

Data protection and privacy of the car ... as a mobile device

EDPS



EUROPEAN DATA PROTECTION SUPERVISOR

29/11/2018, Brussels

Wojciech R. Wiewiórowski

European Data Protection Assistant Supervisor

Type-approval requirements for motor vehicles as regards their general safety and the protection of vehicle occupants and vulnerable road users

The role of European Data Protection Supervisor

- The **European Data Protection Supervisor (EDPS)** is the independent supervisory authority for the processing of personal data by the EU administration;
- **Privacy and data protection are fundamental rights** – see Articles 7 and 8 of the Charter of Fundamental Rights;
- **Independent supervision** is an integral part of the right to data protection – see Article 16(2) TFEU and 8(3) Charter;
- What we do:
 - monitoring and verifying compliance with Regulation (EU) 2018/1725,
 - giving advice to controllers,
 - advising the co-legislators on new legislation,
 - cooperating with Member States' DPAs,
 - handling complaints, conducting inspections
 - monitoring technological developments
 - Promoting data protection aware design and development



International Conference of Data Protection and Privacy Commissioners 2018



International Conference of Data Protection and Privacy Commissioners 2018



International Conference of Data Protection and Privacy Commissioners 2018



European fundamental right

Treaty on Functioning of European Union – Article 16

1. Everyone has the right to the protection of personal data concerning them.
2. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities.
3. The rules adopted on the basis of this Article shall be without prejudice to the specific rules laid down in Article 39 of the Treaty on European Union.

Not an absolute right

- (4) **The processing of personal data should be designed to serve mankind.** The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity.



Recital 8

Any processing of personal data, such as information about the driver processed in event (accident) data recorders or information about the driver on drowsiness and attention monitoring or advanced distraction recognition, should be carried out in accordance with EU legislation on data protection, in particular the General Data Protection Regulation . In addition, the processing of personal data collected through the 112-based eCall in-vehicle system is subject to specific safeguards

