Big Data and B2B Platforms: the next big opportunity for Europe

WAVESTONE

TNO

CEPS

KOMIS

GRIMALDI STUDIO LEGALE

4th workshop: Provide the business case for "fair and equal" data sharing for cooperative, connected and automated mobility

Legal considerations: concrete challenges under data protection laws

Kletia Noti LL.M. (Columbia), Senior Associate Grimaldi

8 October 2020

Pilot – **Legal considerations: an introduction**

- Access to in-vehicle data triggers several legal considerations. **Concomitant legal obligations apply to connected cars, including**:
  - ✓ Directive 2002/58/EC (**ePrivacy Directive**): concerns processing of personal data and the protection of privacy in the electronic communications sector, relevant when data is "in transit" (communication by means of a publicly available electronic communications service). **EDPB Draft Guidelines 1/2020**: the connected vehicle and every device pursuant to it is "terminal equipment" under the ePrivacy Directive, with "terminal equipment" being defined under Directive 2008/63/CE;
  - ✓ the General Data Protection Regulation (**GDPR**);
  - ✓ **Regulation (EU) 2015/758** concerning type-approval requirements for the deployment of the **eCall in-vehicle system**;
  - ✓ Directive 2010/40/EU on the framework for deployment of Cooperative Intelligent Transport Systems (C-ITS);
  - ✓ EU and national **liability and safety rules** (EU Product Liability Directive, Directive 2001/95/EC on general product safety, Directive 2009/103/EC relating to insurance against civil liability in respect of the use of motor vehicles, and Member States liability regimes);
  - ✓ Legal framework on **cybersecurity**;
  - ✓ and EU and national **competition laws**.
- In-vehicle data, including also non personal data, beyond privacy-related aspects, touches upon aspects of data ownership, interoperability, (re)-usability and access to data, and liability vis-a-vis third parties (or vehicle users). In previous workshops, the liability, ownership and competition barriers linked to access to in-vehicle data were highlighted.

Pilot – **Legal considerations: concrete challenges under data protection laws (1)**

- We will zoom onto the data protection aspects of vehicle-generated data.

- Since the inception of the infrastructure, there has been involvement of **legal and ethical** advisor and the **organisational procedures were put in place** which guarantee **privacy-by-design. EDPB draft Guidelines 1/2020:** "Taking into account the volume and diversity of personal data produced by connected vehicles, data controllers are required to ensure that technologies deployed in the context of connected vehicles are configured to respect the privacy of individuals by applying the **obligations** of **data protection by design and by default** as required by art. 25 GDPR".

- Concrete challenges:

  - ✓ What constitutes **personal data**? See: EDPB draft Guidelines 1/2020, WP29 - Opinion 03/2017 on Processing personal data in the context of Cooperative Intelligent Transport Systems (C-ITS). Much of the data that is generated by a connected vehicle relate to a natural person that is identified or identifiable and thus constitute personal data. See DigitalEurope reply: Focus should be on reasonable likelihood that that it will be possible for a natural person to be identified or identifiable, not purely theoretical possibility (e.g. technical brake data). Hence, the GDPR applies to processing of shared server data for personalised services under the Pilot.

  - ✓ **Lawful ground for processing**: GDPR compliant **consent** (see ICCS-NTUA presentation). Important to consider also Article 5(3) of ePrivacy Directive comes into play (takes precedence over GDPR when the activity of access to the information stored in the end users' device, which constitutes personal data, is at stake: EDPB Opinion 5/2019 and draft EDPB Guidance 1/2020). EDPB: (a) **Quality of users' consent** is key: consent must be informed and specific, easily possible to withdraw, and for a specific purpose. (b) **Consent by whom**: *quid* about rented vehicle, such as through Drivy?

  - ✓ **Other lawful grounds for processing than consent** (exceptions under Article 5(3) ePrivacy Directive, other grounds under Article 6 GDPR (e.g. performance of a contract). See also Article 23(1) GDPR which may restrict rights of data subjects).

  - ✓ **Purpose limitation.** Risk: function creep. Can personal data be accessed by Law Enforcement under the Law Enforcement Directive or an insurance company for adapting insurance premiums? Here we understand it may not be an issue for secondary use of data since this is done after data is anonymised. Otherwise, data controllers must ensure that purposes are "specified, explicit and legitimate" (EDPB).

Pilot – **Legal considerations: concrete challenges under data protection laws (2)**

- Concrete challenges:

  - ✓ Processing must be as limited as possible and the use of as little data as possible must be ensured (data minimisation principle): how to reconcile with sensors amassing a large quantity of data? EDPB: Only collect data that is relevant and necessary for processing. **Utmost care must be exercised with location data**;

  - ✓ Data must be as **accurate** as possible. Appropriate **security** measures must be put in place (integrity and confidentiality principle): encrypted containers ensure security of processing (Article 32 of the GDPR);

  - ✓ **Heightened safeguards**. Particular attention must be paid to special categories of **highly sensitive data** (Article 9 GDPR), in particular:

    (a) **location data** revealing sex life or sexual orientation of an individual (geo-location data). **EDPB draft Guidelines 1/2020**: activating geo-location only when the user launches a functionality that requires it and not by default; informing data subject that geolocation has been activated, with the option to deactivate it at any time; when processing is based in consent, such consent must be GDPR compliant; providing information on the scope of processing; adequate configuration of the level of details and frequency of access to geo-location data, relative to the purpose of processing).

