DIGITALEUROPE

24 AUGUST 2023

DIGITALEUROPE Access to In-Vehicle Data Position Paper

This paper should be read as a supplement to DIGITALEUROPE's position paper on the proposed Data Act (see here).

Introduction

DIGITALEUROPE proposes important guidance, as the European Commission is currently weighing up the timing and scope of potential new automotive sector-specific requirements/standards for data-sharing under the umbrella of the proposed Data Act.

We acknowledge, as does the European Commission, the valuable role of data driven innovation for the automotive sector in Europe. Today we are seeing increased efficiencies from automation in manufacturing and AI-powered processes. This trend will deliver continued benefits for sustainability, competitiveness, innovation and resilience. This translates into less waste, greenhouse gas emissions and energy consumption, while at the same time ensuring more jobs and growth for enterprises operation in Europe: the EU stands to maintain its leadership in the global market.

In-vehicle generated data and its associated architecture are the results of years and billions of euros of research and development. Manufacturers and suppliers in the value chain have invested heavily in the development of devices generating in-vehicle data and other services in order to be able to monetise these, develop new products or services, and improve the customer experience. Disclosure of data and even the data management architecture may result in disclosing trade secrets, give an unfair advantage to competitors who have not made corresponding investments, and disrupt nascent business models. Legislation requiring data holders to provide access to the fruits of their own innovation to third-party actors should be done with caution and full assessments of the economic impacts, in addition to the impacts on safety.

DIGITALEUROPE
Rue de la Science, 14A, B-1040 Brussels
T.+32 (0) 2 609 53 10 / www.digitaleurope.org / @DIGITALEUROPE
EU Transparency Register: 64270747023-20

Given the Data Act's wide-ranging horizontal provisions and the findings from the Access to In-Vehicle Data, Functions and Resources Impact Assessment, we recognise that such provisions will have a major impact on the automotive ecosystem and that more specific provisions may be needed, noting that legislative mandates and weak language guarding IP rights will undermine future progress for Europe.

Due to the expected impact on the automotive sector, we offer the following policy recommendations:

1. Key definitions need to be narrowed down to avoid imposing blanket obligations on businesses in the automotive sector

- When applied to the automotive sector, central definitions within the draft Data Act would need to be made more specific and focused during the drafting process of the sectoral proposal, in order to better describe the complexities of the automotive sector. These include "data holder"; "user" and "related services", which in their current formulation run the risk of significant misinterpretation.
- In devising a sectoral regulation, we urge the Commission to remove any ambiguity of what is intended to be captured under the new sectoral rules. For instance, where applicable, specifying that "data holder" when applied to automotive refers to an original equipment manufacturer selling vehicles; or that a "user" refers to an everyday consumer driving their own vehicle for personal or business use.
- Implementing data access functionalities, especially for systems not intended to collect user data, is technically challenging, would create risks of privacy breaches or cybersecurity issues and would increase design, manufacturing and operation costs. Systems not intended to collect user data, which utilise user data for application (e.g., User position for a navigation application), when the user data is not stored but deleted after a reasonable obsolescence delay (e.g., a few minutes in the case of a navigation app), should be excluded from the regulation. A more detailed description and more focused definition of user Data is necessary to keep only systems aiming at collecting user data, beyond the scope of service or application provisioning in the scope of the regulation.

2. Trade secrets, intellectual property and existing contractual arrangements as well as cybersecurity and user privacy must be protected

