of part or all of their data in cloud applications. This should not only occur at the end of the contract, but also on demand or automated for a daily or regular use.

Section VII. Intellectual Property Rights – Protection of Databases

Unfair practices by suppliers who appropriate contractual rights to the business user's data must be stopped. Databases contain sensitive personal and/or commercial data. The business user must remain the owner of his data under all circumstances. This intellectual property right must be guaranteed, including in databases.

The increasing integration and co-development of services based on business users' data and the digital services of suppliers makes it more complex to assign ownership of "enriched" data and to distribute its value**. It is essential to protect data-producing business users from contractual practices granting suppliers rights over their data** (access and use rights for benchmarking purposes in particular, even if the data is anonymised). On the one hand, this practice contravenes the GDPR (for HR or customer databases, for example) and may put the business user in a non-compliant situation. On the other hand, this practice gives suppliers a competitive advantage by creating a distortion of market information. Finally, it constitutes an additional economic drain on the business user, who is already paying licence fees or a subscription for the use of the supplier's services.

Therefore, our associations would also welcome provisions to end unfair practices by IT suppliers which absorb with unilateral contracts, data from their business users. Failure to consider these risks can be detrimental to the European economy. **Business data is particularly exposed in Software as a Service, an exponentially growing cloud market.** The preservation and respect of the confidentiality of non-personal data in SaaS is unclear and largely unregulated. For example, some online service providers contractually grant themselves the right to analyse their customers' data for market research purposes and, in addition, grant themselves ownership of the analysis results. In many cases, business users do not have the negotiation position to change or remove

these clauses (or only with great difficulty), and the anonymisation of the data cannot be checked by the business user.

We consider a revision of the "substantial investment standard" of the Sui Generis right is needed, to clarify that the investments made by the cloud providers to provide the cloud services should not be taken into account to grant Sui Generis protection.

So far, it seems to us that the "Sui Generis" right can have a reverse effect and that fair clauses in the contracts are a better solution, as mentioned in section II and section V.

Section VIII. Safeguards for non-personal data in international contexts

We urge the European Commission to help businesses to reduce their risk of non-compliance and protect them from external interference by creating a clear and consistent legal framework.

Business data are a sensitive and very valuable assets for organizations, that the future "Data Act" should **protect from the exposure of extraterritorial application of third country laws, as well as any undesirable access and use, especially from third parties**. In the current geopolitical context, extraterritorial legislations can support economic intelligence and industrial espionage policies against which the European legislator must protect its organizations and citizens.

In this regard, we believe it is essential that the future Data Act should be an instrument for the protection of sensitive corporate data, in order to protect them against, in particular, non-European legislation in the same way as personal data, as recalled by the CJEU in its ruling of 16 July 2020 on the invalidation of the Privacy Shield.

Appendix: Documented Positions

Appendix to Joint answer to EC consultation on Data Act
Documented Positions

Section II: Business-to-business data sharing
Section IV: Clarifying rights on non-personal Internet-of-Things data stemming from professional use
Section V: Improving portability for business users of cloud services
Section VII: Intellectual Property Rights – Protection of Databases
Illustration of our positions: **A real and operational example** that shows a business running with the fairness rules as guiding principle

Position on section II: Business-to-business data sharing

In the questionnaire, the introduction of this chapter reads as follow

"In this section, we would like to hear your views on fair contractual terms and conditions as an important tool that can stimulate companies to exchange their data while safeguarding the freedom of contracts and in full compliance with applicable legislation (such as the GDPR or competition law). The Data Strategy intends to promote business-to-business (B2B) data sharing which will benefit in particular start-ups and SMEs, putting emphasis on facilitating B2B voluntary data sharing based on contracts. We are seeking options for promoting fairness in contracts governing access to and use of data…

We understand that your question is about fair/unfair practices in contracts for data sharing.
The detailed list in point A hereunder comes from practical experiences of our members in contracts with software providers or Cloud Service providers, not data sharing contracts as such. Yet we are convinced that most of these clauses are also very important in B2B contracts for data sharing. Moreover, contracts with Software providers and Cloud Service Providers are nearly always linked to data sharing in one way or another.

