acea

May 2022

Position Paper

Proposal for a Data Act

CONTENTS

KEY RECOMMENDATIONS

1. The notion of ‘accessible data’ should be introduced and defined. It should spell out manufacturers’ and data holders’ obligations to make available to users and relevant third parties, data that is accessible to them via an existing interface.
2. A requirement should be added to ensure that the user can safely access the data generated by the use of the product.
3. The concept of ‘directly-accessible data’ should be defined as data that is directly available from an on-device data storage, or from a remote server to which the data are communicated.
4. Users who are companies making commercial use of the products from which the data is generated, and that intend to use this data for commercial purposes, should not be entitled to access this data free of charge.
5. Users and third-party data recipients should be barred from using the data obtained from the manufacturer to develop a related service that competes with the product, or with the related service, from which the data originates.
6. The definition of ‘user’ should be amended to establish a primary user who would, in turn, be responsible for managing permissions for subsequent users who use, rent or lease the product from the primary user.
7. The ‘exceptional need’ under which public sector bodies may request privately-held data should be limited to situations of public emergencies.
8. The right to determine whether the sharing of trade secrets is strictly necessary should be granted exclusively to the trade-secrets holder, who should be entitled to determine what measures are put in place to protect trade secrets. Trade secrets should only be disclosed to a public-sector body if the data holder agrees to it, and when all specific measures agreed between the data holder and the public-sector body are taken by the latter to preserve the confidentiality of the trade secrets.
9. The data holder should be provided with detailed information regarding the identity of the recipient(s) of the data which is passed on by a public sector body (Article 21), as well as the activities which this entity will carry out. Trade secrets should not be passed on to a third party without the consent of the data holder.
10. Regarding international data transfers, Article 27(3) should be deleted or amended so that the assessment it requires is performed as part of a binding decision by a competent authority, upon notification of a data-access request from a third country by a data-sharing service provider.
11. The Data Act should apply 36 months after its entry into force, to provide sufficient time for companies to ensure compliance.

THE CONTEXT

In February 2022, the European Commission unveiled its proposal for a Data Act. This proposal sets out horizontal principles aiming at ensuring fair data access and use, as well as empowering consumers to remain in control of their data.

The European Automobile Manufacturers' Association (ACEA) supports the Commission's ambition to put consumers at the centre of the data-sharing process and to achieve fair, reasonable, and non-discriminatory access to data across all sectors of the data economy.

Already today, ACEA's members make vehicle-generated data available for third-party services, in adherence with the objectives of the European Commission's proposal. Data is shared in a manner that meets the customer's usage choices – while also ensuring the protection of the consumer's personal data and the safety and (cyber)-security of the vehicle and its occupants.

Vehicle manufacturers have implemented data-sharing models that are based on clear terms and conditions, ensuring that consumers know what data they share and with whom, in full compliance with privacy and data protection rules. They have implemented these models with tangible results across the automotive value chain and beyond, be it in the B2B, B2G or B2C segment. This includes data sharing to protect pedestrians and cyclists, and other road safety applications (eg the Data for Road Safety ecosystem, with data shared with national road authorities and service providers)[1]. Independent service providers can access vehicle data for repair and maintenance purposes, tailor-made insurance coverage, mobility planning and traffic management, as well as many other innovative services.

Vehicle manufacturers agree with the Commission that customers need to give permission to allow third-party access to data, and that they should always remain in control of data sharing. In that respect, ACEA is pleased to note that many of the principles laid down in the Data Act echo the recommendations already made by vehicle manufacturers in ACEA's position paper on access to data.[2]

However, ACEA is concerned that some of the provisions of this proposal go too far by imposing requirements that are simply unworkable. Such requirements will not deliver on the objectives of securing consumers' rights on their data and establishing a flourishing data economy in the European Union. Instead, they will create legal uncertainty as to how business-sensitive data will be handled and further shared once it is disclosed. This will likely have a discouraging effect on the quantity and quality of the data that businesses gather and process, thus contradicting the Commission's intention to promote the European data economy.