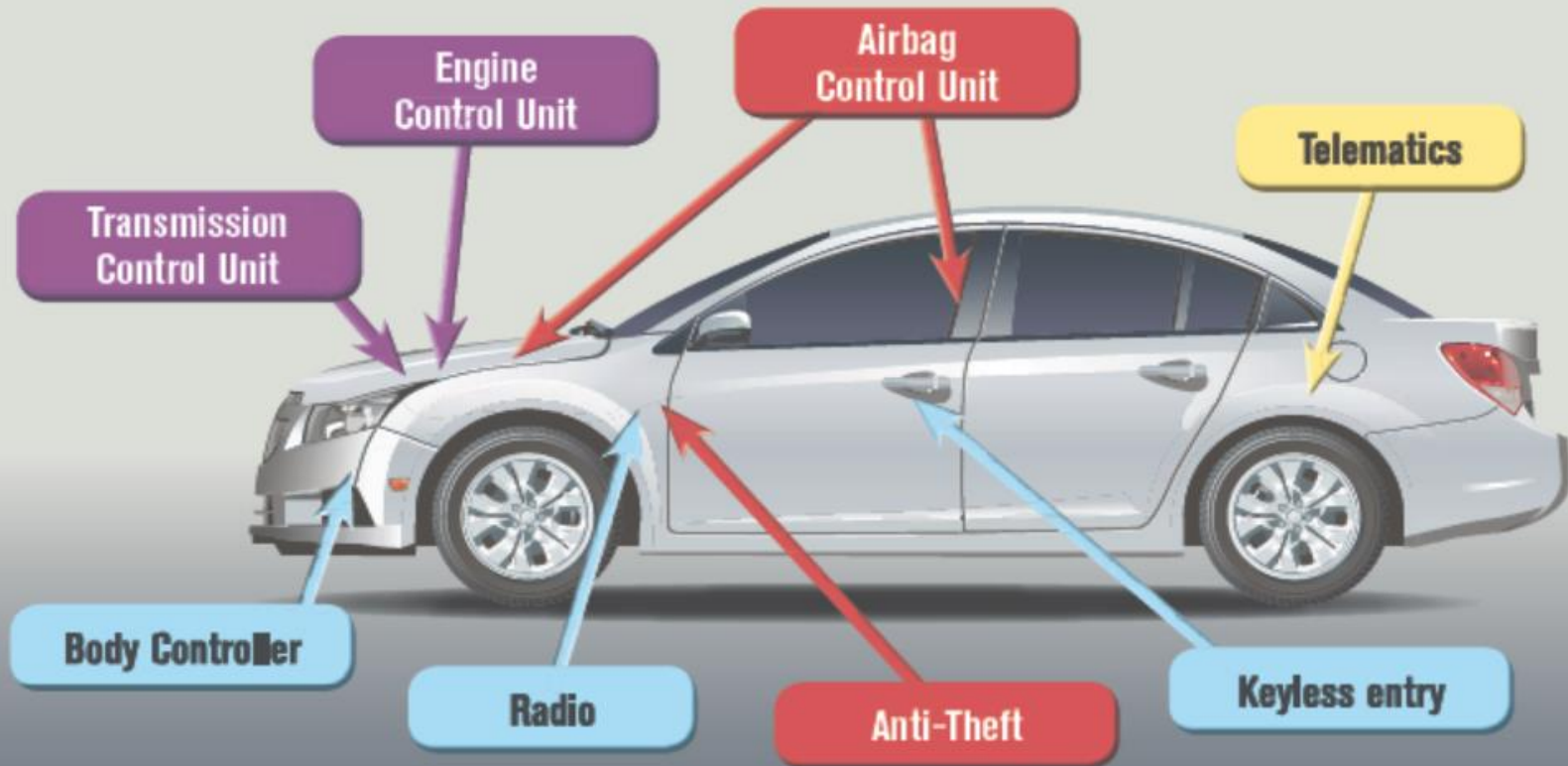
Car as a mobile device

- *All these technologies will be used also for the development of connected and automated vehicles, in which EDPS is being consulted on the privacy implications and has already provided informal comments.*
- *It may also play a role in Intelligent Transport Systems and will definitely co-operate with multimodal logistics chains.*

