Volume 4, No. 6 | November–December 2021

The Journal of Robotics, Artificial Intelligence & Law

fastcase FULL COURT PRESS

RAIL
The Journal of Robotics, Artificial Intelligence & Law
Volume 4, No. 6 | November–December 2021

THE JOURNAL OF ROBOTICS, ARTIFICIAL INTELLIGENCE & LAW (ISSN 2575-5633 (print) /ISSN 2575-5617 (online) at $495.00 annually is published six times per year by Full Court Press, a Fastcase, Inc., imprint. For customer support, please contact Fastcase, Inc., 711 D St. NW, Suite 200, Washington, D.C. 20004, 202.999.4777 (phone), 202.521.3462 (fax), or email customer service at support@fastcase.com.

Publishing Staff
Publisher: Morgan Morrissette Wright
Journal Designer: Sharon D. Ray
Cover Art Design: Juan Bustamante

Cite this publication as:

The Journal of Robotics, Artificial Intelligence & Law (Fastcase)

A Full Court Press, Fastcase, Inc., Publication

Editorial Office

711 D St. NW, Suite 200, Washington, D.C. 20004
https://www.fastcase.com/

POSTMASTER: Send address changes to THE JOURNAL OF ROBOTICS, ARTIFICIAL INTELLIGENCE & LAW, 711 D St. NW, Suite 200, Washington, D.C. 20004.

Articles and Submissions

Direct editorial inquiries and send material for publication to:

Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway, #18R, Floral Park, NY 11005, smeyerowitz@meyerowitzcommunications.com, 631.291.5541.

Material for publication is welcomed—articles, decisions, or other items of interest to attorneys and law firms, in-house counsel, corporate compliance officers, government agencies and their counsel, senior business executives, scientists, engineers, and anyone interested in the law governing artificial intelligence and robotics. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the Editorial Content appearing in these volumes or reprint permission, please contact:

Morgan Morrissette Wright, Publisher, Full Court Press at mwright@fastcase.com or at 202.999.4878

For questions or Sales and Customer Service:

Customer Service
Available 8 a.m.–8 p.m. Eastern Time
866.773.2782 (phone)
support@fastcase.com (email)

Sales
202.999.4777 (phone)
sales@fastcase.com (email)
ISSN 2575-5633 (print)
ISSN 2575-5617 (online)

European Data Protection Board's Guidelines on Connected Vehicles: Key Takeaways

Alja Poler De Zwart*

A number of EU data protection authorities have in recent years published varied opinions on the processing of personal information by vehicle sensors, telematics boxes, and driving applications. The European Data Protection Board now has weighed in on the topic by adopting "Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications." The author of this article discusses the guidelines.

Vehicles are becoming more than just a means of transportation, and the focus of European data protection regulators is increasingly shifting toward the collection and use of personal information generated by smart vehicles. The latest models integrate sensors and connected on-board equipment to collect and record vast amounts of personal information, such as specific driving routes, locations visited, driving habits, and potentially even the driver's well-being. Biometrics (e.g., fingerprints) are also increasingly used for authentication and identification purposes. And when interfaced with mobile applications, a host of other information about the driver and passengers (e.g., their interest in music, video, sports, social media, and other related activities) can be collected by such smart vehicles.

A number of EU data protection authorities ("DPAs") have in recent years published varied opinions on the processing of personal information by vehicle sensors, telematics boxes, and driving applications (such as the German Federal Data Protection Commissioner[1] and France's CNIL[2]). The European Data Protection Board ("EDPB") now has weighed in on the topic by adopting "Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications"[3] (the "Guidelines"). Relevant stakeholders are advised to review and adjust their processing practices accordingly.

Robotics, Artificial Intelligence & Law / November–December 2021, Vol. 4, No. 6, pp. 459–466.

ISSN 2575-5633 (print) /ISSN 2575-5617 (online)

Takeaways for Relevant Stakeholders

Stakeholders using data generated by "Connected Vehicles," which are smart vehicles that are equipped with electronic control units ("ECUs"), will need to review their data collecting, processing, and sharing processes and procedures, and ensure compliance with the recommendations set out in the Guidelines and as summarized below. This will particularly include the following:

1. Determining whether your organization acts as a company responsible for the processing of personal information (i.e., whether your company is a "data controller") in the complex eco-system of various stakeholders;
2. Conducting Data Protection Impact Assessments ("DPIAs") as early as possible in the design process, even when this might not be legally required (as a matter of best practice);
3. Ensuring appropriate legal basis under the ePrivacy rules and the EU General Data Protection Regulation ("GDPR");
4. Integrating privacy by design and default into the Connected Vehicles' setup;
5. Providing appropriate notices to individuals, and considering best ways and technological solutions to bring them to the attention of the individuals using Connected Vehicles;
6. Ensuring local/in-vehicle processing of raw data as much as possible, and otherwise consider applying appropriate anonymization or pseudonymization techniques to raw data;
7. Implementing appropriate technical and organizational security measures; and
8. Considering additional measures when processing location, biometric, and other data that could potentially reveal criminal offenses or other infractions.