ACEA believes that legislation should nurture the market-driven approach, underpinned by the proportionality principle, and should create an environment in which both users and data holders feel safe in sharing data.

[1] See dataforroadsafety.eu
[2] https://www.acea.auto/publication/position-paper-access-to-in-vehicle-data/

The data economy, although largely debated, remains a rather new reality. Businesses that fall under the scope of the Data Act have only just begun to familiarise themselves with data sharing and to explore opportunities to extract value from it. Furthermore, requirements to share data have already been introduced by EU and national legislation, especially in the automotive industry. Businesses should be afforded some time to adjust to recently-introduced and upcoming legislation concerning data sharing.

The Data Act should not become a regulatory obstacle for European companies to grow and invest in high-quality data generation. Indeed, any framework for access to data should not constrain innovation and competitiveness by imposing requirements which will restrict manufacturers' choice of economic model. This would only limit their incentives to invest and compromise the dynamics of innovation, at a time when many sectors, including automotive, are evolving and the market for data and related services is emerging. Instead, it should lay down basic principles in key areas to safeguard fair and non-discriminatory access, technology neutrality, customer choice and – above all – people's safety and security.

ACEA therefore calls on the European Parliament and the Council to clarify this legislation to ensure that the principles that it lays down are served by requirements which facilitate data sharing. These requirements should be based on the principles of fairness, transparency, proportionality, reasonableness, and non-discrimination. The legislation should strive to preserve economic incentives to innovate and invest in connected products, and to generate and share data for all market operators, most of whom already share, or are looking to share, their data.

B2C AND B2B DATA SHARING

PRODUCT DESIGN AND DATA MANAGEMENT

The proposed Data Act states that manufacturers should design their products in such a manner that the data generated by their use are, by default, easily, securely and – where relevant and appropriate – directly accessible by the user (Article 3).

It also states that, where the data cannot be directly accessed, it should be made available to the user without undue delay, free of charge and – where applicable – continuously and in real-time (Article 4).

ACEA believes that it essential for users to know what data can be accessed and shared from their products. However, the notion of 'generated data', without any accompanying definition in the provisions of the proposal, raises questions as to the exact nature of the data that must made available to the user. It also creates legal uncertainty for data holders as to the extent of their obligations under these provisions.

From the onset, if should be understood that there are inherent limitations to the amount of data that can be managed in any given product, and that can be transferred to an interface where it can be accessed. This is true for many products that fall under the scope of the Data Act – the primary function of which is not to generate, manage, share and receive data. From a technical point of view, transferring additional data points often requires major

modifications to the physical architecture and software of a product, which in turn will require oversizing its computing power. Furthermore, any modification to the physical architecture, requires corresponding (cyber)security measures. Such modifications have a significant impact on the total cost, development processes and resource optimisation – not to mention on the environment.

This is especially true for a vehicle, which is a means of transport. Its primary function is to bring people and goods safely from one place to another, not to share data. As such, it requires high standards in safety, security and privacy, and its components must work under extreme 'automotive grade' conditions and in compliance with rules on type approval.

A lot of the data generated by the internal components of a product are not intended to be extracted. Rather, they are 'functional' data, meaning that their function is to allow the product to work as it was designed to. Only a small amount of this data is stored, while the rest is deleted automatically. In addition, some of this data is generated by components that are supplied by first-tier suppliers (and which may be proprietary) and is therefore not accessible to the manufacturer.

In the end, only a fraction of data generated by vehicle use is accessible to the manufacturer – or to anyone else for that matter. Forcing the manufacturer to design products so that all the data generated by their use can be stored, extracted, and made accessible to an interface (be it internal or external), may prove to be impossible. In any case, such an obligation would have severe consequences on the way manufacturers design and manufacture their product, and on the development (capital investment) and connectivity (operational cost) costs required to make all this data accessible to the user or a third party.