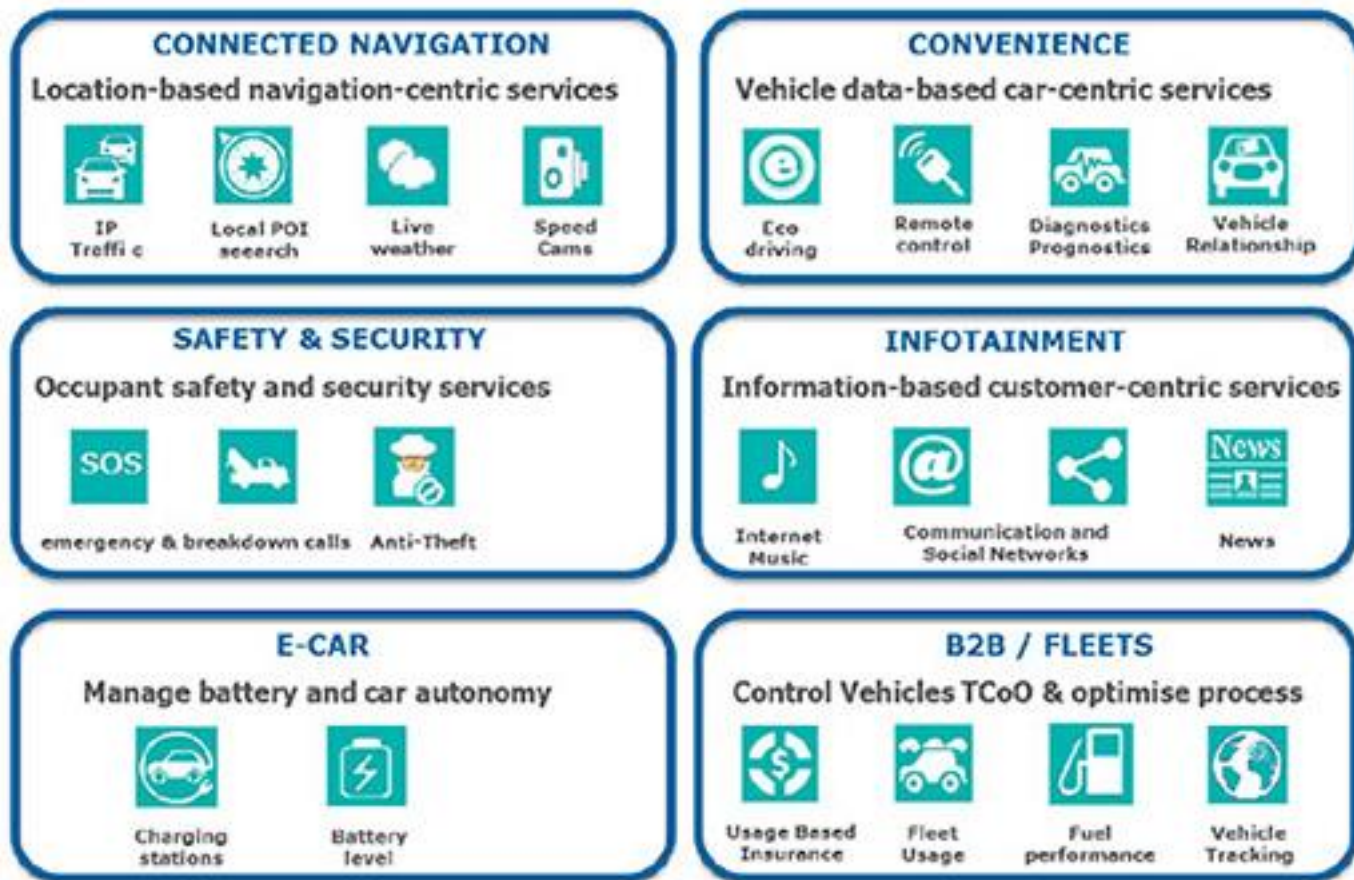
Electronic Control Units

Digital input/output channels appearing on a modern car.

Vehicle to Vehicle Communication



Connected cars



Data around

- **Engine & vehicle data:** fuel consumption, odometer, lights, etc.
- **Telematics device data:**
 - Measured data: acceleration, speed, cornering, location, direction
 - Third party sources:
 - **Public data:** road type, speed limit data
 - **Manufacturers:** fuel consumption, life-cycle parts
 - Derived data: calculation when preventive maintenance is indicated
- **Employer data:** information provided by employers (details employee, car budget etc.)
- **Lease company data:** details leased vehicle, car maintenance history
- **Driver data:** information entered by the driver
- **”Social platforms/networks”** for cars (sic!)

What Europeans think about connected cars



Based on a public survey of 12,000 Europeans in the following countries: Austria, Germany, France, Italy, Spain, Sweden, Switzerland, the Netherlands, UK, Poland, the Czech Republic, Denmark and South Africa. The survey was conducted by Ipsos and the results are representative of each country.



www.mycarmydata.eu



#mycarmydata / @FIA_Region_I



Rue de la Science 41,
1040 Bruxelles



+32 2 280 07 58



info.region1@fia.com



FEDERATION INTERNATIONALE DE L'AUTOMOBILE
REGION I - EUROPE, THE MIDDLE EAST AND AFRICA



Not everyone sees privacy the same way; however, pivotal question should be “What is in it for the driver?”



25%

Type 1: Privacy Fundamentalist

- Values privacy highly
- Rejects idea that others ‘need’ their information
- Likely will refuse to give information when asked
- In favor of strong legislation to protect privacy rights



60%

Type 2: Privacy Pragmatist

- Cares about privacy, but judges case-by-case
- Want to make informed decision about sharing
- Do want a good ‘deal’ for sharing their info
- Favors legislation to prevent undesirable excesses



15%

Type 3: Privacy Nihilist

- Do not really understand all the fuss about privacy
- Sharing information should be the norm, to reap benefits as much as possible
- Regulation is not needed; the market will sort it out

▶ ‘What is in it
for the driver?’