Scope of the Guidelines

The Guidelines focus on Connected Vehicles. The ECUs can be linked together via an in-vehicle network as well as connectivity facilities that allow sharing of information with other devices both inside and outside the vehicle. They can include mobile applications that might (1) connect to a vehicle's entertainment unit, or

(2) work as standalone applications that assist drivers or passengers (such as GPS navigation on smart phones). The EDPB does limit the scope of the Guidelines to mobile applications that are related to the driving environment. So other applications that suggest, for example, places of interest (such as restaurants or museums) are out of scope.

While the Guidelines do not cover employee-monitoring issues, they provide useful insights for various Connected Vehicles stakeholders on how to set up a system that is compliant with the GDPR and the ePrivacy rules. The wide spectrum of stakeholders that the Guidelines are directed toward, includes traditional actors of the automotive industry as well as emerging players from the digital industry. This includes but is not limited to vehicle manufacturers, equipment manufacturers, automotive suppliers, car repairers, automobile dealerships, vehicle service providers, fleet managers, motor insurance companies, entertainment providers, telecommunication operators, and road infrastructure managers.

Compliance with the ePrivacy Rules and the GDPR Is Required

The EDPB leaves no room for doubt whether Connected Vehicles generate personal information. It notes that most of the data collected and processed through Connected Vehicles can be linked to one or more identifiable individuals. This can include directly identifiable data (e.g., the driver's identity), as well as indirectly identifiable data. The latter may include, for example, the details of journeys made, the vehicle usage data (e.g., data relating to driving style or the distance covered), or the vehicle's technical data (e.g., data relating to the wear and tear on vehicle parts). Metadata (such as vehicle maintenance status) may also qualify as personal information.

A Connected Vehicle is furthermore considered to be "terminal equipment," just like any computer, smart phone, or smart TV. Compliance with Article 5(3) of the ePrivacy Directive is therefore required. Organizations wishing to store data in a vehicle, or access such data, will need to obtain prior user consent under the ePrivacy rules, unless an exception applies. Additionally, any processing of personal information must also have a legal basis under Article 6 GDPR in order to be lawful. The EDPB provides one example of

when user consent is not needed, that is, when "processing is necessary to provide GPS navigation services requested by the data subject when such services can be qualified as information society services."

Considering the above, the EDPB sets out a number of specific recommendations for organizations wishing to process personal information generated by Connected Vehicles. Many of the following key recommendations basically reiterate general obligations under the GDPR:

Data Controllership

While the EDPB does not consider in much detail which players in the Connected Vehicles eco-system are (jointly) responsible for the processing of personal information (data controllers), it does specifically call out as such:

- Service providers that send the driver traffic information, eco-driving messages, or alerts regarding the functioning of the vehicle;
- Insurance companies offering "Pay as You Drive" contracts; and
- Vehicle manufacturers gathering data on the vehicles' wear and tear to improve their quality.

Data Protection Impact Assessments

Connected vehicles will often result in high-risk processing; this will particularly be the case when data are processed outside the vehicle because of the potential sensitivity and scale of the data involved. Where this is the case, a DPIA will be required. The EDPB recommends that all responsible stakeholders conduct a DPIA as a best practice as early as possible in the design process, even where this would not be legally required.

Privacy by Design and Default

Connected Vehicle technologies need to be designed to minimize the collection of personal information, provide privacy-protective default settings, and ensure that individuals are well informed and have the option to easily modify their privacy settings.

Organizations should consider specific tools to allow effective exercise of individuals' rights and control over their personal information. In particular:

- A profile management system should be implemented inside the vehicle to store privacy preferences and assist individuals with changing their privacy settings at any time;
- The system should centralize all of the individual's privacy settings and preferences to facilitate individuals' rights requests;
- Individuals should be enabled to stop the collection of certain types of personal information, temporarily or permanently, at any moment, unless there is a specific legal ground justifying continuous collection of specific data. These features should be implemented inside the vehicle, although it could also be provided to individuals through other means, such as dedicated applications;
- In order to allow individuals to quickly and easily remove personal information stored on the car's dashboard (e.g., GPS navigation history, web browsing), manufacturers should provide simple deletion functionalities, such as a delete button; and
- The sale of a vehicle should trigger deletion of any personal information that is no longer necessary and the individual should be able to exercise his or her right to portability.