This would also have very practical implications for the consumer. The costs inferred by the design requirements in terms of processing power and storage would ultimately be reflected in the price of their product. Furthermore, data from a vehicle is transferred via a modem using cellular networks. Should the provisions of the proposal remain as currently drafted, this could mean that several dozen gigabytes of data would be transferred every single day via mobile networks for a single product. Transferring such an overwhelming amount of data would by far exceed current mobile data subscription models, placing extremely high costs on consumers and their mobile data plans. It could even cause the infrastructure to collapse.

Furthermore, the sheer volume of data would most likely overwhelm users, who would struggle to manage, let alone understand, the information. This would ultimately deprive consumers from any meaningful control over their data, preventing them from making an informed choice about the costs and benefits of sharing it.

For manufacturers, this new requirement on the design of the product would conflict with the principle of 'privacy by design and by default'. It would create substantial difficulties in terms of compliance with the principle of data minimisation, according to which the collection, processing and storage of data should be limited to what is necessary in relation to the purposes for which these data are processed or kept.[3] Finally, the processing, storage and

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regards to the processing of personal data and on the free movement of such data, repealing Directive 95/46/EC (General Data Protection Regulation), Article 5.

transfer of such vast masses of data would increase the energy requirements of the product, having a drastic impact on their sustainability.

EMPOWERING USERS TO MANAGE DATA

Providing consumers access to the data they need

Currently, data can only be made accessible if the design and architecture of the product allow for it. This data is accessible to both the manufacturer and the user, and can be used to provide a service for the customer. This is 'accessible' data, meaning that the data holder can obtain it from the product and share it. The user should therefore be aware of, and have access to it, and should be able to determine whether, and with whom, it can be shared.

ACEA therefore believes that the Data Act should enable products and related services to be designed so that the data that is generated by their use and is accessible to the data holder, is also easily, safely and securely accessible to the user (Article 3(1)). A data holder should make available to the user any data generated by the use of a product (or related service) that is accessible to the data holder (Article 4(1)).

Similarly, the Data Act should ensure that, upon a user's request, the data holder makes available to a third party the data generated by the use of a product or related service that is accessible to the data holder (Article 5(1)).

'Accessible data' should be defined under Article 2 as data generated by the use of a product that the data holder can request and obtain from the product onto an existing interface, via a publicly-available electronic communication service, in a digital, machine-readable format.

This would ensure that users can control the data that is obtained from their products, and determine who it is shared with. Furthermore, by ensuring that the user can grant data holders and third-party services providers access to the same data, this proposal would ensure that all market players have access to the same input to provide competing services to the user. This would create a level playing field, allowing market players to compete fairly and on equal grounds, and to continue to innovate in a way that benefits consumers and broadens their choice.

Defining users' means of access to their data

The proposed Act states that manufacturers should design their products in such a way that the data generated by their use are, by default, easily, securely and – where relevant and appropriate – directly accessible by the user (Article 3).

ACEA is concerned that the lack of definition of the concept of 'directly accessible' data in the proposal will create uncertainty for manufacturers as to what system they will be expected to put in place in order to comply with this obligation.

ACEA notes that some clarification is provided under recital 21 of the proposal, which states that "products may be designed to make certain data directly available from an on-device data storage or from a remote server to which the data are communicated".

While ACEA welcomes this clarification, we believe it would be beneficial to include it in a definition under Article 2 to give it legal effect.

Additionally, while ACEA believes that it is essential for users to have access to the data from their products – whether through an onboard storage system or through the manufacturer's server – we are concerned about the lack of guarantees provided to the data holder under Article 3.

The provisions of Article 3 do not provide any protection regarding trade secrets, contrary to the provisions of Article 4 and 5. Furthermore, the provisions of Article 3 may provide a user with the means to bypass the data holder, by transferring data obtained pursuant to Article 3 to third parties.

ACEA therefore recommends that the rules regarding non-disclosure of trade secrets provided under Article 4(3) are also extended to Article 3. Additionally, Articles 3 and 4 should state that data is only shared with third parties based on the provisions of Article 5(1).

