Response to EC consultation on Data Act proposal

Our reference:	COB-TECH-22-048	Date:	17 May 2022
Referring to:	Commission proposal for a Regulation on harmonised rules on fair access to and use of data (Data Act)		
Related documents:			
Contact person:	Danilo Gattullo Policy advisor, Conduct of business	E-mail:	gattullo@insuranceeurope.eu
Pages:	5	Transparency Register ID no.:	33213703459-54

Key messages

- Insurance Europe welcomes the proposal as it sets out common rules on the use of data generated by connected devices, including how to access and share it. We also welcome an enhanced data portability right, which, among others, looks to improve technical standards for access and portability of data generated by individuals.
- However, robust sector-specific legislation on access to in-vehicle data is needed to provide the confidence and incentive independent service providers need to invest in new data driven services.
- In principle, trade secrets and business sensitive information should be excluded from data sharing obligations. The mere risk of having to disclose this data could hamper innovation, with negative consequences for the development of the European data economy.
- The objective of the Data Act should be to create a level playing field between all players in the data economy. It is, however, unclear why unilaterally imposed contract terms that are considered unfair shall be null only if the recipient is an SME.
- The scope and the scenarios of governments' access to data should be more strictly defined in the text.
- The relationship of the Data Act with other legislative provisions, especially the General Data Protection Regulation (GDPR), should be further clarified.
- The Data Act's provisions on cloud switchability are a step in the right direction and will help to establish a more competitive market for cloud computing services.

General remarks

Insurance Europe welcomes the Data Act's overall contribution to creating a single market for data, where data from public bodies, businesses and citizens can be used safely and fairly for the common good.

Data is at the core of the insurance business. Insurers process data to analyse the risks that individuals wish to cover in order to tailor products accordingly. In an increasingly connected world, access to data is essential to continue to offer innovative products. With access to and exchange of more types of data, the insurance industry will be able to offer innovative solutions and serve customers more effectively by, for example, improving existing risk models.

The insurance industry is therefore supportive of efforts to facilitate appropriate data sharing. It is important, however, that the Data Act, together with future sectorial data sharing legislation, strives to achieve a *true* level playing field between different players (including new ones, such as Big Tech), and ensures fair and equal

access to data across all sectors. If level field principles are not applied thoroughly, the future data economy may suffer from distortions in the market structure that can lead to less fair outcomes in terms of prices, quality, choice and innovation.

In addition, data sharing should always be carefully considered in the context of competition law and intellectual property law, which may constitute obstacles by impeding the contractual parties' ability to exchange data. Data which constitutes trade secrets or business sensitive information should not be subject to any data sharing requirements.

Finally, any data sharing framework should adopt a user-centric approach, in which users can choose which data they wish to share, with whom, and for which services. It is important to safeguard consumers' ownership of their data and to ensure that data sharing is consent-based. The scope of the customer's consent must be clear, specific and verifiable, while the purpose of the data sharing also needs to be clear.

Data Act welcomed, but robust automotive-specific legislation urgently required

Insurance Europe welcomes the Data Act proposal as it establishes an important right for users to access the data generated through their use of connected products, and to assign rights of access to that data to a third-party service provider of their choice.

However, while the Data Act represents a relevant step forward towards the development of the European data economy, it will not be sufficient by itself for the automotive sector.

Aside from the user's explicit consent to access their data, third party service providers in the automotive aftermarket sector require stand-alone access rights to the information and resources that are essential to develop competitive services. Under the Data Act approach, all these independent service providers would, however, only receive a derived right, which completely neglects the fact that these parties need, in the first instance, to know and test in advance what data and functions are in principle available and will be at their disposal. Therefore, only an autonomous and stand-alone access right to the tools and resources required to develop the means of access will enable independent service providers to develop innovative digital services in advance so that these can be offered, marketed and advertised to consumers or other data co-generators. In short, access rights must be backed by the proper means to exert them.

Insurance Europe, therefore, welcomes that the European Commission is considering proposing sector-specific legislation on access to in-vehicle data. Only a dedicated piece of legislation will provide the confidence and incentive independent service providers require to invest in new data driven services, which will benefit consumers and the whole of society by providing smarter, safer and more sustainable mobility solutions.