- An event data recorder (EDR) usually is a simple, tamper-proof, read-write memory device.
- The device can store a range of crucial vehicle data over a short timeframe before, during and after a triggering event (for example, the deployment of an airbag)
- It can provide more accurate, in-depth accident data.
- EDR data could also be used, sometimes in conjunction with other vehicle technologies, to record in the few seconds (minutes) before an accident such data as driver steering input, seat occupant size, and sound within a car.
- It accumulates data from a dedicated sensor or, sometimes, from a vehicle network.
- Information stored is limited only by the amount of available memory in the sensor.
- Once the crash data are stored on the EDR, they cannot be erased or altered.

- In modern diesel trucks, EDRs are triggered by electronically sensed problems in the engine (often called 'faults'), or a sudden change in wheel speed. One or more of these conditions may occur because of an accident.
- Information from these devices can be collected after a crash and analysed to help determine what the vehicles were doing before, during and after the crash or event.
- Studies proved that EDR data are useful in analysing crashes.
- They provide specific information about several factors, such as vehicle speed and brake application, which can help investigators understand the crash sequence and provide useful input for government authorities.



Driver drowsiness detection

- Driver drowsiness detection is a car safety technology which helps prevent accidents caused by the driver getting drowsy. Various studies have suggested that around 20% of all road accidents are fatigue-related, up to 50% on certain roads. Some of the current systems learn driver patterns and can detect when a driver is becoming drowsy.
- Many European car companies like BMW, Audi, VW, Volvo, Citroen etc have developed their own driver drowsiness detection systems. There are also in the market available independent devices that can be fitted to any vehicle for this purpose.
- Drowsiness detection systems can be divided into three main categories
 - (1) Vehicle based
 - (2) Behavioural based
 - (3) Physiological based.
- Various technologies can be used to try to detect driver drowsiness: Steering pattern monitoring which uses steering input from electric power steering system. Vehicle position in lane monitoring that uses lane monitoring camera. Driver eye/face monitoring that requires a camera watching the driver's face. Physiological measurement which requires body sensors for measure parameters like brain activity, heart rate, skin conductance, muscle activity.



Privacy concerns

- ‘My car is my castle’
- Access by employers
- Warnings for idle time / why did you stop there / dismissal for repetitive speeding
- Secondary use of data: law enforcement, tax authorities, insurers

Privacy concerns - insurance

- "It is done for public good"
- Mandatory ?
- Benefits for client
- Benefits for company
- Discounts for those who share data
 - You will get 20 % discount !!! = $100 - 20 = 80$
 - But we have to rise prices because of "general circumstances" and necessary investment by 20 % ☹ = $80 + 16 = 96$
 - Nevertheless you will pay less than you did before ☺
 - While those "not cooperating" will pay 120

I AM NOT CONVINCED IT IS FAIR



Privacy concerns

Technological advances in EDR and systems for driver's drowsiness detection may allow greater real time data collection. In addition to that, individual auto manufacturers are free to collect more data, or to collect data for longer time periods, than required. When combined with other technologies, such as on board navigation systems and mapping apps, EDR data could be transmitted beyond the vehicle owner's control.

Privacy concerns

When the technology used as indicated above implies the processing of personal data (as related to the drivers driving behaviour, physical status etc) then the GDPR shall apply to the processing. Especially the fatigue element which the drowsiness technology detects, is related to the drivers health status and can be considered following Article 9 of the GDPR, as processing of special category of data that requires enhanced protection.

Privacy concerns

Currently despite the alerts and warnings in their vehicle owner's manual, many drivers are not aware of their vehicle's recording capability. This should not be the case under the GDPR.