Ensuring user safety and product security

While Article 3 of the proposal refers to security, it does not require that the data be made accessible to the user safely.

It is crucial to understand the distinction between security and safety concerns. Possible security risks, including cybersecurity risks, must be considered when manufacturers design connected products. The question of security, and especially cybersecurity, has to do with preventing unauthorised access to and tampering with the product's data. To that end, third parties who were not granted access by the user must be denied access, while those who were granted access must be clearly authenticated. Furthermore, the manufacturer has a duty to ensure that the right level of access is granted to authorised third parties, so that they can only access the data for which the user has granted them access, and which is necessary to provide the service to the user.

Examples of security risks for vehicles include the unauthorised coding of additional keys, unauthorised remote ECU reprogramming, or the cloning of the vehicle connection interface. Functions which may impact security must be addressed according to the best security practices. To ensure the vehicle's security, the manufacturer must adopt a cybersecurity management system and a strong authentication mechanism, in compliance with European and national legislation on cybersecurity, privacy and data protection.

In addition, there are functionalities that have an impact on safety, either because they interact with the behaviour of the product (for vehicles this includes for instance engine, brakes and steering), or because they distract the user when the manipulation of the product requires their full attention. It is therefore crucial to ensure that data are accessed at a time when they will not interfere with the normal operation of the product, and that any request or notification directed to the user does not distract him or her from operating the product in a safe manner.

Security and safety are clearly distinct issues, even if (cyber)security has a clear impact on a product's safety. The manufacturer not only has a duty to secure the product from

unauthorised access (ie security), but must also ensure that the user and potential authorised third parties access the data a safe way, that is to say, in a way that does not endanger the product and its users (ie safety). ACEA believes that this safety requirement is paramount and should be included in the provisions of Article 3(1).

PROTECTING COMPETITIVENESS AND INNOVATION

Managing user access to data

The proposal requires that the data holder should make available to the user free of charge the data generated by the use of a product or related service (Article 4(1)).

The proposal defines a 'user' as a natural or legal person that owns, rents or leases a product, or receives a service (Article 2(5)).

Commercial use of data generated by products

ACEA believes that it is legitimate to expect that a consumer is able to access free of charge the data generated by the private use of the product that they have purchased, rented or leased. However, based on these provisions, companies that use products for commercial purposes will also be entitled to request that the data holder makes available the data generated by the use of these products free of charge, which they will then be entitled to use for their commercial activities.

As explained above, data holders incur substantial operational costs from collecting, storing, managing and disseminating via electronic means data generated by products. Furthermore, the volume of data required by commercial companies is typically higher than for individual consumers. This will likely increase exponentially as the EU data economy continues to develop. Such costs may become unsustainable for individual manufacturers and will severely undermine the incentives to invest.

ACEA believes that it is legitimate to expect that companies intending to use data for commercial purposes bear some of the costs involved in the collection, storage and dissemination of this data.

Management of multiple users

Some products falling under the scope of the Data Act may be purchased by one user, only to be leased or rented to other users. Some of these products may even be leased or rented multiple times under short-term leases or rentals, leading to situations in which multiple users request data successively or even simultaneously. This is the case in the transport sector, where companies purchase a fleet of vehicles which they lease or rent repeatedly through short-term contracts, to which the data holder is not party.

In situations such as these, the data holder may be unable to keep track of which persons acquire the right to access the data generated by the use of the vehicle, and when these persons lose this right.

ACEA believes that companies that operate such businesses should be expected to manage access permissions for these users, and the relevant access rights to the data generated by their use of the product.

This possibility is touched upon by the proposal, as recital 25 states that the user should be given the necessary technical interface to manage permissions, preferably with granular permission options (including the option to withdraw permission). Nevertheless, this solution is not given effect in the provisions of the proposal and is rendered largely inoperative due to the definition of 'user' in Article 2.

ACEA therefore recommends that Article 2(5) be amended to define a user as any natural or legal person that owns the product, or that rents or leases a product or receives a service from the data holder.