B2C and B2B rules on data generated by IoT products and related services (Chapter II)

Insurance Europe welcomes the proposal as it sets out common rules on the use of data generated by connected devices, including how to access and share it. The Data Act will give both individuals and businesses more control over their data through a reinforced data portability right, copying or transferring data easily from across different services, where the data are generated through smart objects, machines and devices. For example, a machinery owner could choose to share data generated by their use with its insurance company. Such data could help to develop or improve innovative digital services.

There should, however, be more clarity regarding the scope of the Data Act under Chapter II. These provisions would apply to data generated by the use of a connected product or related service including data recorded intentionally by the user. They would not, however, apply to inferred or derived data (Recital 14), as well as data resulting from any software process that calculates derivative data from such data, as these software processes may be subject to intellectual property rights (Recital 17).

Given the variety of internet of things (IoT) products and related services, the text should provide further guarantees about which data sets would be subject to data sharing under this Chapter. On this point, one can distinguish between data that is directly supplied and controlled by the consumer on the one hand, and proprietary data on the other, which is created by processing/enriching consumer data. Data holders should not be obliged to share business-sensitive information or proprietary data that they have generated and analysed/enriched themselves, and which is the outcome of their own work. As it is a key objective of the proposal to support the full realisation of the potential data-driven innovation, the scope of the data should be clear also in Article 4 and Article 5 of the regulation.

In principle, trade secrets should be excluded from data sharing obligations. The mere risk of having to disclose trade secrets could hamper innovation, with negative consequences in the long-term for the development of the European data economy. As a minimum, the Data Act should be clearer on the nature of the specific measures necessary to preserve the confidentiality of trade secrets.

- **Right to share with third parties**

  Insurance Europe welcomes the Commission's proposal to give users more control of their data by establishing the right to share data with third parties (Article 5). Individuals should be able to allow access to their data to a much higher extent than is possible today.

  The rights under Article 5 could be strengthened by clarifying that the data holder must ensure that it is not cumbersome or less attractive for the user to request the data to be shared with third parties.

  Additionally, to prevent undue burden for users and data recipients, the proposal could specify that the data holder must share the data in a market wide used and accepted format.

- **Level playing field**

  Insurance Europe welcomes that the proposal aims to address potential competition concerns by prohibiting the data recipient to develop competing products (Article 6(2)(e)) and by limiting access to gatekeepers as defined by the Digital Markets Act (DMA).

  The Data Act can help to create added value for consumers in the form of new and innovative digital services across various sectors. The European insurance industry is a comprehensively regulated and supervised sector with a sound conduct of business and prudential framework in place. It is important that the Data Act and any future data sharing framework respects the principle of "same activities, same risks, same rules" and safeguard a true level playing field, as recognised in recommendation 13 of the European Commission's expert group on regulatory obstacles to financial innovation (ROFIEG) recommendations.

  It is also important to state that a prohibition to compete with the product or related service that the data originated from does in no way prevent a third party from offering an (aftermarket) service that may be in competition with another service offered by the data holder. For example, it should be possible for a third party to continue offering a repair service even if it competes with the one offered by the data holder.

FRAND principles and unfair contract terms (Chapter III and IV)

The Data Act introduces the principle that whenever a data holder is obliged to make the data available to a third party, such data must be shared under fair, reasonable and non-discriminatory (FRAND) terms.

Under the proposal, data holders would be able to require compensation for making data available, based on a cost-based approach where the data recipient is an SME, and prevent discrimination between comparable categories of data recipients. In this case, costs for the SME would be limited to the cost of making the data

available. Where the recipients are larger companies, the parties would have the margin to negotiate a reasonable compensation (Article 9).

The proposed FRAND principles may be too vague and could result in a growing need for litigation. In particular, the proposal lacks a clear definition of what can be considered reasonable compensation.

It is also unclear why unilaterally imposed contract terms that are considered unfair shall be null only if the recipient is an SME. The objective of the Data Act should be to create a true level playing field between all players in the data economy. Unfair terms unilaterally imposed by the data holder should therefore not be binding for all potential data recipient.

In general, contractual freedom should be at the core of business-to-business relationships. Distortions in price negotiations occur when the data holder can unilaterally impose conditions for data access due to its market dominant position and it is not only related to the size of the data recipient. The legislator should, therefore, intervene with clear rules on framework conditions for data access, including price caps, in cases where there is a clear market distortion, such as in the case of access to in-vehicle data.

