DIGITALEUROPE

4 MAY 2020

Response to EDPB draft Guidelines on connected vehicles and mobility-related applications

Introduction

Connected vehicles and mobility-as-a service solutions are key to Europe's digital transformation, where the increased safety, ease and efficiency of mobility can contribute towards a safer and greener society. A correct application of the General Data Protection Regulation (GDPR) and of the ePrivacy framework are necessary to this end.

DIGITALEUROPE is therefore pleased to submit its comments to the European Data Protection Board's (EDPB) draft Guidelines 1/2020 on the processing of personal data in the context of connected vehicles and mobility-related applications.

The draft Guidelines contain appropriate reference to best practice on privacy-by-design and data protection impact assessments (DPIAs), appropriate exemptions and using interfaces and applications on devices to manage car drivers' preferences.

However, we find that in many parts the draft Guidelines do not expand beyond the key GDPR concepts, which are not sufficiently contextualised if not in the final section on use cases.

In our response, we highlight elements of the draft Guidelines that we believe to be of particular importance. We hope our observations will be useful for an improved final version of the Guidelines.

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

Table of contents

Scope

We agree with the EDPB's focus on personal data processing in relation to the non-professional use of connected vehicles by data subjects. This being said, we believe the final Guidelines could be improved by more explicitly confirming in paras 19 and 30 the professional use cases that are out of scope.

On the other hand, we find that some key use cases that apply to connected cars, particularly with regard to maintenance, safety and vehicle control, are not duly considered in the draft Guidelines. Such use cases will be widespread and issues such as the use of location data or the relationship between local and cloud processing will be central. Similarly, 'ownership takeover management' functions will require the processing of legal identification documents, vehicle registration licences, biometric (e.g. selfie to be compared with ID card) and other data for the purpose of preventing motor vehicle theft.

Privacy by design and anonymisation

In setting out a range of practices to help mitigate risks to rights and freedoms of individuals, the draft Guidelines explicitly recognise the importance of both anonymisation and pseudonymisation.[1] However, the draft Guidelines fail to properly reflect the role of these techniques.

The draft Guidelines state that data from connected vehicles will most certainly be personal data and assume it will always be possible or desirable to link such data to a driver or passenger.[2] However, not all processing of vehicle data will be interested in, or even capable of, identifying individuals and this position fails to recognise a wide range of such scenarios.

The final Guidelines should more clearly elaborate on the fact that for data to be considered personal, thought should be given to 'all means reasonably likely to be used' to identify an individual[3] and recognise scenarios whereby a service provider will not be able to identify an individual from the data received.[4]

It is not sufficient for data to be theoretically traceable to an individual for it to be considered personal. Rather, this determination should centre around the reasonable likelihood that identification will be possible, which should take into

[1] Section 2.4.2 of the draft Guidelines.

[2] See notably paras 3 and 59, ibid.

[3] Case C-582/14: Patrick Breyer v Bundesrepublik Deutschland and GDPR Recital 26 states that the test for whether a person is identifiable depends upon 'all means reasonably likely to be used' to identify the person i.e. a test of likelihood, not just a hypothetical possibility.

[4] Art. 11 GDPR.

account the cost and time required for identification by those who are reasonably likely to access and use the information at hand.[5]

It is in theory not to be excluded, for instance, that braking patterns could be so specific to an individual that technical brake data could be traced back. However, identification will be extremely difficult and therefore unlikely, particularly in situations where precise location, device or online identifiers are not being processed.

In particular, technical data can fruitfully be anonymised or indeed be anonymous from the start. Such data can include, for instance, performance statistics relating to a car's braking system, where any identifying pieces of information either are not collected in the first place or are stripped out immediately after collection, ensuring that only the non-personal bits are processed. This also applies to other examples provided in the draft Guidelines such as engine temperature or tyre pressure.

Similarly, in the context of location data and alerts emitted from devices installed in connected vehicles, anonymisation plays a key role in protecting users. Anonymisation can be achieved through various techniques that remove single vehicle identifiers and full journey details. These techniques provide effective safeguards to prevent identification and/or surveillance of individuals as well as potential misuse of data.

Relationship with ePrivacy and legal grounds for processing

The draft Guidelines are the most direct articulation to date of the relationship between the GDPR and the ePrivacy Directive[6] in Internet of Things (IoT) scenarios. While such relationship had already been explored in previous opinions from both the Article 29 Working Party (WP29) and the EDPB,[7] the draft Guidelines are clearer as to the EDPB's interpretation and its impact in real terms.

In essence, the draft Guidelines argue that it is ePrivacy that will provide the legal bases applicable to the processing of connected vehicle data given the applicability of Art. 5(3) of the ePrivacy Directive to terminal equipment, whose definition covers connected vehicles.