This definition would establish a primary user who would, in turn, be responsible for managing permissions for subsequent users, and would direct the data holder to provide or withdraw access to the data generated by the use of the product to these subsequent users.

Protection of trade secrets

Regarding trade secrets, in relation to the user, the proposed Data Act states that "specific necessary measures" should be agreed between the data holder and the user to preserve the confidentiality of the shared data (Article 4(3)).

The proposal also states that trade secrets can only be disclosed to third parties when strictly necessary to fulfil the purpose agreed between the user and the third party. Here again, it refers to "specific necessary measures" to be agreed between the data holder and the third party (Article 5(8)).

ACEA does not believe that the Commission's proposal provides sufficient protection for trade secrets. Indeed, it does not provide any definition of the "specific necessary measures" expected to be agreed between the data holder and users or third parties, nor does it provide any indication as to how compliance will be monitored and enforced.

What is more, alarmingly, is that ? no indication is provided as to who should determine whether the disclosure of trade secrets is strictly necessary to fulfil the purpose agreed between the user and the third party. Should the user or the third party, or in fact any other party than the trade-secrets holder, be deemed competent to make this determination, it would represent a major threat to the protection of trade secrets afforded by the Trade Secrets Directive.[4]

Trade secrets are instruments specifically designed to enable their holder to exclude others from accessing confidential information. The protection of confidential business data and trade secrets is paramount to a well-functioning internal market. Therefore, the Data Act should not compromise trade secret protection.

[4] Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure.

To that end, ACEA recommends that the Data Act clarifies that the right to determine if the sharing of trade secrets is strictly necessary is granted exclusively to the trade-secrets holder. Furthermore, the nature, scope and extent of the measures agreed between the trade-secrets holder and the data recipient to protect trade secrets should be determined exclusively by the trade-secrets holder.

Protection of the data holder

The proposal states that the user should not use the data obtained from the manufacturer to develop a product that competes with the product from which the data originates (Article 4(4)). This prohibition also applies to third-party data recipients (Article 6(2)(e)).

ACEA welcomes this protection from a situation whereby the data generated by a product could be exploited by potential competitors to gain knowledge about a competing product, or to reverse engineer the product or its components, and develop competing products.

Nevertheless, ACEA is concerned by the inherent limitations of this protection. While the proposal states that the data obtained should not be used to develop a competing product, it fails to extend this to related services. A data recipient would therefore be able to use the data obtained from the product or related service to develop a competing related service.

ACEA therefore recommends that the provisions of Article 4(4) and Article 6(2)(e) be extended to include related services.

B2G DATA SHARING

'EXCEPTIONAL NEED' FOR PUBLIC SECTOR BODIES

The proposal obliges data holders to make data available to public sector bodies that demonstrate an exceptional need to use the requested data (Article 14(1)). It states that such exceptional needs may occur where:

- The data is necessary to respond to public emergencies (Article 15(a)), or to prevent such public emergencies ((Article 15(b))
- The lack of data prevents public sector bodies from carrying out a specific task in the public interest that has been explicitly provided by law (Article 15(c))

ACEA's members fully support the Commission's intention to stimulate the sharing of data which is necessary to prevent or resolve public emergencies affecting the EU population, such as health crises or natural disasters.

However, ACEA believes that the provisions of the proposal far exceed this objective. The provisions of Article 15 should target public emergencies that would have severe and durable repercussions on the EU and its citizens. Yet, the definition of 'public emergency' provided under Article 2(10) covers situations affecting an individual member state, or part of it, and provides for a set of alternative conditions. ACEA believes that this definition should be

amended so that it exclusively targets situations affecting the Union at large and provides for cumulative conditions.

Furthermore, the provisions of Article 15(c) require data holders to provide data upon request to public sector bodies, not in case of exceptional needs, but rather so that they can carry out their day-to-day duties under the law. This would provide a blank check for public sector bodies to request access to privately-held data, at cost (Article 20(2)), whenever it is less burdensome or costly for them than acquiring this data at market rates, or by relying on existing obligations under EU or national law (Article 15(c)(1)). This would be the case even where this data is covered by trade secrets (Article 19(2)).