Transparency

Individuals need to be provided with a comprehensive GDPR-compliant notice that can be provided in layers. The first level should contain the most important information. The EDPB does not expand on what this information is, except to say that it should include information about data recipients (e.g., vehicle manufacturers or insurance providers).

Organizations can consider using (1) concise and easily understandable clauses in the vehicle's purchase or service contracts; (2) other written forms, distinct documents (e.g., the vehicle's manual) or an on-board computer; and/or (3) standardized icons that can potentially reduce the need for vast amounts of written information. The icons should be used to let the individuals know

when certain types of information (such as location) are being collected. The EDPB suggests a light coming on in the vehicle, or moving arrows on relevant screens.

In-Vehicle Processing

Organizations should consider processing raw data inside the vehicle—thus not transferring it to vehicle manufacturers or insurers. This includes individuals having direct access to the data generated by their vehicles and any associated applications, and being enabled to permanently delete any personal information before their vehicles are put up for sale.

Organizations should also consider "hybrid processing." The EDPB suggests, for example, that insurance companies should not have access to raw driving data. The data should instead be processed in the vehicle (or by a third-party service provider) to generate a "score," which is then shared with insurance companies.

If it is necessary to transfer data outside the vehicle, organizations should instead consider anonymizing or pseudonymizing the data first. When anonymizing, the responsible party (data controller) should take into account all processing involved that could potentially lead to re-identification of data, such as the transmission of locally anonymized data.

Security

Given that risks to security can endanger the lives of the driver of a vehicle and any number of other individuals, organizations need to consider a number of security measures:

- Various forms of encryption (including encrypting communication channels, putting in place an encryption key management system and adequately protecting and updating such keys);
- Ensuring data integrity (e.g., by hashing);
- Making access to personal information contingent on reliable user authentication methods (e.g., passwords or electronic certificates);
- Keeping vehicles' vital functions separate from non-vital functions (e.g., "infotainment" systems);

- Implementing technical measures that will allow vehicle manufacturers to rapidly patch security vulnerabilities during the entire lifespan of the vehicle;
- Setting up an alarm system in case of an attack on the vehicle systems; and
- Storing of a log history of any access to the vehicle's information system, so that attacks or other potential anomalies can be detected.

Data Requiring Special Attention

The EDPB points out that the following three categories of personal information warrant special attention because of their potential sensitivity:

- *Location*: Organizations are advised to:
  1. Not activate location processing by default;
  2. Point out to individuals that location has been activated by using icons (e.g., arrows that moves across the screen);
  3. Provide options to deactivate location at any time; and
  4. Define limited storage period for location data.
- *Biometrics*: Organizations should:
  1. Provide for non-biometric alternatives (e.g., physical keys or codes to unlock a car);
  2. Store the biometric templates/models in the vehicle, in an encrypted form (using a cryptographic algorithm and key management that comply with the state of the art);
  3. Process raw data (used to make up the biometric template and user authentication) in real time without ever being stored (not even locally);
  4. Limit the number of authentication attempts; and
  5. Adjust the biometric solution use (e.g., the rate of false positives/false negatives) according to the security level of the relevant access control.
- *Data revealing criminal offenses or other infractions*: The EDPB notes that some categories of personal information from connected vehicles could reveal that a criminal offence or other infraction has been (or is being) committed (e.g., data indicating that the vehicle crossed a white line or the instantaneous speed of a vehicle combined with precise

location data). When processing data revealing criminal offenses or other infractions, organizations should consider resorting to local processing whereby individuals have full control over the processing in question, and use robust security measures to ensure that there is sufficient protection against illegitimate access, modification and deletion of the data in question. Such processing should also be fully compliant with Article 10 GDPR.

Notes

* Alja Poler De Zwart is a partner at Morrison & Foerster (International) LLP, representing clients in privacy, data security, and e-commerce matters. She may be reached at apolerdezwart@mofo.com.

1. https://www.bfdi.bund.de/SharedDocs/Publikationen/Faltblaetter/VernetzteFahrzeuge.pdf.

2. https://www.cnil.fr/en/connected-vehicles-compliance-package-responsible-use-data.

3. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012020-processing-personal-data-context-connected_en.