Hence, in the following pages we'll provide concrete inputs on unfair practices and how reduce them:

A. a list of the most important unfair practices our members face in dealing with suppliers and what we see as necessary changes;
B. the Belgian law offering an example of how to regulate unfair business practices.
C. some thoughts on the need for protocols for sharing data in ecosystems.

A. The most important fair/unfair practices for the 4 associations

The 4 associations share these concerns since more than 5 years and have invested time and effort to gather fair/unfair practices clauses in B2B contracts between business users and Software providers or Cloud service providers. This has given a long list of clauses. To be able to pinpoint the most important ones we have asked each association to put priorities on the list so that we have ended with the most important clauses.

Please find hereunder a list of fair/unfair practices that have been chosen as essential by the 4 associations:

Our associations will develop these principles with concrete examples, to be able to make them understandable for all stakeholders.

Contractual terms and conditions should be clear, unambiguous and not unilaterally changeable: No 'URL conditions', clear and concise definitions, customer should be able to determine their obligations easily, customers should be able to rely on stable conditions. This includes metric definition, solution descriptions, term and termination rights (exit clause), anniversary and renewal notification, etc. Terms and conditions should be listed and available in the contract or terms of purchase (order form or similar). Vendors could be allowed to make changes to an agreement, if there are no material nor financial adverse effects to the Customer and with upfront notification. In case terms and conditions are not attached to the signed agreement, at least all previous and current standard t&c's should be available for consultation online. This also includes: name changes, support lifecycle and price lists.
Contractual terms should not restrict or discriminate for customer's choice of cloud provider, outsourcing partner or hardware platform: Pricing should be non-discriminating and uniform between running workload in the cloud (any choice of cloud vendor), on prem or in any hybrid setup. Even converting from on-premise to cloud should be cost neutral or at least safeguard the customer investment.
Contractual terms for licensing and subscriptions should be free from geographic and entity restrictions: at least within the same customer group or holding. (subject to law, for example import and export restrictions). All current and future entities should be covered, as long as they are majority-owned. Vendor should accept the 'Customer' definition in accordance with the intended use and contracted scope of the services/solutions.
Contractual terms should allow customers to use progressive technologies and deployment models: Contractual terms should within reasonable timeframe adopt licensing rules that give the benefit of technological process to the customer. More granular and efficient management of compute resources should be recognized and supported. For example: physical computing -> Virtual computing -> Containers

Commercial models should not be changed unilaterally and adhere to an active 'opt-in' principle:
Customer should not be forced from a perpetual license model with maintenance to a subscription model during the same renewal stream and without material changes to the solution's functionality.
Maintenance and support conditions should be capped and/or transparently communicated upfront, commercially available features should not be enabled by default.

Commercial models and offerings should be consistent and reasonable, not mixing 'best of both worlds':

Commercially available products under a subscription model (i.e. cloud) should represent the flexibility and scalability as technically marketed. Subscriptions should therefore be non-committed, flexible and pay-as-you-go. Vendors should not require upfront investment or large usage fees during development and deployment.
Software offered as a perpetual right to use (i.e. licenses with maintenance) are naturally a frontloaded investment, which provides benefit for both customer and vendor upfront. The subsequent maintenance results in an agreed and predictable cost for the customer.
Mixing both models is always detrimental for the customer value: Changing from perpetual to subscription is only in the benefit of the vendor and the customer loses the initial investment combined higher subsequent subscription charges.
In addition, vendors requiring upfront investment under a subscription model attempt to frontload the initial investment, while the subscription does not represent a perpetual right to use (or intangible asset).

Vendors should not create a technical or commercial lock-in:
IT vendors should adhere to open technical standards and not intentionally restrict customers in any commercial or technical matter to exercise portability right, switching providers, regain ownership of data.
Customer solely rely on the termination clause of a contract as sole remedy against vendor lock-in or exit strategy, since there are a lot of hidden costs in change management, training, adoption and configuration which makes the cost of switching higher than only the fee for the services/solutions.