- Any automotive sector-specific requirements must include a clear description of the data in scope to prevent data misuse and anti-competitive behaviour.
- This must include a clear recognition of trade secrets, protections against the development of competing products and an acknowledgement of the need for data holders and recipients to agree suitable contractual and compensation terms.
- Any provision regarding data sharing in the automotive sector should not only grant the data holder the right to oppose data sharing requests in specific circumstances, when the data holder can demonstrate that it is likely to suffer damage from an acquisition, disclosure or use the disclosure of trade secrets, or due to cybersecurity, health, security and privacy risk, but also ensure compensation for costs tied to data sharing, data management, and third-party software integration and validation.
    - Example: A battery-management start-up that is promising users' insights in their EV battery performance is owned by a competing car manufacturer. The battery-management start-up is requesting access to all data points generated in the car, claiming that all data points are needed to significantly increase the range of EVs. Such data disclosure could be used by the competing car manufacturer to gain a competitive advantage against the rest of the industry.
- Any provisions should also allow the manufacturer to manage and verify any data or other third-party access in accordance with several conditions. These include situations where such access could potentially affect user safety or privacy, scenarios where it could influence the vehicle's safety parameters or driving behaviour, and circumstances where access could have potential repercussions on the vehicle's security, whether in a cyber or physical context. Access to functions or resources should only be granted if deemed feasible and safe by the manufacturer of the product in question.
    - Example: Rent-a-car companies require access to remotely close the windows of cars when the user returned the car but forgot to close the windows. If an unconditional access is granted for the functioning of the windows, there is a possibility that a driver's hand gets injured by forceful window closing.

- Example: unauthorised or malicious access to charging data can reveal patterns indicating when someone is typically at home, the office, or another private location. Such insights risk not only invading personal privacy but may also facilitate criminal activities against property or individuals (burglary, motor vehicle theft, robbery, etc).

- The level of access should be adjusted according to its intended use. Some data points should only be readable, meaning that values can be retrieved from the vehicle, but not modified. Others might need to be writable, allowing for updates to configurable elements, or functions that could be activated. Importantly, some data points should be entirely off-limits to third parties for security (including cybersecurity) and vehicle safety reasons. It is important that any matrix of data point accessibility considers the authorisation level of the user; each data point should be evaluated individually to determine whether it requires "read" or "write" access, or both. This approach ensures that data is managed in a more secure and efficient manner, reducing the risk of unauthorised access or manipulation.

  - Example: The number of kilometres driven should be an access-only data point so that users and repair shops are aware of the real usage of the car and maintain it properly. On the other hand, data on favourite radio stations can be a writable data point for the user.

3. Duplication of data-sharing requirements that are already in place under EU law must be avoided

- The Data Act generally presupposes that data reporting requirements either do not exist or are not in development for different sectors.

- For the purposes of ensuring coherence and legal certainty, the upcoming proposal should explicitly state its precedence over the Data Act in instances of conflicting stipulations.

- The Access to In-Vehicle Data Impact Assessment makes mention to reporting obligations for manufacturers to “inform competent authorities…about the implementation of access rights”. The Commission must ensure that any such reporting obligations do not conflict with or undermine the efficacy of similar obligations already set out for the automotive sector such as those under the Market Surveillance Regulation (EU) 2018/858 and General Safety Regulation (EU) 2019/2144 those stemming from it: e.g., Automated Lane Keeping Systems (under UN Regulation 157)[1], Emergency Lane Keeping

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:42021X0389&qid=1677520993037&from=EN

Systems Regulation (EU) 2019/2144[2], Intelligent Speed Assistance Regulation (EU) 2021/1958[3] and the recently-adopted ADS Type Approval Regulation (EU) 2022/1426[4].

4. Feasibility of a common technological approach to data sharing

- The proposed Data Act's interoperability requirements envision large-scale harmonisation of functionalities of data processing services being used by all parties. This is not only concerning but infeasible when applied to already-regulated motor vehicles, motor vehicle equipment, and related products and services within the automotive sector like logistics, EU-wide trucking and others.
- We urge the Commission to consider the cost impacts of an industry-wide technological approach, especially in light of ongoing discussions about how to implement a European Mobility Data Space.
- To achieve the best results for consumers and all stakeholders involved, the data and software solutions, and the ecosystems they are based on should all be motivated to innovate and compete with each other. Prescriptive requirements on implementation limit the available solution space and should thus not be included in the upcoming proposal. Due to the varying solutions of different manufacturers, they should be allowed to deem the appropriate mode of granting access to any vehicle functions.