    EDPB Guidelines 4/2020, while dealing with contact tracing apps, can inspire here too: **ePrivacy Directive** applies. Article 5(3) and Article 6 and 9 **ePrivacy Directive** (storing is allowed only if (i) the user has given consent; or (ii) the storage and/or access is strictly necessary for the information society service explicitly requested by the user; data can only be transmitted to authorities or other third parties if they have been anonymised by the provider or, for data indicating the geographic position of the terminal equipment of a user, which are not traffic data, with the prior consent of the users). Derogations are possible under the ePrivacy Directive (see Article 15) when proportional, necessary and appropriate within a democratic society (see CJEU C-275/06, *Productores de Música de España (Promusicae) v. Telefónica de España SAU*). Additional safeguards for re-use must be ensured: data can be "further processed with the additional consent of the data subject or on the basis of a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Art. 23(1) GDPR"). Need to also look at **Member State laws** (possible fragmentation).

    (b) **biometric data: in its draft Guidelines 1/2020,** EDB recommends mechanisms to be put in place to ensure data being secure, to consider encryption etc.

Pilot – **Legal considerations: concrete challenges under data protection laws (3)**

- Concrete challenges:
  - ✓ **Offense related data:** see Article 10 GDPR. Also see EDPB draft Guidelines 1/2020: EDPB recommends local processing for these data and strong security measures be put in place.
  - ✓ **Information to data subjects** and **rights of data subjects** must be ensured: controllers must adequately inform data subject on right of access to data, right to data portability, right to erasure, to correction, etc.
    - In particular, see right to **data portability** (Article 20 GDPR): Article 20(1) of the GDPR provides that data subjects have the right to transmit the data to another controller without hindrance from the controller to which the personal data have been provided (see also Recital 68 GDPR).
    - According to the EDPB draft Guidelines 1/2020, the data controller shall provide the data subject (among others) with the information on the right to data portability in clear, simple, and easily-accessible terms. The EDPB strongly recommends data controllers to clearly explain the difference between the types of data that a data subject can receive through the rights of subject access and data portability.
    - See also Article 29 WP 2017 Guidelines on the right to data portability: "GDPR does not explain how to address the challenge of responding where a large data collection, a complex data structure or other technical issues arise that might create difficulties for data controllers or data subjects". Data controller should provide an overview "in a concise, transparent, intelligible and easily accessible form, using clear and plain language" (see Article 12(1)) of the GDPR) in such a way that data subject should always have clear information of what data to download or transmit to another data controller in relation to a given purpose".
  - ✓ **Storage limitation principle** must be ensured: do not keep it for longer than you actually need it. When personal data exceeds its retention period, organizations can either erase, anonymize, or pseudonymize the data no longer needed.
  - ✓ **Adequate data protection measures must be taken,** including organisational and decision making requirements in place to avoid data breaches (here we have attribute based access control that minimises the risk of data leaks, container solutions), codes of conduct, data protection impact assessments (DPIAs), etc). **EDPB draft Guidelines 1/2020**: Given the scale and sensitivity of the personal data that can be generated via connected vehicles, it is likely that processing will often result in a high risk to the rights and freedoms of individuals (...). Industry participants will be required to perform DPIAs to identify and mitigate the risks as detailed under Articles 35 and 36 GDPR.

Legal considerations: concrete challenges under data protection laws (4)

- Article 29 WP Opinion 05/2014: *"Once a dataset is truly anonymised and individuals are no longer identifiable, European data protection law **no** longer applies"*
  - However, the creation of a truly anonymous dataset from a rich set of personal data is not easy
  - **Anonymisation** = result of processing personal data with the aim of **irreversibly** preventing identification of the data subject

    Note: several anonymisation techniques may be envisaged as there is no prescriptive standard in EU legislation

    3 essential risks in anonymisation:
    1. *Singling out* = possibility to isolate records which identify an individual in a dataset
    2. *Linkability* = possibility to link, at least, two records concerning the same data subject or a group of data subjects
    3. *Inference* = possibility to deduce, with significant probability, the value of an attribute from the values of a set of other attributes

- Anonymisation techniques are generally be based on
  - **Randomization** ➡ Noise addition; Permutation; Differential privacy
  - **Generalization** ➡ Aggregation and K-anonimity; L-diversity/T-closeness;

  Sometimes anonymisation techniques can be used in combination with one another. **EDPB draft Guidelines 1/2020**: "If data must leave the vehicle, consideration should be given to anonymise them before being transmitted. "Anonymisation, where relevant, may be a good strategy to keep the benefits and to mitigate the risks in relation to connected vehicles".

- Pseudonymisation (≠ Anonymisation): replacing one attribute in a record (typically a unique attribute) by another. The natural person is therefore still likely to be identified indirectly. Therefore, when used alone, pseudonymisation will not result in an anonymous dataset. **EDPB draft Guidelines 1/2020**: Other techniques such as pseudonymisation can help minimize the risks generated by the data processing, e.g. through a hash algorithm. Pseudonymisation, if reinforced by security safeguards, improves the protection of personal data by reducing the risks of misuse. Pseudonymisation is reversible, unlike anonymization, and is considered as personal data subject to the GDPR.