Service Levels and product specifications should be explicitly listed and relevant in the context of the customer: including the consequences for not meeting the service levels (credits, termination rights, etc.)
Definition of maintenance windows and excluded time needs to be stated in the contract.

Vendors should accept consequences which are sufficiently material compared to the impact of such failure and aligned with the critically and scope of the service for the customer.

The foregoing also applies to IP infringements, regulatory compliance and waivers.

Vendor and customer should fulfill regulatory obligations: GDPR, PCI, etc. For example under GDPR: fulfill its duties as Processor and/or Controller, adhere to contracted location of data, etc. Vendors should take responsibility for the data they manage on behalf of the customer. Furthermore they should provide cloud technologies in such a way that customers can comply to regulations they are subject to.
Customer should remain owner of own data and all data uploaded or processed by the service/solution: The agreement should specify the Customer's right to their own data, the processing and the restrictions. Data that has been processed and potentially enriched by the vendor solution, should still remain solely property of the customer. The algorithms remain ownership of the vendor.
The scope, execution and intended outcome of audit should be clearly defined in the contract. The audit right in itself is not unfair if customers formally agree to it in a contract. However, the outcome, timing, objectivity and intended purpose if often beyond the nature of a factual audit. Where possible, the software should be self-regulating so it does not lend itself to misuse or overuse, resulting in reduction of effort for the customer to prove compliance in case of an audit. During an audit, customers should not be held liable for software installed by default, but never used nor activated (for example by a license key).

B. The Belgian B2B Act - Law of 4 April 2019 on abuse of economic dependency, unfair terms and unfair market practices between undertakings

To handle the general problem of unfair practices in B2B, another interesting input can inspire the Data Act: the **Belgian B2B Act** combines an open norm prohibiting abuse of economic dependence with a number of unfair practices in both a grey and black list.

A deliberate choice was made to keep the personal scope of application general, and not to limit it, for example, to the protection of SMEs only. The existence of a privileged position is not necessarily linked to the size of the company; certain small niche players also abuse their position when the business customer is economically dependent on them (exploitative abuse). The assessment of the imbalance in a contract, or of the existence of unfair market practices, is, moreover, independent of the size of the enterprise, but concerns a factual assessment.

The Belgian legislator indicated in the preparatory works that it has long been known that certain companies often have no choice but to accept the contract terms of their co-contractor without any real possibility of negotiation. In addition, they often have to accept the negative consequences of contractual terms negotiated to their legal disadvantage. Even the European Commission stated, when preparing the text of what is to become Directive 1993/13/EC on unfair terms in consumer contracts: "Standard contract terms play an important role not only in consumer contracts, but also in contracts between professionals...It should be borne in mind that many of the arguments put forward are also applicable to other contracts, especially contracts between sellers or suppliers".

Law of 4 April 2019 on abuse of economic dependency, unfair terms and unfair market practices between undertakings ("B2B-Act").

So far, European legislation has only remedied the market failures arising from the power imbalance between the contracting parties in a Business-to-Consumer (B2C) context. The Belgian legislator concluded that such power imbalance might also occur in Business-to-Business (B2B) relationships where one of the businesses can disproportionately leverage a superior position to the detriment of its contracting partner.

The B2B act therefore regulates the abuse of economic dependence, the adoption of unfair terms in B2B contracts and unfair market practices. We will discuss the first two categories of rules.

Economic dependence

Economic dependence is defined as the position of submission of one company to another, characterized by (i) the absence of a reasonable equivalent alternative that is available within a reasonable time and under reasonable conditions and costs (ii) that allows this company to impose conditions that cannot be obtained under normal market conditions.

The position of economic dependence is not prohibited; only the abuse of it. The act lists examples of such abuses which are entirely inspired by the list of prohibited abuses of a dominant position contained in article 102 TFEU (see above).