Conclusion

We support the Commission's ambition to continue fostering an innovative and competitive data driven automotive sector in Europe. A sensible proposal on the access of in-vehicle data, functions and resources can help apply the principles of the Data Act to the automotive sector. Not doing so could disincentivise innovation and pose risks to the safety and security of vehicles, user privacy and cybersecurity. This proposal should guarantee that innovators, which have invested heavily in developing systems able to generate data in order to monetise them, develop new products or services, and improve customer experience, are able to benefit from their investments in the EU, and not required to compromise on the most important characteristic of a motor vehicle: safety.

---

[2] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32021R0646&from=EN

[3] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32021R1958&qid=1677520993037&from=EN

[4] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R1426&qid=1677521780909

FOR MORE INFORMATION, PLEASE CONTACT:

João Tato Marinho

Associate Director for Digital & Green Transformation Policy

joao.marinho@digitaleurope.org / +32 491 56 11 24

Ray Pinto

Senior Director for Digital Transformation Policy

ray.pinto@digitaleurope.org / +32 472 55 84 02

About DIGITALEUROPE

DIGITALEUROPE is the leading trade association representing digitally transforming industries in Europe. We stand for a regulatory environment that enables European businesses and citizens to prosper from digital technologies. We wish Europe to grow, attract, and sustain the world's best digital talents and technology companies. Together with our members, we shape the industry policy positions on all relevant legislative matters and contribute to the development and implementation of relevant EU policies, as well as international policies that have an impact on Europe's digital economy. Our membership represents over 45,000 businesses who operate and invest in Europe. It includes 102 corporations which are global leaders in their field of activity, as well as 41 national trade associations from across Europe.

DIGITALEUROPE Membership

Corporate Members

Accenture, Airbus, Applied Materials, Amazon, AMD, Apple, Arçelik, Arm, Assent, Autodesk, Avery Dennison, Banco Santander, Bayer, Bosch, Bose, Bristol-Myers Squibb, Brother, Canon, CaixaBank, Cisco, CyberArk, Danfoss, Dassault Systèmes, DATEV, Dell, Eaton, Epson, Ericsson, ESET, EY, Fujitsu, GlaxoSmithKline, Google, Graphcore, Hewlett Packard Enterprise, Hitachi, Honeywell, HP Inc., Huawei, ING, Intel, Johnson & Johnson, Johnson Controls International, Konica Minolta, Kry, Kyocera, Lenovo, Lexmark, LG Electronics, Mastercard, Meta, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe, NEC, Nemetschek, NetApp, Nintendo, Nokia, Nvidia Ltd., Oki, OPPO, Oracle, Palo Alto Networks, Panasonic Europe, Pearson, Philips, Pioneer, Qualcomm, Red Hat, RELX, ResMed, Ricoh, Roche, Rockwell Automation, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Siemens Healthineers, Skillsoft, Sky CP, Sony, Sopra Steria, Swatch Group, Technicolor, Texas Instruments, TikTok, Toshiba, TP Vision, UnitedHealth Group, Visa, Vivo, VMware, Waymo, Workday, Xerox, Xiaomi, Zoom.

National Trade Associations

Austria: IOÖ
Belgium: AGORIA
Croatia: Croatian Chamber of Economy
Cyprus: CITEA
Czech Republic: AAVIT
Denmark: DI Digital, IT BRANCHEN, Dansk Erhverv
Estonia: ITL
Finland: TIF
France: AFNUM, SECIMAVI, numeum
Germany: bitkom, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: Technology Ireland
Italy: Anitec-Assinform
Lithuania: Infobalt
Luxembourg: APSI
Moldova: ATIC
Netherlands: NLdigital, FIAR
Norway: Abelia
Poland: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Romania: ANIS
Slovakia: ITAS
Slovenia: ICT Association of Slovenia at CCIS
Spain: Adigital, AMETIC
Sweden: TechSverige, Teknikföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
Ukraine: IT Ukraine
United Kingdom: techUK