Comments to the draft Guidelines 1/2020 of the European Data Protection Board on processing personal data in the context of connected vehicles and mobility related applications

On 7 February 2020, the European Data Protection Board published its draft Guidelines 1/2020[1] *"on processing personal data in the context of connected vehicles and mobility related applications"* (hereinafter referred to as Draft Guidelines).

The draft Guidelines present the technological development of connected vehicles, as well as the complexity of the issue. Compared to previous EDPB guidelines, the draft Guidelines seem to be less theoretical concerning the examples given; however, it still contains some questionable statements.

I. A positive statement in the draft Guidelines

Paragraph 110 acknowledges that data—in connection with a contractual relationship—can be stored until the end of the "statutory limitation periods", which is a considerable leap forward after many instances of a very restrictive interpretation of the contractual relationship [GDPR Article 6(1)b)] by WP29 and the EDPB. Unfortunately, paragraphs 89 and 123 do not follow this approach and (again) ignore civil law requirements. Further, there is no justifiable reason to distinguish between "commercial and transactional data" and "usage data" (paragraph 110), because without "usage data" (that are evidences of the parties' activities under the contract, including if the parties exercise their rights in accordance with the contract), the parties cannot exercise their rights within the limitation period (although the meaning of the limitation period is just this).

II. Issues to be reconsidered

In addition to the said positive statement of the draft Guidelines, the EDPB should further elaborate or reconsider some other points.

1. First of all, in my view, the draft Guidelines erroneously interpret the ePrivacy directive in paragraph 11 reads "*if most of the "ePrivacy" directive provisions (art. 6, art. 9, etc.) only applies to providers of publicly available electronic communication services and providers of public communication networks, art. 5(3) ePrivacy directive is a general provision. It does not only apply to electronic communication services but also to every entity that places on or reads information from a terminal equipment without regard to the nature of the data being stored or accessed."* This interpretation is not sufficiently grounded:

[1] See at https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202001_connectedvehicles.pdf

- Article 1(1) of the ePrivacy Directive (Directive 2002/58/EC) clearly defines the scope of the Directive: its provisions apply "in the electronic communication sector",
- Article 5(3) contains the term "user" which means—according to Article 2(a) of the ePrivacy Directive—"any natural person using a publicly available electronic communications service", and the definition of the "electronic communications service" (see in Directive 2002/21/EC that also applies due to Article 2 of the ePrivacy Directive).

Therefore, it is clear that Article 5(3) applies to electronic communication services (only) and it is not a "general provision": the ePrivacy Directive applies in the relationship of the actors (including user as well) falling within the scope of the ePrivacy Directive. This erroneous interpretation can also be found in Section 1.5.3 and paragraph 105.

2. Further, the interpretation of "data relating to criminal convictions and offences" (paragraph 53) or "data revealing criminal offenses or other infractions" (subchapter 2.1.3) seems to be erroneous as well. The fact that the GDPR does not give definition of "data relating to criminal convictions and offences" or "data revealing criminal offenses or other infractions" does not mean that the definition is unlimited:

a) firstly, considering Directive 2016/680, one can argue that the said data are those that are processed by "competent authorities". For example, Hungarian legislation defines "data relating to criminal convictions and offences" as *"criminal personal data means personal data related to the data subject and to a criminal record,* ***generated by organs*** *authorised to conduct criminal proceedings or to detect criminal offences,* ***or by the prison service during or prior to criminal proceedings*** *(emphasis added – Zs.B.), in connection with a criminal offence or criminal proceedings"*;
b) the interpretation given in Hungarian legislation seems to be logical. In case all "data ***revealing*** criminal offenses or other infractions" would be considered as falling within the scope of Article 10 of the GDPR, the activity of the person/entity being aware of such data (i.e. the recognition of such data) would be *per se* illegal because it is almost sure that the given person/entity will not meet the requirement of Article 10 of the GDPR;
c) Meanwhile, such data, considered by the draft Guidelines as "data relating to criminal convictions and offences" or "data revealing criminal offenses or other infractions", can be relevant in civil law relationships as well: speeding might be a criminal offence or other infraction (under criminal and/or public administration law) but it might be a breach of contract as well, e.g. in case of an insurance contract or renting cars (as part of the relevant terms and conditions). The other party to the contract (i.e. the insurance company or the car rental company) may apply contractual sanctions (e.g. termination of the contract, penalty payment, etc.). Hopefully, it does not require further explanation that a contracting party such as an insurance company or car rental company can impose terms and conditions that ban speeding (i.e. just simply demanding the observance of the Highway Code) and can control the observance of such conditions.