As opposed to article 102 TFEU, economic dependence under the B2B-act does not require an absolute dominant position, measures by means of market share or ability to exclude competitors from the market. Instead, the assessment requires a case-by-case assessment in which the specific circumstances of the relationship of the parties are taken into consideration.

The Belgian competition authorities are fully competent to investigate such practices and impose sanctions, including fines up to a maximum of 2% of the worldwide turnover of the company concerned. Ordinary judges too will remain competent to sanction such practices and to impose damages.

Unfair terms

Parallel to Directive 93/13/EEC of 5 april 1993 on unfair terms in consumer contracts, the B2B act introduces four clauses (in the so-called black list) which are always prohibited in B2B contracts, as well as eight clauses (the so-called grey list) which are only allowed in contracts if they can be justified.

This relates to our position in A.

C. Ecosystems for B2B data sharing.

Next to B2B contractual clauses, operational data sharing requires the definition of a data dictionary and data exchange protocols common to the members of the Ecosystem, in a structured, commonly used and machine readable format.

The GAIA-X project intends to promote and develop these kinds of sectoral Ecosystems, by providing open standards and protocols to facilitate inter-company data sharing as well as portability.

Moreover the Software Providers or Cloud Service Providers that gather the data from a lot of customers will play an important role in B2B data sharing: They should develop and promote data exchange protocols to facilitate data sharing between the customers using their platform, but also with customers using other Software Providers or other Cloud Service Providers.

Position on section IV: Clarifying rights on non-personal Internet-of-Things data stemming from professional use.

Data generated by “smart” objects are becoming a fundamental part of the Digital economy, so the access to these data is crucial for the future growth of European Businesses.

The manufacturer of a connected 'smart' object plays a crucial role in deciding on the data which is produced by the object, but the most important is his role on allowing or not the access to this data by third parties. In case he is the only one who can collect, interpret and turn the data in value, the fairness of the market is seriously disturbed. **As long as the collection of the data is not disturbing the correct and safe functioning of the object, the data should be available at a reasonable cost to the whole ecosystem and allow the value creation for every player.**

We met several manufacturers not allowing or limiting the access to the data for third-party IoT companies. The main reason used by those manufacturers is the loss of warranty on the product. This "threatening" has no technical and legal ground, but many customers are afraid to sign contracts with third-party IoT service providers.

In case the access to the machine generated data is prohibitive and is not granted by a fair contract, staring with building of IoT services for those products is riskful for the customer as well as for its third-party IoT service providers. **If the manufacturer can limit/close the access to the data source by different technical / financial means, the data ecosystem is disturbed and cannot play its constructive role**.

Members of the business users community trying to build IoT related business by monetizing machine generated data, or trying to use this data for improving their internal operations, are facing these **limitations. The major ones are technical related, limiting or closing the access to the data, but in many cases the financial conditions are prohibitive as well**. It seems, there are just a few manufacturers being open to collaborate with third party IoT service providers by sharing the data collected from the products.

To have a fair data ecosystem that can play its constructive role, we ask Europe to publish new rules to avoid that the manufacturer can limit/close the access to the data source by different technical / financial means. A balance needs to be struck between the commercial/service interests of the manufacturer, those of its business user community and the very important data security considerations

Position on section V: Improving Portability for business users of Cloud services

Art. 6 porting of data Recital 29 of the **free Flow of Non-Personal Data ("FFNPD")** explicitly acknowledges that, as opposed to the situation for consumers, "the ability to switch between service providers is not facilitated for those users who act in the course of their business or professional activities".

As a result of article 6 FFNPD, a multi-stakeholder group called "SWIPO – Switching Cloud Providers and Porting" was created to facilitate the creation of codes of conduct. In July 2020, several codes of conduct were published, addressing IaaS (Infrastructure as a Service) and SaaS (Software as a Service).

Yet, there are remaining ambiguities and gaps in the codes of conduct. We refer to the extensive analysis conducted by Beltug and Cigref and transmitted to the SaaS SWIPO workgroup on February 11th, 2020.