---

[5] Recital 26 GDPR.

[6] Directive 2002/58/EC as modified by Directive 2009/136/EC.

[7] See notably the WP29 Opinion 8/2014 on Recent Developments on the Internet of Things and the EDPB Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR.

Any residual application of the legal bases under the GDPR will be limited to consent and contractual necessity, which merely confirm the legal bases already authorised by the ePrivacy Directive as the general consent rule and its two exemptions.[8] Similarly, any further processing on the basis of Art. 6(4) GDPR will be forbidden.[9]

To be even more specific, what this means is that for any practical purposes, rather than complementing, ePrivacy *supplants* the GDPR when it comes to the legal bases for processing terminal equipment data.

We would like to stress how such combined interpretation, if confirmed under the text currently being discussed for an ePrivacy Regulation,[10] would *de facto* exclude reliance on the GDPR for use cases where the impact on individuals' privacy would be minimal or non-existent such as the use of anonymous data that we have highlighted in the previous section.

We urge policymakers to carefully consider the implications of this approach for Europe's competitiveness in the development and deployment of beneficial, non-invasive IoT and artificial intelligence (AI) applications in the mobility sector. An overreliance on consent, combined with a restrictive interpretation of contractual necessity, will make data processing in these scenarios exceedingly difficult or impossible – what is worse, with no benefits for data subjects.[11]

The draft Guidelines themselves recognise there may be inherent difficulties in obtaining consent and providing notice to drivers of connected vehicles,[12] without offering any real solutions or guidance on how to address these difficulties.

Recognising that in some scenarios provision of notice may be impossible or disproportionate as outlined in Art. 14(5)(b) GDPR, for example because a service provider has no direct relationship with the driver of a connected vehicle, suggestions of alternative approaches would be highly beneficial.

---

[8] See para. 17 of the draft Guidelines, which refers to the two exemptions to the consent rule established by Art. 5(3) of the Privacy Directive. Both exemptions – transmission and provision of an information society service – coincide with the contract legal basis under Art. 6(1)(b) GDPR.

[9] See Section 1.5.3 of the draft Guidelines.

[10] COM(2017) 10 final.

[11] See also pp. 7-8 of our position paper *Almost two years of GDPR: celebrating and improving the application of Europe's data protection framework*, available at https://www.digitaleurope.org/wp/wp-content/uploads/2020/01/Position-paper-on-GDPR-review.pdf. Our consolidated position on the proposal for an ePrivacy Regulation is available at https://www.digitaleurope.org/wp/wp-content/uploads/2019/01/DIGITALEUROPE%E2%80%99s%20consolidated%20position%20on%20ePrivacy%20Regulation.pdf

[12] Para. 48 of the draft Guidelines.

Similarly, the final Guidelines should provide more practical guidance on how to apply alternative legal bases under the GDPR (and potentially the future ePrivacy Regulation) such as contract and legitimate interest.

Local processing

The draft Guidelines stress the importance of local processing, for example in relation to biometric templates. Correctly, the draft Guidelines find that such local processing falls outside the scope of the GDPR altogether.

However, contrary to the draft Guidelines, such local processing is not subject to the GDPR not so much because it falls under the household exemption[13] but because no controller or processor is *actually processing* the data at hand.

From this perspective, we are puzzled by para. 73 of the draft Guidelines, which states that the GDPR in such cases anyway 'does apply to controllers or processors, which provide the means for processing personal data for such personal or household activities (car manufacturers, service provider, etc.).' The examples provided in Recital 18 GDPR, which this paragraph of the draft Guidelines is modelled after, all imply an actual processing activity performed by a 'natural or legal person, public authority, agency or other body,' which the local device itself clearly isn't. This being said, the reference to Recital 78 GDPR, in the part relating to producers, is correct.

Similarly, we believe the last use case on rental car dashboards[14] should consider that any data processing in this context happens locally in the car. To the extent that the rental company – or, for that matter, any other entity – does not process such data, it cannot be regarded as a data controller or processor. Again, this does not eliminate the need for them as well as producers to take into account data protection when developing and designing their products, services and applications.

Criminal offences

Section 2.1.3 of the draft Guidelines classifies as personal data relating to criminal convictions and offences – for which the draft Guidelines coin the expression 'offence-related data,' which is not found in the GDPR – any data from which infractions can *in theory* be inferred. This, however, is not justified by Art. 10 GDPR, where this category of data refers explicitly to the criminal convictions and offences themselves or the related security measures. The mere processing of speed and location data does not amount to the processing of data

[13] Para. 71, ibid.

[14] Section 3.5, ibid.

about a conviction or offence, unless it is linked to the existence of such conviction or offense as registered by competent authorities.