Therefore, the same data can be of different nature and the use of the same data in different proceedings (i.e. criminal proceeding, civil law proceeding, public administration law proceeding) cannot be assessed from the perspective of only one of the potential proceedings. Otherwise, as in the draft Guidelines, the result will be *argumentum ad absurdum*.

3. In my view, the draft Guidelines go beyond the GDPR (therefore, the draft Guidelines violate the GDPR) when the draft Guidelines prescribe that a data processor is to be involved in some data processing activities (e.g. paragraph 75): such obligation cannot be deducted from the GDPR. The data controller may freely decide if it involves a data processor in a data processing activity or not. Nothing in the GDPR authorises the EDPB to impose additional obligations on data controllers.

4. Similar concerns may be raised regarding the requirement of anonymisation of data *"before [they are] being transmitted"* from the vehicle (cf. paragraph 76). Although this is just a strong recommendation from the EPDB, but this issue (i.e. selecting and applying the appropriate TOMs) is within the responsibility of the data controller. Further, anonymisation—in many cases—seems to be pointless, since anonymised data can be useless for the purposes of the application or the service provided.

5. Similarly, in many cases, raw data are necessary for the purpose of a contract and—for example—"a score relating to driving habits" (paragraph 108) is not enough. For example, if only average speed is received by an insurance company, such an average may not reveal the violation of (e.g. an insurance or car rental) contract. It is easily understandable that 240 km can be driven in two hours with a constant speed of 120 km/h (which seems to be absolutely appropriate on highways) but can also be driven with the speed of 180 km/h for 80 minutes and with a 40-minute break (for example in the café of a petrol station). In the second case, many rules are, likely, violated and—within the insurance/car rental contract—the insurer/car rental company has the right to be aware of the violation of the contract in order to exercise its right under the contract.

6. The draft Guidelines do not pay any particular attention to the issue of who the data controller is in different cases. Seemingly, the draft Guidelines consider everything that happens in a vehicle as a single data-processing activity conducted by a single data controller. However, this is not necessarily true: the issue of controllership should be examined separately in case of each and every application, function, software installed in a given vehicle: the manufacturer is not necessary the data controller in the case of all the applications installed in the vehicle. Since the GDPR regulates relationship between "a" given data subject and "a" given data controller, the clarification of the parties of this relationship is an essential requirement. If and when this is clarified, the obligations imposed by the GDPR can be allocated to the respective data controller (cf. paragraphs 46, 78, 79, 93 etc.).

7. In connection with the remark in point 6 above, and as it has already been raised by many, it would be necessary to clarify what constitutes "a" data processing activity. When there are multiple data controllers, their activities cannot constitute a single data processing activity but,

very likely, different data processing activities with the possibility of different legal grounds, purposes (cf. paragraph 54 which uses a singular noun – "purpose"), etc. Since, under the GDPR, a legal relationship comes into being between "a" given data controller and "a" given data subject. And within this legal relationship, the rights and obligations of both parties are determined: the data controller is not responsible for other data controllers' activity even if both controllers process the data of the same data subject (unless, obviously, if they are considered as a joint controller).[2]

8. Concerning the legal grounds (cf. point 1 above as well) explained in different scenarios (paragraphs 105, 145, 160), it should be realised that in the context of a contract (and an information society service is *per se* a contractual relationship) "consent" cannot be a separate legal ground for the core elements of the contract [the subjects (parties), the object (the service(s) what is/are provided by the parties to each other) and the content (the rights and obligations of the parties)], since the contract is, *per definitionem*, a *mutual* agreement of the parties, and the existence of the contract (or any core elements of it) cannot be separated from the agreement given. In other words: withdrawal of the "consent" would mean the termination of the contract with all the contractual consequences agreed by the parties. Therefore, the "contract" necessarily absorbs the consent of the data subject—as many have clearly explained it to the EDPB already, and as—in the context the PSD2—even the EDPB has already acknowledged.

9. Lastly, it is necessary to remind the EDPB that the interpretation of the data portability is not in conformity with the intention of the legislator as expressed earlier by the Commission.[3]

by Zsolt Bártfai

[2] That is why recital 26 of GDPR must be interpreted narrowly, especially the expression [means to be used] "either by the controller or by another person", because otherwise even the anonymisation can lose its meaning: the entity receiving a document "anonymised" by another entity (the original data controller) should also be considered as data controller because in this context the original data controller can identify the persons…

[3] See for example https://iapp.org/news/a/european-commission-experts-uneasy-over-wp29-data-portability-interpretation-1/