Some examples are:

- The SaaS CoC does not assure data export for inter-operability, nor porting at all times (for example for the purpose of periodic back-ups).
- The SaaS CoC does not assure data export in case of organisational changes (eg. mergers, bankruptcy, etc. of business customers).
- The SaaS CoC does not mitigate certain operational risks relevant to all business customers, such as the unwillingness by the cloud service provider to port the data in case the cloud service customer is in breach for some aspects of the contract or deletion of data by the cloud service provider without explicit acknowledgement of the successful porting by the business customer.

We note the failure of self-regulation in the digital services market, due to the structural imbalance between the parties in this market, and **recommend that part of the SWIPO** (SWItching cloud and POrting data) **codes of conduct become ex-ante rules.**

From a practical perspective, it is disappointing to see that in August 2021 so few providers adhered to the IAAS CoC and none to the SAAS CoC (according SWIPO AISBL website communication). From users' perspective, there's no market knowledge, no provider's adhesion and thus no market effect.

These codes provide a list of good or wrong practices. Unfortunately, their implementation relies on voluntary adherence. Besides**,** the SWIPO codes of conduct should be revised to take into account the detailed analysis and the remarks formulated by our national user associations in this document: SWIPO. A new Code of Conduct for data import and data export for SaaS Suppliers: Observations and recommendations.(https://www.beltug.be/file/2094/2020.11.18_SWIPO_-_observations_and_recommendations_Beltug_-_Cigref_-_CI/)

Apart from these considerations regarding ambiguities and gaps, article 6 FFNPD and the resulting codes of conduct in general are limited to the provision of cloud services. The issue of vendor lock-in also

extends to the provision of software solutions which are hosted on premise.

Vendor lock in explained

Anno 2021, business-oriented software such as CRM software (customer relationship management) and ERP software (enterprise resource planning) is ubiquitous. Start-ups, SMEs as well as multi-national companies rely on these types of software to run their daily operations. The efficiency benefits of a well-organized and successful software solution can be substantial to a company. It has become one of the most important investments to remain competitive.

To answer the needs of companies active in a variety of industries and markets, such software solutions need to be flexible, scalable and compatible with companies' other software components and operating systems. Often times, businesses only have a few options to choose from with regard to the right software or cloud service which meets their business demands. Due to the large scale on which software and in particular cloud service suppliers operate, such suppliers leave little to no margin for negotiation of specific contracts with customers. This evidently results in supplier-favorable contracts.

Whenever a customer commits to a certain supplier, the costs of switching to another supplier, in case of dissatisfaction or because of a better business opportunity, are increasing throughout the duration of the relationship with the supplier. Due to the specific nature of business software as an often tailored product which interacts with other business software within an organization, customers face substantial costs in reorganizing their entire software or cloud infrastructure. While software license or cloud service agreements might grant customers the right to terminate the contract, often times the economic reality prohibits customers from effectively doing so. This effect is reinforced by the refusal of suppliers to technically facilitate the switching from one provider to another. Suppliers are able to consolidate their customer base by restricting the level of interoperability and data portability of the software and cloud services they offer. This leads to a situation of **vendor lock-in**: customers are deprived from a feasible opportunity to step away from their supplier.

The importance of business software and cloud services on the one hand and the issue of vendor-lock in on the other hand result in an **economic dependence of customers vis-à-vis their suppliers.** Due to such dependence, suppliers are able to leverage their position of power in the contractual relationship with their customers. This results in a plethora of unfair practices, such as unilateral price changes, the obligation to adopt new additional software products and/or services, highly imbalanced liability provisions, the inability to comply with the stringent conditions of the agreement, etc.[1] Dissatisfied customers are deprived from all bargaining power to address such unfair practices and have no other option than to accept. Moreover, they are also unable to object to such unfair practices by changing their software/cloud service provider.

We conclude that the economic dependence to software and cloud suppliers leads to a market failure, which is unlikely to be remedied by the market itself. This market failure not only harms business customers, small and large, but also impacts the development of the European economy and affects end-

users through consumer pricing and the quality of consumer products and services.