In ACEA's view, these provisions are disproportionate to the objective served and are counterproductive to the Commission's objective of encouraging data sharing and fostering the EU data economy.

Habitual data needs of public bodies are best be served by the market. Introducing provisions that allow public bodies to bypass the market will create distortions and imbalances. Additionally, voluntary data sharing can play an important role to support authorities and is already successfully undertaken by vehicle manufacturers, for example regarding road safety.

In specific cases where the legislator has deemed it necessary to create obligations on private data holders to share data with public sector bodies for specific purposes (eg law enforcement), these bodies can rely on existing obligations laid down in current legislation to access privately held data.

The provisions of the Data Act should be limited to enacting a special derogation for public sector bodies facing public emergencies. Such exceptional circumstances justify this exceptional measure. It should also be considered that data sharing in this context will come at cost for the data holder. If emergency situations, such as a global pandemic, are sustained over several months or years, public bodies should at least consider covering some of the costs incurred by sharing data with them.

Additionally, data holders have an interest in ensuring the protection and confidentiality of the data they hold. Hence, it must be ensured that the data is protected against access by unauthorised third parties or cyber-attacks. It is therefore essential to ensure that appropriate technical and organisational measures (TOMs) are adopted by public sector bodies to ensure the confidentiality and integrity of the data shared by private entities.

In any case, trade secrets should only be disclosed when the data holder agrees to it, and when all specific measures agreed between the data holder and the public sector body are taken by the latter to preserve the confidentiality of the trade secrets.

RE-USE OF DATA SHARED FOR EXCEPTIONAL NEEDS

The proposal states that public sector bodies that are a recipient of data under Article 14 of the Regulation are entitled to share that data with third parties in view of carrying out scientific research or analytics, or to national statistics bodies and Eurostat.

ACEA agrees that it may be necessary to share data gathered to prevent or respond to a public emergency with entities carrying out scientific research. ACEA notes, in that respect, that some guarantees have been laid down in the proposal to ensure that privately-held data acquired by public sector bodies could only be shared where it serves the purpose for which the data was requested, ie to face a public emergency, and with entities acting on a non-for-profit basis.

Nevertheless, ACEA believes that these limited guarantees fall short of offering the legal protection and certainty that private stakeholders who share data to serve the public interest should be afforded. Data shared with a public sector body under Article 14 should not be passed on without the prior agreement of the data holder.

At a minimum, the data holder should be provided with detailed information regarding the identity of the recipient(s) of the data, as well as the activities which will be carried out by this entity. In that regard, the notification provided for under Article 21(4) appears insufficient.

In any case, here again, additional protection should be afforded to trade secrets shared by the data holder. Trade secrets should only be passed on with the agreement of the data holder, and where all specific measures agreed between the data holder and the public sector body are taken by the third party to preserve the confidentiality of trade secrets.

INTERNATIONAL DATA TRANSFERS

LEGAL CERTAINTY FOR DATA-PROCESSING SERVICES

The Commission's proposal establishes requirements for data-processing service providers to handle requests for access to non-personal data held in the EU from authorities in non-EU countries (Article 27).

ACEA salutes the legal certainty provided in Article 27(2) which lays down rules for international data transfers. This Article clarifies that data-processing service providers are not expected to share data based on a judgement or an administrative decision issued by a third country, unless it is based on an international agreement in force between the third country and the EU or a member state. ACEA believes that these limitations provide clear and actionable guidance to data-processing service providers.

For this reason, ACEA regrets that the legal certainty provided by Article 27(2) is negated by the provisions of paragraph 3. This paragraph contradicts paragraph 2 by allowing data sharing with a third country where no international agreement exists between the third country and the EU or one of its member states. It then lays down several very broad criteria based on which a data-processing service provider is expected to assess the legality of the judgement or decision and to assess the third country's legal system prior to sharing the relevant data with the third-country authority.