As such, we find no basis for the draft Guidelines' assertion that 'external processing of data revealing criminal offences or other infractions [i.e. from which such offences could *only in theory* be inferred] is forbidden.' If such interpretation were to be followed, processing of basic data, such as an IP address, that may in theory be linked to criminal activity would not be authorised.

In-vehicle Wi-Fi

The draft Guidelines describe in-vehicle Wi-Fi connectivity provided by 'road professionals,' such as taxi drivers or companies, as an internet access service.[15] This is incorrect. The taxi driver or company merely provides access to a communications network provided by a telecoms operator and is to be considered as the provider of an information society service, not of the underlying internet access service.[16]

The draft Guidelines also find that the household exemption is not applicable in cases where an individual allows other passengers to connect to the in-vehicle Wi-Fi network. In addition to being perplexed by this extremely limited interpretation of the household exemption, which makes ordinary people data controllers,[17] we find the reference to the exemption misleading: a vehicle's driver or owner will themselves as a rule not be processing any data relating to such Wi-Fi connection – let alone determining the purposes and means of such processing – and hence they cannot be considered a controller in the first place.

Cars and the surrounding environment

Contrary to the draft Guidelines, we submit that cars are not a totally private area where people can act 'without encountering any external interferences.' Cars are a means of transport that on the contrary must necessarily interact with the surrounding environment – other vehicles, pedestrians and infrastructure (respecting traffic lights, road signs, etc.) – and constantly react to it.

---

[15] Para. 98, ibid.

[16] See notably Case C-484/14.

[17] On the household exemption, see pp. 3-4 of our response to the EDPB consultation on video devices, available at https://www.digitaleurope.org/wp/wp-content/uploads/2019/09/DIGITALEUROPE-response-to-EDPB-consultation-on-video-devices.pdf.

From this perspective, digital services and connectivity do not fundamentally change the nature of transportation, but can provide useful tools to improve the safety, convenience and environmental footprint of mobility.

While data processing from connected cars also generates a corresponding need to protect the related personal data, as well as the security of the related non-personal data, it is wrong to assume that such protection starts from a situation where cars do not face interference from the outside world.

FOR MORE INFORMATION, PLEASE CONTACT:

Alberto Di Felice

Director for Infrastructure, Privacy and Security

alberto.difelice@digitaleurope.org / +32 471 99 34 25

Martin Bell

Privacy and Security Policy Officer

martin.bell@digitaleurope.org / +32 492 58 12 80

About DIGITALEUROPE

DIGITALEUROPE represents the digital technology industry in Europe. Our members include some of the world's largest IT, telecoms and consumer electronics companies and national associations from every part of Europe. DIGITALEUROPE wants European businesses and citizens to benefit fully from digital technologies and for Europe to grow, attract and sustain the world's best digital technology companies. DIGITALEUROPE ensures industry participation in the development and implementation of EU policies.

DIGITALEUROPE Membership

Corporate Members

Accenture, Airbus, Amazon, AMD, Apple, Arçelik, Bayer, Bosch, Bose, Bristol-Myers Squibb, Brother, Canon, Cisco, DATEV, Dell, Dropbox, Epson, Ericsson, Facebook, Fujitsu, Google, Graphcore, Hewlett Packard Enterprise, Hitachi, HP Inc., HSBC, Huawei, Intel, Johnson & Johnson, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, MasterCard, METRO, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe Inc., NEC, Nokia, Nvidia Ltd., Océ, Oki, Oracle, Palo Alto Networks, Panasonic Europe, Philips, Qualcomm, Red Hat, Ricoh Europe PLC, Rockwell Automation, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Siemens Healthineers, Sony, Swatch Group, Tata Consultancy Services, Technicolor, Texas Instruments, Toshiba, TP Vision, UnitedHealth Group, Visa, VMware, Xerox.

National Trade Associations

Austria: IOÖ
Belarus: INFOPARK
Belgium: AGORIA
Croatia: Croatian Chamber of Economy
Cyprus: CITEA
Denmark: DI Digital, IT BRANCHEN, Dansk Erhverv
Estonia: ITL
Finland: TIF
France: AFNUM, Syntec Numérique, Tech in France
Germany: BITKOM, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: Technology Ireland
Italy: Anitec-Assinform
Lithuania: INFOBALT
Luxembourg: APSI
Netherlands: NLdigital, FIAR
Norway: Abelia
Poland: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Romania: ANIS, APDETIC
Slovakia: ITAS
Slovenia: GZS
Spain: AMETIC
Sweden: Teknikföretagen, IT&Telekomföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
Ukraine: IT UKRAINE
United Kingdom: techUK