To conclude this section, we believe that the codes of conduct should be supplemented by Standard Contractual Clauses translating the Codes' requirement into contractual elements.

Position on section VII: Intellectual Property Rights – Protection of Databases

Instead of discussing this point theoretically we have chosen to analyse the application of the Directive 96/9/EC (Database Directive) based on the practical and operational example described at the end of this document.

Firstly, databases can be protected, when original, **under copyright law**. Copyright protection applies to databases (collections of data) that are creative/original in the selection and/or arrangement of the contents and constitute their authors' own intellectual creation.

In our example at the end of this document the structure of the rich and complex database – with more than 100 different tables linked together – created by the software provider is protected. Moreover, it is a trade secret so that a competitor cannot use this intellectual creation.

Secondly, databases for which a substantial investment has been made into the obtaining, presentation

and verification of the data can benefit from the protection **under the so-called "sui generis" right**.

In our example, the software provider made a substantial investment in developing migration tools – more than 100.000€ - and put in place a team of several people during 4 years – more than 500.000€ - to use these tools effectively to normalize and adapt the data coming from each broker to conform to the new database model and migrate these normalized data into the SaaS Application.

If the "Sui Generis right" would be applied, the software provider would obtain "near ownership" rights on the data normally owned by the insurance brokers or the insurance companies.

In our example **the "Sui Generis right" would be contrary to the fairness principle and to the contractual clauses that specify that the data remain full property of insurance brokers**.

When reading the Evaluation of Directive 96/9/EC on the legal protection of databases, published in 2018 we can read the following elements:

- *Page 12*

"The framers of the Directive took into account the economic and technical reality of the early 1990s, when copyright industries such as publishers were the main marketers of databases. The typical database of the time was static and offline. Scientific and legal databases or company catalogues on CD-ROMs are good cases in point.
Since 2005 there has been a shift in the economic and technological use and value of data. While, as a consequence of the CJEU rulings, the sui generis right, does not generally apply to data economy situations, increasingly more datasets may come to be considered databases. It is therefore necessary to assess whether the sui generis protection might extend to cases for which the right had not been originally designed."

- *Page 19*

According to the online survey, when users consider using a database (for instance, when a climate research institute considers using a private database commercialised by a firm that obtains data from multiple hydroelectric companies), they mostly worry about database prices and contractual terms and conditions, both ranking significantly higher than those restrictions that might be imposed by the Database Directive.

- *Page 38*

The sui generis right is an extra layer of intellectual property on datasets, fundamentally built on top of other legal protections, such as contracts, copyright, unfair competition rules or trade secret laws.

- *Page 39*

Yet the debate around a data ownership right has clearly revived, and is currently part of the policy reflections on the data economy around the globe.

- *Page 40*

The interaction of the sui generis right with the broader data economy is not fully clear at this stage and would need to be further monitored.

Conclusion

The example described at the end of this document can be generalized with (cloud) software providers like Microsoft, Google, Amazon, SAP, Oracle, …) that would be very happy to be granted "Sui Generis right" on the data of their customers and they probably can demonstrate that they have made "a substantial investment into the obtaining, presentation and verification of the data". This should be prevented, as it would enable such huge technology providers to exploit databases collected by their customers even more than is currently the practice. A practice moreover that the Digital Markets Act is aiming to redress.

The Data Act must make clear that **it is decisive to guarantee that data owners retain full control over whether they can share or transfer data, to whom, and on what terms.**

As it stands, the "Sui Generis right" may have a perverse effect on the protection of customer data. **It seems to us necessary to revise the standard of substantial investment,** taking into account the significant investments made also by the customer. **Such a revision could amount to clarifying that investments made to provide cloud services should not be taken into account for granting "Sui Generis" protection.**

Eventually, we remind that fair clauses in the contracts can be a good solution as well. This is the direction we took in other sections of the Data Act consultation:

- section II "**Business-to-Business data sharing**"
- section IV "**Clarifying rights on non-personal Internet-of-Things data stemming from professional use**"

So we have answered to these chapters with these elements.