Another key obstacle in data sharing negotiations is to identify the scope of the data. This comes with important challenges as datasets may be mixed with personal and non-personal data. The determination of clear data perimeters — defining the raw data that would be needed for specific use cases — could be helpful in order to guarantee fair access to data conditions. However, given its complexity, such work should be carried out in close collaboration with stakeholders and based on actual use cases/business cases in the context of dedicated sectorial initiatives.

Overall, non-binding model contract terms for B2B data sharing contracts could be a useful tool to incentivise data sharing, especially for start-ups. However, industry should also be involved in drafting these models.

Business to government data sharing (Chapter V)

The proposal sets out an obligation to make data available to public bodies in case of public emergencies or in situations where public sector bodies have an exceptional need to use certain data. The reasons for government access should, however, be more strictly defined.

The proposal should better frame the concept of "exceptional need", leaving less room for (mis)interpretation. For example, the case described in Article 15 (c) considers the lack of available data preventing a public body from fulfilling a specific task in the public interest as an exceptional need. The data should not be available on the market and current measures would not ensure the timely availability of the data. Certain key aspects, such as the definition of what can be considered "timely", is, however, left subject to interpretation. Circumstances around the possible lack of data can often occur in the public sector (for example, in cases where new legislation is introduced) and the Data Act should not become the main tool thanks to which public bodies can request access to privately held data.

In its current form, the text would grant public sector authorities a broad discretion when requesting access to privately held data as they can determine, among others, key factors such as scope, duration and purpose of the data sharing obligation. This is problematic as such discretion can lead to legal uncertainty. In contrast, government access to data should be based on a legal basis that is sufficiently clear and foreseeable. The scope of the covered data needs to be more strictly defined, as well as the set of scenarios under which mandatory B2G data sharing would be required as a last resort. In the case of a lack of available data, public bodies should primarily rely on already existing instruments and methods to make the necessary data available (eg legislation to extend official statistics).

Finally, although Insurance Europe recognises the potential added value of the analysis for scientific purposes, any additional disclosure of the received data should be considered carefully in order not to undermine the exceptional character of the data sharing obligation. This should be clarified in Article 21.

Consistency with GDPR and other current legislation

To achieve its purpose of harmonising rules on data availability, it is key that the scope of the provisions of the Data Act and their relationship with other legislative provisions, especially the GDPR, are clear and that users' rights are not undermined.

At this stage, the interplay and consistency with current privacy rules are not fully ensured. In particular, it is unclear how the provisions under Article 6 will interplay with GDPR's rules on further processing (Article 6(4)).

The purpose limitation principle under the GDPR protects data subjects by setting limits on how data controllers can use personal data (Article 5(1)(b)). The principle has two key elements: personal data must be collected for 'specified, explicit and legitimate' purposes (purpose specification) and not be 'further processed in a way incompatible' with those purposes (compatible use). Further processing is, therefore, possible, provided that the new purpose is compatible with the original purpose. In this case, a substantive compatibility assessment on a case-by-case basis must be carried out.

The Data Act proposal sets out specific limits about how data received pursuant to Article 5 can be processed. Article 6(1) sets out a clear obligation for third parties to process the data received only for the purposes and under the conditions agreed with the user. While Article 6(2)(c) prohibits third parties to make available the data received to another third party, in raw, aggregated or derived form, unless this is necessary to provide the service requested by the user.

As the Data Act would complement, and is without prejudice to, EU law on data protection and in particular the GDPR, it is unclear how these rights can be reconciled. In order to ensure more legal certainty, the Data Act should be aligned with GDPR rules on further processing.

Cloud switchability (Chapter VI)

Insurance Europe welcomes the Data Act's provisions on cloud switchability which will help to establish a more competitive market for cloud computing services. Insurers have reported difficulties concerning the concentration of cloud service providers, which results in a lack of competition in the market and an imbalance in the negotiating power between the parties.

To fully enable companies and SMEs to switch freely between cloud services without undue burden, the provision in Article 24(1)(b) could be better refined. The requirement to include in the contract an exhaustive specification of all data exportable during switching process may be too burdensome depending on the level of required granularity. In this regard, a general description of the respective data should be sufficient.

Insurance Europe welcomes the Commission's intention to develop interoperability requirements for cloud processing services. It is important that such requirements take into account market-wide used standards as this would ensure that the cloud switching provisions will be effective in practice. It is also key to ensure that such interoperability requirements are aligned with other upcoming EU initiatives on cloud, such as the expected Commission's standard contract clauses.