ACEA considers that the assessment process provided under Article 27(3) is unworkable. A private entity cannot reasonably be expected to carry out what effectively amounts to a

judicial review of a judgment or decision, and an assessment of the procedural law and legal system of a third country, every time it is faced with a data-access request.

ACEA understands that these data-processing service providers will be entitled to ask the opinion of relevant competent authorities and may rely on guidelines from the Commission to determine whether the conditions referred to in Article 27(3) are met. Nevertheless, in the absence of such guidelines, these entities may only rely on the opinion of national competent authorities, which may vary from one member state to another. Furthermore, as these opinions are non-binding, the burden of deciding whether to share data with a third country remains squarely with the data-sharing service provider. The legal burden imposed on such an entity, especially if it is a micro-, small or medium enterprise, is simply untenable.

ACEA believes that the provisions of Article 27(3) should be deleted. Alternatively, Article 27(3) should be amended to state that the assessment will be performed by a competent authority upon notification of a data-access request by a third country from a data-sharing service provider. It should also clarify that the subsequent decision of this competent authority would be binding on the data-sharing service provider. This would preserve the spirit and intent of this provision, while removing the burden of performing the assessment – and of shouldering the consequence of the decision – from data-sharing service providers.

SUI GENERIS RIGHT

The proposal provides that the *sui generis* right provided for in Article 7 of the Database Directive[5] does not apply to databases containing data obtained from or generated by the use of a product or a related service (Article 35).

ACEA is concerned over this exception to the *sui generis* right created by the Database Directive, and the consequences that such an exception may entail for the protection of the intellectual property rights covered under this legislation.

As stated under this directive, the making of databases requires the investment of considerable human, technical and financial resources, while such databases can be copied or accessed at a fraction of the cost needed to design them independently. Databases are a vital tool in the development of an information market within the EU.

ACEA therefore believes that it is essential not to hinder the exercise of the rights provided to users under the Data Act. Nevertheless, further reflection and discussion should be carried out on how these rights can be ensured without jeopardising the intellectual property rights protected under the Database Directive.

ENTRY INTO FORCE / APPLICATION

The proposal states that the Data Act will apply 12 months after the date of its entry into force (Article 42).

[5] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases

As explained above, ACEA believes that some of the provisions of this proposal go too far by imposing requirements that are simply unworkable, and which manufacturers and data holders would struggle to implement – regardless of the lead-time afforded to them. The ACEA recommendations in this position paper would help clarify this legislation to ensure that the principles it lays down are served by clear and workable requirements.

However – even if ACEA's recommendations are followed – we still consider that the requirements of this regulation are extensive and far-reaching, requiring businesses to implement complex and costly processes to ensure compliance. As was provided under the General Data Protection Regulation, ACEA therefore believes that additional lead-time should be granted to companies to ensure compliance.[6] The Data Act should therefore apply 36 months after its date of entry into force.

[6] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Article 99.

ABOUT THE EU AUTOMOBILE INDUSTRY

- 12.7 million Europeans work in the auto industry (directly and indirectly), accounting for 6.6% of all EU jobs
- 11.5% of EU manufacturing jobs – some 3.5 million – are in the automotive sector
- Motor vehicles are responsible for €398.4 billion of tax revenue for governments across key European markets
- The automobile industry generates a trade surplus of €76.3 billion for the European Union
- The turnover generated by the auto industry represents more than 8% of the EU's GDP
- Investing €58.8 billion in R&D per year, automotive is Europe's largest private contributor to innovation, accounting for 32% of the EU total

ACEA REPRESENTS EUROPE'S 16 MAJOR CAR, VAN, TRUCK AND BUS MANUFACTURERS

ACEA
European Automobile
Manufacturers' Association
+32 2 732 55 50
info@acea.auto
www.acea.auto

twitter.com/ACEA_auto

linkedin.com/company/acea

youtube.com/c/ACEAauto