Illustration of our positions - A real and operational example that shows a business running with the fairness rules as guiding principle in the Insurance sector

We provide this real-life example of the cooperation between business users and other business users and their cooperation with a cloud service provider. We presume this will be useful to understand our positions taken in:

- chapter II: Business-to-business data sharing
- chapter V: Improving portability for business users of cloud services
- chapter VII: Intellectual Property Rights – Protection of Databases

With this example you will also be able to understand how extensive the unfair strategic advantages of the software provider or the cloud service provider would be if the fairness rules were not applied.

The use case – Insurance brokers database

With more than 10 years of investment and experience, a software provider has developed an excellent application to manage all the functionalities required by insurance brokers to manage their business and has developed migration tools to help the insurance brokers to migrate their data on its SaaS platform. 11.000 users from 3.000 insurance brokers have made the migration of their data in this Application and are connected to this SaaS platform to manage their business.

So the software provider has gathered detailed data on 3 million households, 5 million people, 12 million active contracts and has stored 500 million documents.

What is the software provider allowed do with all these data?

Nothing else than the functionalities described in the Application for the use of the insurance brokers. The software provider is NOT THE OWNER of the data.

The SaaS contract between the software provider and each broker is clear about that:

"The software provider will host on its servers – or those of a cloud provider – all the data of the insurance broker … The data of the insurance broker hosted on the software provider servers – or those of a cloud provider – REMAIN FULL PROPERTY of the insurance broker."

The insurance broker might at any time receive a copy of his data following a procedure described in appendix of the contract.

In fact the broker can receive different kind of copy of his data:

- If the broker wants a one shot copy of his data,
  he can ask for a partial or full copy on demand, as mentioned in the appendix

  "Upon payment of the operational cost, the insurance broker will obtain a copy of all or part of his data and documents in the form of ASCII delimited files. Each table will correspond to a file."

- If the broker wants a daily copy of part of his data (for example the customer file or the accounting file) an automated procedure will be used for automatic daily file transfer.
- If the broker wants to analyse a part of his data (ex: the claims) he can initiate himself the transfer of a copy of the claims file to his PC.

- If the broker wants to transfer specific records (for example a car and the driver) to a registered user of the ecosystem (ex: an insurance company) he can initiate it himself.

In this example you can understand that portability is not only a file transfer process at the end of the SaaS contract. To the contrary, **data sharing is a daily and flexible requirement that is absolutely essential for the business users.**

The software provider guarantees explicitly that he – or his suppliers – WILL NOT ACCESS the data and will not make any use of the data except those described in the present contract (the functionalities of the Application) or the law.

The software provider engages explicitly to guarantee the perfect confidentiality of the data to which he would have access."

Each of the 3.000 insurance brokers remain full owner of their respective data so that there are in fact 3.000 separated databases and each broker decides to which user he gives access.

September 3rd, 2021

Sharing the data in this trusted ecosystem.

An insurance broker can decide to share some data (ex: car and driver data) with one or many insurance companies to ask for an offer. In return the company can decide to share the data of the offer – and then the contract – with the broker to update his database.

In this very productive ecosystem it might become difficult or even impossible to say if it is the broker or the insurance company who is the owner of the data, but one thing is sure:

The software provider will never have the ownership of the data nor decide which data exchange should take place. He is only responsible to provide the mechanisms for the secure data exchange.

Analysis of the data in this trusted ecosystem.

It is evident that statistical analysis of the data – or even AI analysis – might have added value for managing the broker business or the insurance company business or provide additional services to the customers.

It is the responsibility of the brokers and/or of the insurance companies with agreement of the brokers to ask for this kind of anonymized analysis.

Some or all brokers can decide to share data among them and ask for analytics on their data (ex: which clients are keen to take which products?).

The software provider will be paid to develop the tools and the processes to deliver the results to the responsible asking parties. He is of course not the owner of the results of the analysis.