- **Purpose limitation and Lawful Access to data:**
 - with the owner's consent;
 - in response to a court order or probable cause of an offense;
 - for improving vehicle safety by auto dealers and auto technicians seeking to repair a vehicle,
 - for public authorities when data shall be anonymised.


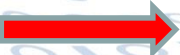


Privacy concerns

Data storage Issues

- *Is data stored locally or is it shared using software with data from other locations?*
- *Access to EDR data is generally under the control of the vehicle owner, since the physical interface for the device is inside the vehicle. However, it is possible to transmit the data, if the vehicle is so equipped.*
- *Vehicles with Advanced Automatic Crash Notification systems transmit EDR information to a central location when software in the vehicle determines that a crash has occurred, based on data from the EDR.*
- *In vehicles with wireless data transmission capabilities, it would be possible to have regular or continuous transmission of EDR data.*

Privacy concerns

Data Protection Authorities distinguish three approaches to data flows

- IN  IN, i.e., the data collected in the vehicle stay in the vehicle and are not be shared with service providers (e.g., the dashboard monitors how the user drives and provides the user with advice on how to drive in the most eco-friendly manner)
- IN  OUT, i.e., the data collected in the vehicle are shared outside of the vehicle, in order to provide services to the individual (e.g., pay as you drive)
- IN  OUT  IN, i.e., the data collected in the vehicle are shared outside of the vehicle in order to prompt an automated action back in the vehicle (e.g., dynamic *infotrafic* used by the vehicle to calculate a new itinerary)

Navigate the Collingridge dilemma

**The effects of new technology cannot be easily predicted
until the technology is extensively deployed**

**Yet once deployed become entrenched
and are then difficult to change**

- Require companies and governments who implement a new technology to evaluate the privacy aspects thereof already in the design stage
 - *Privacy by Design*, e.g., by means of a so-called Privacy Impact Assessment.
- Prediction is that there will (also) be numerous ethical issues that are currently less visible and that we do not yet have good answers for
 - Also *Ethics by Design*

Data Protection by Design and by default

Privacy by Design Resolution
27-29 October 2010, Jerusalem, Israel
**32nd International Conference of Data Protection
and Privacy Commissioners**

Privacy by Design: The 7 Foundational Principles

1. Proactive not Reactive; Preventative not Remedial
2. Privacy as the Default Setting
3. Privacy Embedded into Design
4. Full Functionality: Positive-Sum, not Zero-Sum
5. End-to-End Security — Full Lifecycle Protection
6. Visibility and Transparency — Keep it Open
7. Respect for User Privacy — Keep it User-Centric

Data Protection Impact Assessment

- Security of the processing (article 32 of the GDPR) is an essential element for the processing by these technologies especially when there will be additional risks (connected vehicles technologies) .Protecting the availability, confidentiality and integrity of the information. Security risks should be addressed depending on the technology used. Currently many vehicle manufacturers and third parties are working to develop “connected vehicle technologies,” a system in which vehicles would constantly be communicating with other vehicles and roadside infrastructure regarding traffic, road conditions, and vehicle performance data in order to minimize the risk of collision and maximize traffic flow. It is possible that hackers would be able to compromise the security of EDR data by accessing wireless data exchanges among vehicles. This information might become commercially valuable if manufacturers expand EDR data collection far beyond the minimum requirements turning the EDR into a hub for a wide variety of vehicle data, much of which may have nothing to do with crashes.



Anonymisation

Data anonymisation is essential for the purpose of central collection of data to provide input for accidents data analysis

Recommendations

- *Manufacturers shall post a window sticker in each new car, stating that there is an EDR in the vehicle, where it is located, the type of information it records, and the availability of that information to law enforcement officials.*
- The owner of the car shall control the recording of information on the EDR especially in cases where the car change ownership. An EDR is the vehicle owner's property and can be retrieved only with the owner's consent, in response to a court order, or by a vehicle repair technician.

Thank you for your attention!

www.edps.europa.eu
edps@edps.europa.eu



@EU_EDPS

